

# NFT'LER ÖZELİNDE SİBER SİGORTAYA BİR BAKIŞ

## *An Overview of the Cyber Insurance in Specific to NFTs*

**Eyüp Ensar ŞAĞBAN \***

### **Öz**

Siber dünya, kişilerin hayatına her geçen gün daha fazla dahil olmaktadır. Hatta bir parçası haline gelmektedir. Siber ortamda ortaya çıkan riskler siber çözümler getirmektedir. Günümüz itibarıyla birçok sigorta şirketi siber sigorta hizmeti sunmaya başlamıştır. Beri taraftan, Blokzincir teknolojisinin gelişimi ile ise NFT'ler yaygın kazanmaya başlamaktadır. Bunun sonucunda milyonlarca doları bulan ürünlerin sigortalanması ihtiyacı da belirmektedir. Ancak henüz NFT sigortasına rastlanmamaktadır.

**Anahtar Kelimeler:** NFT, Siber, Risk, Sigorta, Blokzincir.

### **Abstract**

Cyberworld is included more in people's lives day by day. Furthermore, it becomes a part of the life. Cyber risks arising out of the cyber world need cyber-remedies. At the present time,

---

\* Avukat, Maden ve Petrol İşleri Genel Müdürlüğü, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Tezli Yüksek Lisans Programı Öğrencisi, ensarsagban@outlook.com ORCID: 0000-0003-2387-1581.

**Makale Gönderim Tarihi/Received:** 29.05.2021.

**Makale Kabul Tarihi/Accepted:** 06.09.2021.

**Atıf/Citation:** Şağban, Eyüp Ensar. "NFT'ler Özelinde Siber Sigortaya Bir Bakış." *Bilişim Hukuku Dergisi* 3, no. 2 (2021): 430-493.

numerous insurance companies begin to offer cyber-insurance services. On the other hand, NFTs (Non-Fungible Tokens) gain wide currency due to the development of the Blockchain's technology. Consequently, the products that reaching millions of dollars are need to be insured. Nevertheless, NFT-insurances are yet to be seen.

**Keywords:** NFTs, Cyber, Risk, Insurance, Blockchain.

## GİRİŞ

Siber âlemde ortaya çıkan virüs, trojan, solucan ve sair casus yazılım ile kötü amaçlı yazılımların sebep olduğu zararlar karşısında bu zararların bertaraf edilmesi veya sonuçlarının tazmin edilmesi maksadıyla hukuki çarelerin düşünülmesi kaçınılmazdır.

Bu yazının ele alınış sebebi öncelikli olarak kişilerin sanal varlıklarının her geçen gün arttığı siber âlemde ortaya çıkabilecek risklere karşı düzenlenecek sigortalar üzerine düşündürmektedir. Bu noktada, siber sigortanın ne olduğu ve ne şekilde koruma sağladığına değinilecektir.

Çalışmanın ikinci kısmında ise, NFT adı verilen jetonlarla emsalsiz olarak üretilen eserlerden bahsedilmektedir. Bu kapsamda, işbu jetonların kullanıcılarına ne şekilde olanaklar sağladığına değinildikten sonra, bu eserlerin sigorta sözleşmelerine konu edilip edilemeyeceği hususları değerlendirilecektir.

## İ. SİBER SİGORTANIN TANIMI, TEMEL VE İLİŞKİLİ KAVRAMLAR

Çalışmanın bu kısmında, siber sigortayı anlayabilmek için öncelikle siber risk, siber tehdit gibi temel kavramlardan bahsedilecek ve siber sigortanın dijital sigorta gibi ilişkili kavramlardan farkı açıklanacaktır.

## A. Siber Risk

Sigorta şirketleri, karşılaşacakları riskleri önceden bilip üzerine çalışma yaptıktan sonra bunların olası etkilerini bertaraf edebilmeyi amaçlamaktadır. Bunu yaparken de risklerin doğru bir şekilde ölçülmesi ve ardından bu riskin çoğunluğa dağıtılması gerekmektedir. Sigortanın temel çalışma esası da budur.<sup>1</sup> Buradan hareketle söylenebilir ki, sigorta poliçesi riskleri ortadan kaldırmaz. Yalnızca riskin dağıtılması esası ile müşterisinin finansal bir şok yaşamasının önüne geçmeyi amaçlamaktadır.<sup>2</sup>

Tüm diğer sigortalar gibi siber sigortalar açısından da bu durum geçerliliğini korumaktadır. Bu sebepten dolayı, siber tehditlerin ne olduğunun ve yaratacağı risklerin çok iyi bilinmesi gerekmektedir. Zira kimse bilmediği bir şeye karşı mücadele yürütemez. Benzer söyleyiş ile, "ölçülmeyen yönetilemez".<sup>3</sup> Bu noktada, öncelikle siber sigortanın temelini oluşturan siber riskin açıklanması gerekmektedir. Ancak farklı tanımlar mevcut ise de yaygın şekilde kabul edilen genel bir tanım olmadığından bahsedilmiştir.<sup>4</sup> Öte yandan, tanım yapma gücünün zorluğu karşısında ayrıca ifade edilmiştir ki, siber riskler bütüncül ve yıkıcı tehditler içermektedir. Bu sebeple, risklerin tespiti ve bunlarla baş edilmesi zor ve pahalıdır. Bu noktada, siber riskler

---

<sup>1</sup> Levent Sezal, "Sigortacılık Sektöründe Karşılaşılan Riskler ve Etkin Risk Yönetimi", *Sosyal Bilimler Dergisi*, no. 17, (Aralık 2018): 186-192.

<sup>2</sup> Daniel Bara, Sanja Ćorić ve Goran Jurišić, "The role of the Cyber Insurance in managing and mitigating Cyber Security Risk (With special emphasis on the potential of Croatia and Serbia Cyber insurance market)", *Međunarodna naučno-stručna konferencija IKT bezbednost (Uluslararası Bilimsel-Profesyonel BİT Güvenliği Konferansı)*, (Ocak 2015): 40.

<sup>3</sup> Sezal, "Sigortacılık Sektöründe," 192.

<sup>4</sup> Ahmet Karayazgan, "Sigorta Sektöründe Siber Risk-Siber Sigorta", iç. *Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Makalelerim Işığında)*, İstanbul: Legal Yayıncılık, 2020, 5.

sigorta poliçelerine konu risklerin diğer hiçbirine benzememektedir.<sup>5</sup>

Kavramsal açıdan bir açıklama yapma ihtiyacı karşısında, siber risk şu şekilde tanımlanabilir: Bilişim teknolojileri vasıtası ile herhangi bir sistem, hizmet veya veritabanı üzerindeki mahremiyet, bütünlük veya mevcudiyete yönelik risklerdir.<sup>6</sup>

Siber tehditlerin yelpazesinin oldukça geniş olduğu belirtilmelidir. Buna göre, veri hırsızlığı ve fidyecilik gibi günlük hayatta karşılaşılabilecek ancak daha yüksek sıklık taşıyan risklerin yanında, birçok işletmeyi etkileyebilecek ve uluslararası bilişim sistemi krizlerine neden olabilecek ancak daha düşük sıklık taşıyan riskler de bulunmaktadır. Oxera'nın çalışmasında bu büyük çaplı saldırılara NotPetya ve Wannacry saldırıları örneklenmiştir.<sup>7</sup>

## B. Siber Tehdit ve Siber Saldırıları

Siber riske dayanak olacak siber tehditler ve siber saldırılar ise belli ölçüde çeşitlilik arz etmektedir. Bu tehdit ve saldırıların taslağı şu şekilde çizilebilir: Öncelikle siber saldırı, kötü amaçlı yazılım veya hemen takip eden paragrafta belirtilen diğer şekillerde bilişim sistemlerini devre dışı bırakmak veya bilişim sistemlerinde mevcut fikri mülkiyet ve sır niteliğinde olanlar ve kişisel veriler dahil her cins verileri çalmak amacıyla yapılan saldırılardır. Siber tehdit ise, siber saldırıların başarılı olarak gerçekleşmesi olasılığını ifade eder.<sup>8</sup>

---

<sup>5</sup> PWC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience, (2015): 7.

<sup>6</sup> Oxera, The value of cyber insurance to the UK economy: Prepared for the Association of British Insurers, (Kasım 2020): 1.

<sup>7</sup> Oxera, "The value of cyber insurance," 2.

<sup>8</sup> Ahmet Korkusuz, "Kurumlarda Siber Güvenlik ve Siber Riskler" (Yayımlanmamış yüksek lisans tezi, Bahçeşehir Üniversitesi, 2020), 14-15.

Siber sigortaların kapsamı konusunda poliçelerde teminat altına alınan siber tehditler ise başlıklar itibarıyla şu şekilde sayılabilir: fidyecilik (ransomware), phishing (oltalama), kırma (cracking), ortadaki adam (man in the middle), sosyal mühendislik (social engineering) ve nesnelerin interneti (internet of things – IoT).

Siber tehdit çeşitlerine ilişkin olarak iki çalışma dikkate şayandır. Öncelikle, Şekeroğlu ve Özüdoğru tarafından yapılan çalışmada bahsedilen bu tehditlerin, sonrasında Cebeci tarafından yapılan çalışmada genişletildiği görülmektedir. Halihazırda bu konuda detaylı çalışma yapıldığı için ve doğrudan çalışmanın inceleme konusuna temas etmediği için bu tehdit çeşitlerine ilişkin detaylı açıklamada bulunulmayacaktır.<sup>9</sup>

Yukarıda sayılanlara, kredi ve banka kartı dolandırıcılıkları, DOS/DDOS atakları ve yine dolandırıcılar tarafından yollanan SMS, bilgi çalma, reklam gösterme gibi mobil tehditler de eklenebilir.<sup>10</sup> Tehditlerin tek tek vuku bulması söz konusu olabileceği gibi birden fazlası tehdidin ve hatta hepsinin birden de tek bir saldırının sonucunda vuku bulması mümkündür. Öyle ki, saldırıların büyüklüğüne göre, iflas etme ihtimali bile söz konusu olabilecektir.<sup>11</sup>

---

<sup>9</sup> İlgili çalışmalar için bkz: Sinan Şekeroğlu ve Haşim Özüdoğru, “Dijital Dönemin Koruyucuları: Siber Risk Sigortaları,” 4. *International Research Congress on Social Sciences (11-13 September 2019)*: 55-64; İpek Cebeci, “Türkiye’de Siber Risk Sigortalarına İlişkin Bir Değerlendirme,” *Üçüncü Sektör Sosyal Ekonomi Dergisi* 56, no. 1, (2021): 163-188.

<sup>10</sup> Eda Altuntaş, Emine Kara, Abdullah Buğra Soylu ve Erdem Kırkbeşoğlu, “Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar,” *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, no. 12, (Aralık 2018): 10.

<sup>11</sup> Cüneyt Çatuk, “Siber Riskler Karşısında KOBİ’lerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örneği” (Yayımlanmamış doktora tezi, Hasan Kalyoncu Üniversitesi, 2018), 1.

İlave etmek gerekir ki, siber tehditler her zaman yalnızca veri ihlaline neden olacak riskler içermez. Nitekim, anılan riskler iş süreçlerini baltalayacak şekilde zararlara da yol açabilir. Buna göre, kötü niyetli saldırılar, ele geçirilen bilgiler üzerinden rant sağlama dışında bilgileri doğrudan yok etmeye yönelik de olabilir. Karayazgan, çok uluslu bir şirkete yapılan saldırıda şirket ağının yok edildiğini belirtmektedir. Bu tarz saldırıların kurtarma maliyeti ve itibar hasarına dikkat çekmektedir.<sup>12</sup>

Buraya kadar yapılan açıklamalarda, siber tehdit ve saldırıların ancak ekonomik ve dijitalleşmiş veriler üzerinde sebep olabileceği zararlardan bahsedilmişse de ayrıca, siber tehditlerin bazı zamanlarda fiziksel hasarlara da neden olabileceği görülmüştür. OECD'nin hazırladığı raporda, Almanya'da 2014 yılında çelik fabrikasında gerçekleşen ve Ukrayna'da 2015 yılında gerçekleşen geniş ölçekli güç kesintilerinin siber saldırılar sonucunda meydana geldiği ifade edilmiştir. Dolayısıyla, her ne kadar ilk bakışta siber tehditlerin çoğunlukla maddi olmayan varlıklar ve itibar gibi maddi olmayan kavramlar üzerinde zarar oluşturacağı düşünülse de verilen örneklerde olduğu gibi gözle görülebilen zararlar oluşturması riski de mevcuttur.<sup>13</sup>

Diğer siber tehditlerin çoğunlukla gerçek kişi veya kişilerce işlenebilecek fiillere bağlı olarak hukuka aykırılık ve kast unsurlarını taşımasına karşın, nesnelere interneti (Internet of Things- IoT) kavramında teknolojik ürünlerin doğası gereği birtakım riskler barınmaktadır. Özellikle, son dönemde robot süpürge veya benzeri akıllı ev ürünlerinin yaygınlaşması sıradan bir son kullanıcı açısından da risk oluşturabilecektir.

---

<sup>12</sup> Karavazgan, "Sigorta Sektöründe", 23.

<sup>13</sup> OECD, Supporting An Effective Cyber Insurance Market, *OECD Report for the G7 Presidency*, (Mayıs 2017): 4.

Yine nesnelere internetinin gelişimi ve 5G teknolojisinin kitlelerin erişimine açık hale getirilmesi ile birlikte çevrede bulunan ve internet erişimi sağlayan milyarlarca cihazın veri sağlayıcısı olacağı beklenmektedir.<sup>14</sup> Bu noktada, bu verilerin yönetimi ile otonom karar alan bu cihazların oluşturacağı risklerin göz ardı edilmemesi gerekliliği açıktır. Zira, internete bağlı çokça cihaz olması demek, bir anlamda siber tehditlerin de bir o kadar artması demektir.<sup>15</sup>

Siber riskin çerçevesini oluşturduktan sonra, siber sigortanın tanımına yer verdikten sonra, konuya ilişkin olarak siber sigortanın diğer bazı kavramlardan farkını ortaya koyabilmek adına benzer sigorta kavramlarına ilişkin tanımlara yer vermek gerekecektir.

### C. Siber Sigorta

Siber risk, siber tehdit ve siber saldırılara ilişkin tanımların ardından, nihayetinde kavramsal olarak siber sigorta, bilişim sistemlerinde ortaya çıkan siber riske bağlı olarak sigorta lehtarının kayıplarını konu alan sigorta çeşidi olarak tanımlanmıştır.<sup>16</sup> Bir başka tanımda, siber sigorta, gizliliği haiz ve korunma ihtiyacı duyulan verilerin hukuka aykırı yollarla ortaya çıkması ile oluşacak hasara karşı yapılan sigorta poliçesi olarak ifade edilmiştir.<sup>17</sup>

---

<sup>14</sup> Sezai Tunca ve Bülent Sezen, "Sigorta İşlemlerinde Blokcincir (Blockchain) Teknolojisi Uygulamaları," *Bankacılık ve Sigorta Araştırmaları Dergisi*, no. 14, (2020): 17.

<sup>15</sup> PWC, "Insurance 2020 & beyond," 9.

<sup>16</sup> Karayazgan, "Sigorta Sektöründe," 28; Altuntaş, Kara, Soylu ve Kırkbeşoğlu, "Siber Sigortalar," 12.

<sup>17</sup> Şekeroğlu ve Özüdoğru, "Dijital Dönemin Koruyucuları", 55. Aynı yönde bkz: Alperen Çotak, "Sigortacılık Sektöründe Siber Güvenliği, Dünyada ve Türkiye'de Gelişmelerin İncelenmesi", (Yayımlanmamış yüksek lisans tezi, Marmara Üniversitesi, 2019), 16.

Sigortacılık faaliyetlerin internet kanalıyla yapılması, anılan sigortayı kendiliğinden siber sigortanın bir alanı veya çeşidi olarak kabul edilmesi sonucunu doğurmayacaktır. Tanımda da ifade edildiği üzere, öncelikle siber ortamdaki faaliyetlerden kaynaklanan bir rizikonun mevzubahis olması gerekmektedir. Tanım bu yönüyle halihazırda zaten ilgisinin de olmadığı dijital sigortadan ayrılmaktadır.

#### **D. Dijital Sigorta veya Sanal Sigorta**

Dijital sigorta veya sanal sigorta olarak adlandırılan kavramın ise, sigorta poliçelerinin yalnızca alım satım değil, ara işlemleri de dahil olmak üzere tüm süreçlerinin elektronik ortamda yürütülmesi faaliyeti olarak tanımlandığı görülmektedir.<sup>18</sup> Dijital sigortacılığın kapsamında görülen bu ara işlemleri ise, poliçelerin uygulanması, oluşan zararlara ilişkin başvuruların neticelendirilmesi ve poliçe bilgilerinin arz edilmesi gibi bilgilendirici hizmetler ile muhasebe ve aracılık hizmetleri gibi faaliyetlerden oluşmaktadır.<sup>19</sup>

Dijital sigorta hizmetlerinin özellikle konut veya araç sigortaları gibi somut verileri belirgin olan ve bu noktada birbirlerine yakın teklifler sunulabilen sigorta poliçeleri açısından dikkat çektiği belirtilebilir. Bu şekilde mobil ve dijital dağıtım kanalları üzerinden poliçe teklifleri sunulabilmektedir.

---

<sup>18</sup> Nuri Ömürbek ve Fatma Gül Altın, "Sigortacılık Sektöründe Bilgi Teknolojilerinin Uygulanmasına İlişkin Bir Araştırma," *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 13, no. 3, (2008): 113.

<sup>19</sup> Müberra Yurdakul ve Nilüfer Dalkılıç, "Sigortacılık Sektöründe Dijital Çağ," *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, no. 50, (Ekim 2016): 50-52.



Ayrıca, tüketicilerin karşılaştırma yapma ve çıkarlarına en uygun düşeni satın alma kolaylığı da oluşmaktadır.<sup>20</sup>

### E. Diğer İnternet Sigortaları

Siber sigortanın, dijital sigorta kavramının yanı sıra, farklı sigorta teminatları içeren diğer bazı sigortalardan farkının da ortaya konulması gerekir.

Bu noktada, örnek olarak İnternet aracılığıyla hizmet sunanların yapacağı “İnternet Sorumluluk Sigortası” ve bu hizmetin sunulduğu teknolojik ürünlerde ortaya çıkacak teknik risklerin teminat altına alınması maksadıyla “Elektronik Cihaz Sigortalarından” bahsedilebilir.<sup>21</sup>

Elektronik cihaz sigortaları, siber faaliyette bulunulan teknik cihazların yangın, elektrik kesintisi, su baskını ve sair sebeplerle uğrayabileceği maddi zararların teminat altına alması ile siber sigortadan ayrılmaktadır.

İnternet sorumluluk sigortası ise, internet erişimi sağlayan hizmet sağlayıcıların veya e-ticaret yapan kimselerin mesleki sorumluluklarına istinaden düzenlenen poliçeleri ifade etmektedir.

Netice itibarıyla, gerek elektronik cihaz sigortaları olsun ve gerek internet sorumluluk sigortaları olsun, siber riske istinaden

<sup>20</sup> Levent Sezal, “Türk Sigortacılık Sektöründe Mobil Teknoloji Uygulamaları”, *Sosyal Bilimler Dergisi*, no.19, (Ocak 2018): 131. Bul da ayrıca sağlık ve hayat sigortası gibi karmaşık ve çok değişkenli sigorta poliçeleri için geleneksel dağıtım kanalları olan acente ve brokerlere olan ihtiyacın ortadan kalkmadığını belirtmektedir. Konu hakkında daha detaylı açıklama için bkz: Aycan Bul, “Sigorta Dağıtım Kanallarının Dijitalizasyonu”, 15. Ulusal İşletmecilik Kongresi Bildirileri, (26-28 Mayıs 2016): 1. Erişim Tarihi: 09 Ağustos 2021. [https://www.researchgate.net/publication/313837149\\_SIGORTA\\_DAGITIM\\_KANALLARININ\\_DIJITALIZASYONU](https://www.researchgate.net/publication/313837149_SIGORTA_DAGITIM_KANALLARININ_DIJITALIZASYONU).

<sup>21</sup> Huriye Kubilay ve Atakan Kubilay, “Sigortacılık Sektöründe Bilişim Teknolojilerinin Rolü,” *Yaşar Üniversitesi E-Dergisi*, no. 8, (2013): 1827.

düzenlenen poliçeleri ifade etmediği için çalışma konusu olan siber sigorta kavramının dışında kalmaktadırlar.

## II. SİBER SİGORTANIN TİCARİLEŞTİRİLMESİ

Sigorta şirketlerinin esasen bir şirket olması hasebiyle, asıl amaçlarının klasik şirket anlayışıyla paralel olarak kâr etmek olduğu belirtilebilir. Aksi bir düşüncenin kabulünde bu şirketlerin dernek veya vakıf gibi örgütlenmesini gerektirirken, bunun imkansızlığı karşısında sigorta teminatına konu edilebilecek herhangi bir riskin belirlendikten sonra öncelikli amacın bunun ticarileştirilmesi olduğu da belirtilebilir. Üretilen primler incelendiğinde de siber sigortanın ılımlı bir şekilde artan ivmeyle ticari menfaatler sağladığı görülmektedir. Çalışmanın bu bölümünde siber sigorta poliçelerinin çerçevesi çizilerek, siber risk artışına paralel olarak siber sigorta poliçelerindeki değer artışına değinilecektir.

### A. Siber Sigorta Poliçeleri

Siber sigortalar, dünyanın diğer yerlerinde olduğu gibi Türkiye’de de sigorta şirketleri, acente ve brokerler tarafından veri koruma, siber koruma ve sair isimlerle poliçe olarak tüketicilere sunulmaya başlanmış durumdadır.

Yirminci asrın son on yılında dünyada ortaya çıkan<sup>22</sup> siber sigortanın Türkiye’de ilk kez 2017 yılında Anadolu Sigorta tarafından piyasaya sürüldüğü ifade edilmektedir.<sup>23</sup> Beri taraftan, Amerika merkezli AIG Sigorta’nın ise Türkiye’de 2012

---

<sup>22</sup> OECD, “Supporting An Effective,” 5.

<sup>23</sup> Sigorta Gündemi, “Siber risklere karşı Türkiye'nin ilk bireysel sigortası”, Erişim Tarihi: 24 Mayıs 2021. <http://www.sigortagundem.com/haber/siber-risklere-karsi-turkiyenin-ilk-bireysel-sigortasi/1262619#ixzz52TtNbm84>.

yılından beri bu alanda sigorta hizmetinin verildiği belirtilmiştir.<sup>24</sup>

Bugün ise hemen her sigorta şirketi tarafından ürün olarak sunulmasa dahi, Hazine ve Maliye Bakanlığının hayat dışı sigorta branşında faaliyet gösteren ruhsat sahibi 39 sigorta şirketinden 11'inin tek başına siber sigorta poliçesi teklif ettiği görülmektedir.<sup>25</sup> Sigorta şirketlerinin ayrıca acente ve brokerleri tarafından da tekliflerini sunduğu görülmektedir. Acente ve brokerler bir yana Türkiye'de farklı isimlerle siber sigorta ürünü teklif eden sigorta şirketleri ise tespit edilebildiği kadarıyla şunlardır:

Aksigorta A.Ş.	Siber Koruma Sigortası
Allianz Sigorta A.Ş.	Siber Sorumluluk Sigortası
Anadolu Anonim Türk Sigorta A.Ş.	Ticari Siber Güvenlik Paket Poliçesi
CHUBB European Group SE Merkezi Fransa Türkiye İstanbul Şubesi	Veri Koruma Sigortası

<sup>24</sup> Gözde Yeniova, "Siber saldırılara karşı sigorta teminatı geldi," Ekonomist, Erişim Tarihi: 24 Mayıs 2021. <https://www.ekonomist.com.tr/teknoloji/siber-saldirilara-karsi-sigorta-teminati-geldi.html>.

<sup>25</sup> Hazine ve Maliye Bakanlığı, 26 Ekim 2020 tarihi itibarıyla Sigorta ve Reasürans Şirketleri ile Emeklilik Şirketlerinin Ruhsat Sahibi Olduğu Branşları Gösterir Tablo, Erişim Tarihi: 24 Ağustos 2021. <https://ms.hmb.gov.tr/uploads/2020/10/Sigorta-ve-Reas%C3%BCrans-%C5%9Eirketleri-ile-Emeklilik-%C5%9Eirketlerinin-Ruhsat-Sahibi-Oldu%C4%9Fu-Bran%C5%9Flar%C4%B1-G%C3%B6sterir-Tablo-26.10.2020.xlsx>.

Doga Sigorta A.Ş.	Ticari Siber Güvenlik Sigortası
Zurich Sigorta A.Ş.	KOBİ Kimliğim Güvende

**Tablo.1:** Kurumsal müşterilerine siber sigorta teklifinde bulunan sigorta şirketleri

Anadolu Anonim Türk Sigorta A.Ş.	Bireysel Siber Güvenlik Sigortası
Axa Sigorta A.Ş.	Dijital Güvence Sigortası (Siber Sigortam Yanımda)
Mapfre Sigorta A.Ş.	Özel Risk Sigortaları (Bilgisayar Suçları)
Ray Sigorta A.Ş.	Cyberella
Quick Sigorta A.Ş.	Kimlik Hırsızlık Sigortası
Sompo Sigorta A.Ş.	Dijital Güvenlik Sigortası
Zurich Sigorta A.Ş.	Zurich Dijital Güvenlik Sigortası

**Tablo.2:** Bireysel müşterilerine siber sigorta teklifinde bulunan sigorta şirketleri

## B. Siber Aktivitelere Artış

Siber sigortaların özellikle taçvirüs<sup>26</sup> döneminin de etkisi ile çevrimiçi faaliyetlerin ve siber risklere yönelik farkındalığın

<sup>26</sup> Türk Dil Kurumuna ait "Türk Dili" dergisinde yayımlanan bir çalışmada, "korona" ve ilişkili kelimelerin bulunduğu terimlerin önceki dönemlerde Türkçe'ye "taç" ile ilişkili olacak şekilde çevrildiği belirtilmekte ancak

artması sonucu talep artışına geçtiğini söylemek mümkündür.<sup>27</sup> Yeni normal olarak ifade edilen bu süreç içerisinde sosyal hayat günbegün sanal hayatla bütünleşmekte, günlük hayatta sürdürülen aktiviteler adım adım sanal ortama taşınmaktadır. Sanal ağ üzerindeki bu bağlantı artışı ile birlikte, siber saldırıların hedefinin de arttığı ve dolayısıyla küresel ölçekte siber risklerin ciddileştiği söylenebilir.

Özellikle, bulaş durumunu azaltmak maksadıyla ve kimi sektörlerde bulaştan bağımsız olarak kalıcı hale getirilen uzaktan çalışmaya yönelik talebin artış göstermesi siber risklerin de artması sonucunu doğuracaktır.

### C. Personelin Uzaktan Çalışmasına Bağlı Risk Artışı

Aile, Çalışma ve Sosyal Hizmetler Bakanlığınca hazırlanan ve 10 Mart 2021 tarihli ve 31419 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren “Uzaktan Çalışma Yönetmeliği” ile her ne kadar uzaktan çalışmanın sözleşmesel esasları tespit edilmiş ve çerçevesi ortaya koyulmuşsa da siber riske ilişkin etraflıca bir düzenlemeye yer verilmediği görülmektedir.

Anılan Yönetmeliğin 11’inci maddesi ile, verilerin korunması amacıyla gerekli önlemlerin alınacağı ve buna ilişkin hususlara sözleşmede açıkça yer verileceği düzenlenmiş ise de veri koruma faaliyetinin ne şekilde gerçekleşeceğine yönelik

---

koronavirüs özelinde henüz bir tanım getirilmemektedir. Anılan incelemede yalnızca, “koronavirüs” kelimesinin bitişik yazılması gerektiğine değinilmiştir. Konu hakkında bkz: Hamza Zülfikar, “Gündemi Meşgul Eden Sağlık Terimleri,” *Türk Dili*, no. 821, (Mayıs 2020): 11. Ortaya çıkan tabloda önceden taç kelimesi ile ilintili olacak şekilde çeviri yapıldığı gözetilerek dilimize bu şekilde geçmesi bu çalışmanın yazarı tarafından temenni edilmektedir.

<sup>27</sup> Oxera da bu hususu belirtmektedir. Bkz: Oxera, “The value of cyber insurance”, 11.

herhangi bir detaydan bahsedilmemiştir.<sup>28</sup> Bu açıdan, siber riskteki artışın önlenmesi amacıyla ne yapılacağı hususu cevapsız kalmakla, işletme sahiplerinin bu sorunları kendilerinin çözmelerinin beklendiği anlaşılmaktadır.

Bu haliyle, uzaktan çalışanın sebep olabileceği siber risklerin işletme organizasyonu açısından üzerinde durulması gereken bir risk olduğu ihmal edilmemelidir. Çünkü, Verizon'un yaptığı çalışmaya göre, işletme çalışanının hakimiyeti olmaması nedeniyle oluşan sistem hatası ve oltalama gibi saldırılara maruz kalınması gibi risk doğuran hareketler, siber tehdide konu olan tüm riskler içerisinde %40'ı aşan bir kısmı oluşturmaktadır ki bu hiçbir şekilde göz ardı edilebilecek bir oran değildir.<sup>29</sup> Bu sebeple, özellikle çalışanların eğitimi hususu bir işletme açısından hayati önem taşımaktadır. Anılan Yönetmeliğin herhangi bir çerçeve ortaya koymuyor oluşu bu istatistikle birlikte değerlendirildiğinde, siber riskin azaltılması amacıyla işletme sahiplerine (= işverenlere) ciddi bir sorumluluk doğmaktadır.

#### **D. Siber Sigortada Ekonomik Beklentiler**

Sektörün içinde bulunduğumuz yıl itibarıyla 10 milyar Dolara yaklaşacağı<sup>30</sup> 2022 yılında ise 15 milyar Dolar seviyelerine

---

<sup>28</sup> RG. 10.03.2021, S.31419. "(1) İşveren; uzaktan çalışanı, işyerine ve yaptığı işe dair verilerin korunması ve paylaşımına ilişkin işletme kuralları ve ilgili mevzuat hakkında bilgilendirir ve bu verilerin korunmasına yönelik gerekli tedbirleri alır. (2) İşveren, korunması gereken verinin tanım ve kapsamını sözleşmede belirler. (3) Verilerin korunması amacıyla işveren tarafından belirlenen işletme kurallarına uzaktan çalışanın uyması zorunludur."

<sup>29</sup> Verizon, 2021 Data Breach Investigations Report, 15.

<sup>30</sup> Sözcü, "Siber sigorta pazarı 9.5 milyar dolara ulaşacak," erişim tarihi: Mayıs 24, 2021, <https://www.sozcu.com.tr/2021/sigorta/siber-sigorta-pazari-9-5-milyar-dolara-ulasacak-6221265/>.

ulaşacağı öngörülmektedir.<sup>31</sup> Bu alandaki çalışmalar ve farkındalıklar arttıkça piyasadaki pastanın genişleyeceğini tahmin etmek güç değildir. Özellikle kamu tarafından da gerek regülasyon yoluyla ve gerek teşvikler ile desteklenmesi halinde yükseliş trendinin hızlanacağı beklenebilir.

Marsh'ın yeni yayımladığı bir çalışma göstermektedir ki, özellikle pandeminin getirdiği siber ağa katılımın artması ve bunun doğrudan sonucu ile siber risklerin artışına bağlı olarak siber sigorta branşındaki fiyat artışı ABD'de %56'yı ve Birleşik Krallık'ta %35'i bulmuş vaziyettedir. Bu artışlar önceki seneye göre %50 daha fazla bir artış anlamına gelmektedir.<sup>32</sup> Bu durumun kullanıcı talebini olumsuz etkilememesi halinde üretilen primlerin toplam değerinde bir artış yaratacağı da ifade edilebilir. Fiyat artışının tüketici yönünde tolere edilebilir seviyede kalmasının, piyasaya katılma konusunda diğer paydaşların da iştahını artıracaktır. Nihayetinde, ekonomik bir kazanım sonucu doğabilecektir.

Siber sigortanın sağladığı teminatlarla risk transferine olanak sağlamanın yanı sıra, siber riskin gerçekleşmesi halinde zararın giderilmesi maksadıyla yapılacak harcamanın ekonomik hayatın içinde tutulması da refah artışına olumlu yönde etki sağlayacaktır. Nitekim, siber güvenlik tedbirlerine harcanan bedel, riskin gerçekleşmesi ihtimalinde ortaya çıkacak kaybın çok daha azı bir bedel ile iç ekonomide kalmaktadır.<sup>33</sup>

Önceki bölümde ifade ettiğimiz nesnelere internetinden de beklentiler bu yönde olup siber sigorta ile uyum içinde çalışması

---

<sup>31</sup> Shay Simkin'in açıklamalarından alıntılan Dünya, "Siber sigorta pazarı 15 milyar dolara gidiyor," erişim tarihi: Mayıs 24, 2021. <https://www.dunya.com/sectorler/sigortacilik/siber-sigorta-pazarı-15-milyar-dolara-gidiyor-haberi-455727>.

<sup>32</sup> Marsh, *Global Insurance Markets: Pricing Increases Moderate in Second Quarter*, (Temmuz 2021): 2.

<sup>33</sup> Oxera, "The value of cyber insurance," 13.

arzu edilmektedir. Nesnelerin internetinin gelişimiyle birlikte bu cihazların internete olan erişimi sayesinde tehditlerin önceden tespiti ile sigorta müşterilerinin karşılaşabilecekleri risklere karşı uyarma ve yönlendirme etkileşimi sağlayabilecektir. Böylelikle, sigortanın rizikonun gerçekleşmesinden sonra ortaya çıkan zararın tazmin edici özelliğinden ziyade, hasarın gerçekleşmesinden evvel yani önleyici bir nitelik kazanması beklenecektir. Bu şekilde de sigorta şirketlerinin en büyük gider kalemi olan hasar ödemeleri de azalacaktır.<sup>34</sup> Ayrıca yine nesnelerin interneti uygulamaları ile son kullanıcıların beklentilerinin daha rahat ölçülerek kişiselleştirilmiş tekliflerin sunulması beklenmektedir.<sup>35</sup>

### **III. SİBER RİSKİN GERÇEKLEŞMESİ İLE SİBER SİGORTA TEMİNATININ DEVREYE GİRMESİ VE BU KONUDAKİ ENDİŞELER**

Siber sigortaya konu olan rizikonun gerçekleşmesi ile veri ihlali veya yukarıda izah edilen şekilde benzeri hasarlar ortaya çıkabilmekte ve ciddi bir mali külfet yaratan sonuçları doğabilmektedir. Siber riskin gerçekleşmesini müteakiben sigortalılarca siber sigorta poliçesindeki teminatlardan faydalanılmak istenecektir. Sigortalının poliçe şartlarına uygun davranması halinde bu imkanların sigortacı tarafından tanınması gerekmektedir. Beri taraftan, siber sigorta ödemesinin temini konusunda ve siber riskin poliçe kapsamında olup olmadığı noktasında sigortalıların endişesi ortaya çıkabilmektedir. Halihazırda, çoğu sigorta şirketinin kaçınmakta olduğu siber sigorta alanında çalışan sektör bileşenlerinin bu noktada siber riskin vuku bulması ile ortaya çıkan zararların giderilmesine yönelik çalışması gerekmekte, müşterilerini adeta

---

<sup>34</sup> Bul, "Sigorta Dağıtım Kanallarının Dijitalizasyonu," 5.

<sup>35</sup> Fatih Acer, "Sigorta sektörü InsurTech ile gelişecek," *Sigorta Medya*, erişim tarihi: Temmuz 31, 2021, <https://www.sigortamedya.com.tr/fatih-acer-sigorta-sektoru-insurtech-ile-gelisecek/>.



ikinci bir zarara uğratacak şekilde tutumda bulunmamaları önem arz etmektedir. Bu bölümde, siber riskin gerçekleşmesi ile ortaya çıkan durum ve beklentiler ile siber sigorta teminatlarına değinilecektir.

### A. Siber Riskin Gerçekleşmesi

Önceki bölümde belirttiğimiz üzere, siber tehdit ve saldırılara ilişkin temel yaklaşım gerekli tedbirlerin alınarak risklerin azaltılmasıdır. Ancak öte yandan siber risklerin gerçekleşmesi ihtimalinde ise siber sigorta ile teminat altına alınan yükümlülükler uygulama bulacaktır. Buna göre, kişilerin ortaya çıkan zararlarının sigorta şirketine aktarılması mümkün olacaktır.<sup>36</sup>

Çalışmanın önceki kısmında belirtilen ekonomik duruma rağmen piyasa aktörlerinin yaklaşımı çeşitlilik arz etmektedir. Zira, siber sigorta ile risk transferi yapılan rizikonun gerçekleşmesi halinde teminatların yerine getirilmesi için sorumluluğun nihai üstlenicisinin kim olacağı noktasında bir endişe mevcuttur. Buna göre; sigorta şirketi, acente ve broker gibi kimi piyasa oyuncuları milyarlarca doları bulan primlerden pay almaya yanaşmakta iken, kimi sigorta paydaşları ise bu riskin üstlenmek için fazlaca büyük olduğunu düşünerek siber sigorta tekliflerinden kaçınmaktadırlar.<sup>37</sup>

Marsh'ın çalışmasının ABD içinde yapılan araştırmanın en önemli kısımlarından birinin bazı sigorta paydaşlarının siber koruma teminatı hizmeti sunmaktan vazgeçtiğini, kimilerinin ise sigorta poliçelerinde kayda değer değişikliklerle daraltmaya gittiğini göstermektedir.<sup>38</sup> Çalışmanın Avrupa ayağında ise

---

<sup>36</sup> OECD, "Supporting An Effective," 3.

<sup>37</sup> PWC, "Insurance 2020 & beyond," 9.

<sup>38</sup> Marsh, "Global Insurance Markets," 6.

trendin devam ettiği ancak sözleşmesel hükümlerde ve teminat dışı hallerin düzenlenmesinde değişikliklerin devam ettiği görülmektedir.<sup>39</sup>

## B. Siber Sigorta Teminatları

Siber sigortanın yapısı gereği birinci ve üçüncü taraf teminatlar getirdiği görülmektedir.<sup>40</sup> Ancak siber sigortanın, teminatlarının rizikonun gerçekleşmesinden sonra ve öncesi için ikiye ayrılarak incelenmesi mümkündür. Aslında geleneksel sigortacılık anlayışı ekseninde siber sigortanın sağladığı temel teminatın finansal zarar, hukuki yardım ve tazminat kalemleri gibi hususlar olduğu düşünülmektedir. Fakat klasik anlayışa ilaveten aslında bu gibi riskleri azaltmak amacıyla, saldırılar gerçekleşmeden öncesine yönelik personelin eğitilmesi, gerekli siber güvenlik önlemlerinin alınması ve ihlal oluşacak alanların ortaya çıkarılmasına yönelik çalışmalar ile riskin azaltılması ve harcamaların bu şekilde dengeli tutulması da öncelikli yararları arasında sayılabilir.<sup>41</sup>

Siber tehditlerin yol açtığı hasarlar ve teminatların kapsamı ise genel olarak veri kaybı, şantaj, iş ve üretimlerin durdurulması, ele geçirilen bilgilerin ifşası ve itibar kaybı olarak belirtilmektedir. Üçüncü kişilerin hasarlarının teminata alınması açısından ise dava masrafları, kriz yönetimi ve medya sorumluluğu ile veri ve gizlilik yükümlülüklerine dair teminatlar da sayılabilir.<sup>42</sup>

Bireysel müşterilere yönelik olarak sunulan siber sigorta tekliflerinde ise; kimlik hırsızlığına karşı getirilen korumalar, ödeme araçlarının hileli kullanımından oluşacak zararlar ile

---

<sup>39</sup> Marsh, "Global Insurance Markets", 11-12.

<sup>40</sup> Karayazgan, "Sigorta Sektöründe," 41.

<sup>41</sup> Oxera, "The value of cyber insurance," 12, 13.

<sup>42</sup> Altuntaş, Kara, Soylu ve Kırkbeşoğlu, "Siber Sigortalar," 11-13.

sanal saygınlığa ilişkin hukuki destekler, ortalama gibi saldırılar sonucu oluşacak maddi kayıpların poliçede belirtilen miktarla sınırlı olmak üzere giderimi, siber fidye ve şantajlar sebebiyle doğacak kayıplar, veri tarama hizmetleri ile kredi ve bank kartı ile cep telefonu, e-posta ve benzeri araçlara yönelik şifre koruma hizmetleri ile ihlal halinde poliçe çerçevesinde kayıpların tazmini, iletişim ve seyahat masrafları görülmektedir.<sup>43</sup>

Literatürde belirtilen teminatlar bahsinde sayılanlara ayrıca *siber kişiliğin korunması* hususu da eklenebilir. Zira her geçen gün kişilerin gerçek hayatlarıyla kimi zaman bütünleşik ve kimi zaman ise ayrı bir sanal kişilikleri oluşmakta ve bu kişiliklere olan olası saldırıların teminata dahil edilmesi talebi ise haklılık arz etmektedir. Sosyal medya ve paylaşım sitelerinde içerik üreticisi olarak kazanç elde edenler açısından sanal kişiliklerinin ve itibarlarının korunması hususu bu vesile ile bir kez daha anlaşılmaktadır.

Nihayetinde siber sigortanın maddi varlığı olmayan siber değerlere ve bilgilere karşı oluşan tehditleri tamamıyla oradan kaldıran bir nitelikte olmadığı anlaşılmaktadır. Siber sigortanın siber güvenlik ihlali ile oluşan maddi zararlara karşı bir önlem olarak lehtarını finansal kayıplarını azaltmayı amaçladığı görülmektedir.

Bazı ülkelerde sigorta kapsamlarına adli ve idari para cezalarının dahil edilememesinin o ülkeler özelinde siber sigortanın gelişimini kısıtladığı düşünülmektedir.<sup>44</sup> Ülkemizdeki sorumluluk sigortaları genel şartlarında da

---

<sup>43</sup> Söz konusu teminatlar, siber sigorta teminatlarının neler olabileceğini göstermek amacıyla, sigorta şirketlerinin bireysel tekliflerinde yer alan teminatlara göre bu çalışmanın yazarı tarafından derlenmiştir. Her şirketin sunduğu teklifte, bu açıklamada sayılan teminatların tamamının bulunduğu anlamına gelmemektedir.

<sup>44</sup> OECD, "Supporting An Effective," 8.

taraf larca aksine anlaşıl madıkça idari ve adli para cezalarının teminat kapsamının dışında olduđu görölmektedir. Ancak yine ölkemizdeki siber sigorta poliçelerinin kimilerinde para cezalarının da teminat kapsamına alındığı görölmektedir.<sup>45</sup> Tüketicilerin bu aşamada ihtiyaç duyduđu teminatı içeren poliçeyi tercih etmelerinde fayda olacaktır.

Klasik teminatların yanı sıra bazı poliçelerde anlık risk takibi ile SMS ve e-posta bilgilendirmesi ve antivirüs yazılımının poliçe içeriği olarak sunulması gibi önleyici hizmetler de sunulduđu görölmüştür.<sup>46</sup>

Sigorta şirketlerinin teminatların uygulanabilmesi için yer yer sigortalılara antivirüs yazılımlarını güncel tutma, düzenli yedekleme faaliyetinde bulunmuş olma ve benzeri yükümlölükler getirdiği de görölmektedir.

Siber sigortaya ilişkin olarak poliçe ile birlikte teminatların başladığı hususu ifade edilmektedir. Karayazgan'a göre, Türk Ticaret Kanunu'nun 1473'üncü maddesinden hareketle<sup>47</sup>, zararın sigorta süresi içerisinde gerçekleşmesinin sigortanın işletilmesi için yeterli olduğunun ayrıca talebin bu süre içerisinde yapıp yapılmadığına bakılmasına gerek olmadığını kabulü gerekmektedir.<sup>48</sup> Ancak, anılan hükmün Türk Ticaret

---

<sup>45</sup> Örneğin, Anadolu Sigorta'nın bilgilendirme formunda idari para cezalarının teminat kapsamında olduğu açıkça yazılmıştır.

<sup>46</sup> Örneğin, Axa Sigorta'nın teklifinde önleyici hizmetler açıkça belirtilmiş, Quick Sigorta'nın teklifinde Bitdefender Total Security isimli antivirüs ve güvenlik paketinin poliçe kapsamına dahil edildiği gösterilmiştir.

<sup>47</sup> RG. 14.02.2011, S.27846. "Sigortacı sorumluluk sigortası ile sözleşmede aksine hüküm yoksa sigortalının sözleşmede öngörülen ve zarar daha sonra doğsa bile, sigorta süresi içinde gerçekleşen bir olaydan kaynaklanan sorumluluğu nedeniyle zarar görene, sigorta sözleşmesinde öngörülen miktara kadar tazminat öder."

<sup>48</sup> Karayazgan, "Sigorta Sektöründe," 49.

Kanunu'nun sorumluluk sigortaları başlığı altında olduğu düşünüldüğünde, şayet siber sigorta teminatlarının mal sigortası kapsamında değerlendirilmesi yapılacak ise, tersine bir yorum suretiyle talebin de sigorta süresi içerisinde yapılması gerekecektir.

### C. Siber Sigortaya Yönelik Endişeler

Kimi sigortaçıların siber sigortaya yönelik endişelerinin anlaşılması mümkündür. Çünkü, siber sigortanın üzerinde yeterince çalışma yapılmaması ve saldırıların ne şekilde etkiler doğurabileceğine dair yeterli bilgi olmaması sigorta şirketleri açısından siber sigortanın üzerindeki şüphelerin kalkmasını zorlaştırmaktadır.<sup>49</sup>

Üstelik siber sigorta konusundaki farkındalık ve verilerin yetersizliği yalnızca sigortacı tarafında değil, sigortalı tarafında da endişeye neden olmaktadır. Burada önemle belirtilebilir ki, sigortacılık mesleğinin kilit taşının "güven" olduğu unutulmamalıdır. Siber risklerin olduğu "güvenilmez" bir ortamda, kişilerin sigorta yaptırmasının önemini anlatabilmek ve bu kişilerin güvenini kazanabilmek önem arz eder. Nitekim, kimse güvenmediği bir hizmete karşı bedel ödemek istemeyecektir.<sup>50</sup>

Güven meselesine sebep olan hususun ve esasen asıl unsurun ise tecrübe eksikliği olduğu ifade edilmektedir. Zira sigorta hizmetinin sağlanabilmesi için şirketin konuya ilişkin elinde veri olması gerekir. Siber sigortaların henüz bu denli veri

---

<sup>49</sup> PWC, "Insurance 2020 & beyond", 4.

<sup>50</sup> Bu konuda meslek mensubunun görüşleri için bkz: Okan Utkueri, "Dijital Sigortacılık ve Güven", Sigortacı Gazetesi, Erişim Tarihi: 27 Mayıs 2021. <https://sigortacigazetesi.com.tr/dijital-sigortacilik-ve-guven/>; Siber sigortanın önündeki en önemli engellerden birinin güven meselesi olduğu hakkında bkz: Cebeci, "Türkiye'de Siber Risk", 181.

sağlayamaması da riskin ve karşılığı olan primin öngörülmesini zorlaştırmaktadır.<sup>51</sup> En azından prim karşılığı olan teminat kapsamını tüketici aleyhine daraltmaktadır.

Sigorta şirketlerinin de sosyal medya ve internet kanallarında varlıklarını artırmaları ile uygulamalı olarak riskleri görme ve tecrübe etme şanslarının artması bu konudaki gelişimin diğer sigorta branşlarına kıyasen daha hızlı olacağı beklenebilir. Bu noktada, Yurdakul ve Dalkılıç'ın çalışmasında mevcut sigortaların dijital platformlar üzerinden pazarlanmasının önemine işaret edilmekte ve müşteri ile sigorta şirketlerinin dijital yapı sayesinde aynı çatı altında olacağından bahsedilmektedir.<sup>52</sup> Sigorta şirketlerinin iş ve işlemlerinin dijitalizasyonu şirketlerin müşterileri ile aralarında siber riskler ve siber sigorta açısından çok daha kuvvetli bağların oluşacağı da açıktır.

Beri taraftan, özellikle siber sigortalarda, piyasa aktörlerinin siber risklerin azaltılması konusunda kayda değer bir teklif sunamaması ve somut bir teminat gösterememesi de pazarın en önemli sorunlarından biridir. Bunun nedenin bu çalışmada da birden fazla kez tekrarlanan siber riskin sınırlarının tam olarak bilinmemesi olmakla birlikte, netice itibarıyla müşterilerin güven sorununun çözülememiş olması gerçeğini de değiştirmemektedir. Zira tüketicide, siber riskin gerçekleşmesinin ardından karşılık gelen ödemenin yapılıp yapılmayacağı noktasında endişeler devam etmektedir.<sup>53</sup> Burada ayrıca eklenmelidir ki, müşterilerin güven algısının oluşması bakımından sigorta şirketlerinin öncelikle kendi güvenliğini

---

<sup>51</sup> Detaylı bilgi için bkz: Altuntaş, Kara, Soylu ve Kırkbeşoğlu, "Siber Sigortalar", 9.

<sup>52</sup> Bkz: Yurdakul ve Dalkılıç, "Sigortacılık Sektöründe", 55.

<sup>53</sup> OECD, "Supporting An Effective", 3, 11; Aynı yönde bkz: PWC, "Insurance 2020 & beyond", 10.

sağlaması gerekmektedir. Kendini koruyamayan bir işletmeye, müşterilerinin itimat etmesi beklenemez.<sup>54</sup>

Çalışmanın ikinci kısmında yer alan NFT'lerle de ilişki olması sebebiyle açıklanacak olmasına rağmen yeri gelmişken belirtilebilir ki, blokzincirinin gelişimi ile sahtekarlıkların belirli oranda azalacağı, sorunların çözümünde akıllı sözleşmelerden faydalanılmasının ve merkezi yönetimin doğurduğu risklerin merkezi olmayan yapı sayesinde bertaraf edilmesi ile birlikte tüketicilerin güven sorununun aşılacağı temenni edilmektedir.<sup>55</sup>

#### **IV. SİBER SİGORTANIN BRANŞI VE GENEL ŞARTLARI**

Bazı yazarlarca siber sigortanın genel itibarıyla mesleki sorumluluk sigortası genel şartları hükümlerine tabi olacağı hususu ifade edilmektedir.<sup>56</sup> Ancak yukarıda Tablo.1 ve Tablo.2'de gösterilen ve tek başına siber sigorta poliçesi teklifinde bulunan sigorta şirketlerinin kimilerinin siber sigorta poliçelerini mesleki sorumluluk sigortası genel şartlarına değil de, ferdi kaza sigortası genel şartları veya hırsızlık sigortası genel şartları hükümlerine tabi tuttıkları da görülmüştür. Buradan hareketle sigorta şirketlerinin, sağladıkları teminata ve siber risklerden tercih ettikleri ihlal sebeplerine göre genel şartları seçtikleri söylenebilir. Zira, siber risklerin tamamının gerçekleşmesi halinde hırsızlık veya kaza olayları ile aynı sonucu doğurmadığı da görülmektedir.

Karayazgan'ın da ifade ettiği şekilde, siber sigorta poliçesinde birden fazla çeşit teminat bulunduğundan tek bir branşa veya genel şarta tabi tutulması imkanı bulunmamaktadır.

---

<sup>54</sup> PWC, "Insurance 2020 & beyond", 14.

<sup>55</sup> Görüş hakkında bkz: Tunca ve Sezen, "Sigorta İşlemlerinde Blokzincir", 15-16.

<sup>56</sup> Altuntaş, Kara, Soylu ve Kırkbeşoğlu, "Siber Sigortalar", 12.

Teminatın ilgili olduğu branşa göre bir değerlendirme yapmak gerekecektir. Bu anlamda, zarar (mal veya sorumluluk) sigorta kapsamından uygun düşenine göre bir değerlendirme yapmak gerekecektir. Yazarın da değindiği şekilde genç bir sigorta dalı olan siber sigortanın genel şartlarının düzenlenmesi gerekliliği ortaya çıkmaktadır.<sup>57</sup>

Beri taraftan, siber sigortanın herhangi bir mevzuata tabi tutulmamasının sözleşme serbestisine tabi olduğu da söylenmekte ve bu sebeple ortaya çıkan zarar bakımından değerlendirme yapılabileceği de ifade edilmektedir.<sup>58</sup>

Sorumluluk sigortası hususunun, içerik ve yer sağlayıcıları bakımından halen kabul edilebilir nitelikte olduğu ifade edilmesinde bir beis yoktur. Ancak siber kişiliklerin ortaya çıkması ile birlikte üretilen ve çalışmanın ikinci kısmında yer alan NFT'ler gibi içeriklerin bir eşya olarak kabul edilmesi halinde mal sigortası olarak kabul edilmesi gerektiği de söylenebilir.

Siber sigortanın doğrudan sorumluluk sigortası hükümlerine tabi olduğu her ne kadar açıkça belirtilmemiş ise de Oxera'nın çalışmasında fiyat kıyası açısından Marsh'ın 2015 yılının Mart ayında Birleşik Krallık Hükûmetine sunduğu "UK Cyber Security The Role of Insurance in Managing and Mitigating the Risk" isimli rapordan yaptığı alıntıda genel

---

<sup>57</sup> Karayazgan, "Sigorta Sektöründe", 41-44.

<sup>58</sup> Mahmut Barlas, "Türk Hukukunda Siber Sigorta", Fintechtime, Erişim Tarihi: 24 Mayıs 2021. <https://fintechtime.com/tr/2020/09/turk-hukukunda-siber-sigorta/>; Karayazgan da mesleki sorumluluk sigortası genel şartlarına tabi olduğunu ancak bunun zorlama bir yorum olduğunu belirtmekte, siber sigortanın kendine özgü bir genel şartlara ihtiyaç duyduğunun altını çizmektedir. Bkz: Ahmet Karayazgan, "Hukuki Yönüyle Siber Sigorta ve Sessiz Siber Teminatının Çalışma Esasları", iç. *Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Makalelerim Işığında)*, İstanbul: Legal Yayıncılık, 2020, 139-141.



sorumluluk sigortası fiyatları ile siber sigortanın fiyatlarının artışına dair grafiği paylaştığı görülmektedir.<sup>59</sup> Yalnızca buradan hareketle Oxera'nın siber sigortaya en yakın branş olarak genel sorumluluk sigortasını gördüğü düşünülebilir. Zira, Marsh'ın anılan çalışmasında, kıyas yapılan tabloda mülkiyet sigortasına da yer verdiği de görülmektedir.<sup>60</sup> Böylece Oxera'nın çalışmasından hareketle siber sigortanın mal sigortası içeriğinde tasnif edilmemesi gerektiği kanaatine varılabilir.

Siber sigortanın ayrı bir poliçe olarak sunulması dışında, geleneksel sigortaların ana teminat ve ek teminatları olarak da düzenlenmesinin mümkün olduğu ifade edilmektedir.<sup>61</sup> Bu haliyle, kendisine mahsus genel şartları olmadığından diğer branştaki sigortaların alanına gireceği de ifade edilebilir. Nitekim, Tablo.1 ve Tablo.2'de çeşitli isimlerle siber sigorta teklifinde bulunan sigorta şirketlerinin yaptığıının da esasen bu husus olduğu görülmektedir. Ancak bu şekilde, teminat altında olmadığı açıkça ifade edilmeyen hususların da teminat kapsamında sayılacağı 03 Haziran 2007 tarihli ve 5684 sayılı Sigortacılık Kanunu'nun 11'inci maddesinin dördüncü fıkrasında yer alan temel kuralı<sup>62</sup> karşısında sigorta şirketlerinin aleyhine bir kapsam kazanacaktır. Bu sebeple, siber sigorta konusunda genel şartların hazırlanması ihtiyacına yönelik düşünce ifade edilmiştir.<sup>63</sup>

---

<sup>59</sup> Oxera, "The value of cyber insurance", 10.

<sup>60</sup> Marsh ve Birleşik Krallık Hükûmeti, UK Cyber Security The Role of Insurance in Managing and Mitigating the Risk, 22.

<sup>61</sup> OECD, "Supporting An Effective", 5.

<sup>62</sup> RG. 14.06.2007, S.26652. "(4) Sigorta sözleşmelerinde kapsam dahiline alınmış olan riskler haricinde, kapsam dışı bırakılmış riskler açıkça belirtilir. Belirtilmemiş olan riskler teminat kapsamında sayılır."

<sup>63</sup> Karayazgan, "Sigorta Sektöründe", 42-44.

Ancak yalnızca genel şartın hazırlanması da yeterli olmayacaktır. Gelişen teknolojilere uygun olarak siber varlıkların karşılaştığı risklere karşı özellikle teminat tutarı ve kapsamının belirlenmesi hususunda düzenleme yapılması zarureti de ortaya çıkmaktadır. Konuya ilişkin, yapılan araştırmalar da kamunun siber sigorta konusunda özel sektör temsilcileri ile fikir teatisine girilmesi ve buyurucu hükümler ile konu hakkında regülasyona gidilmesi noktasında taleplerin bulunduğunu göstermektedir.<sup>64</sup>

## V. SİBER SİGORTANIN REASÜRANSI

Siber sigortanın gelişiminden daha yavaş olan bir alan siber sigortanın reasüransı meselesidir. Daha önceden de bahsedildiği şekilde, riskin büyüklüğü ve belirsizliği karşısında sektörün ilerlemesindeki yavaşlık reasürans işlemlerinin yaygınlaşabilmesi açısından daha da yavaş olmaktadır.<sup>65</sup> Ancak siber sigortadaki gelişimle birlikte artışın devam ettiği de görülmektedir.

Oxera'nın çalışmasında brokerlere daha fazla rol düştüğü de ifade edilmektedir. Nitekim, siber sigorta kullanıcılarının genel brokerlerden ziyade bu alana mahsus olarak görev üstlenen "siber brokerleri" tercih ettiği de belirtilmiştir.<sup>66</sup>

Türkiye'de faaliyet gösteren reasürans şirketlerinden gerek Milli Reasürans T.A.Ş.'nin ve gerek Türk Reasürans A.Ş.'nin 2020 yılı faaliyet raporlarında pandemi koşullarının oluşturduğu dijitale yönelimin siber riski çok ciddi bir şekilde artırdığından bahisle, neredeyse tüm branşlara ilişkin reasürans anlaşmalarında siber risklerin istisnai kloz olarak eklendiği

---

<sup>64</sup> Marsh ve TÜSİAD, "Araştırma", 3.

<sup>65</sup> PWC, "Insurance 2020 & beyond", 13.

<sup>66</sup> Oxera, "The value of cyber insurance", 11.

belirtilmektedir.<sup>67</sup> Söz konusu raporlarda şirketlerin siber sigortaya yönelik reasürans işlemlerine dair bilgi verilmemektedir. Ancak, siber riskin tolere edilmesi için artan siber sigorta ihtiyacı ve bunun riskinin reasüre edilmesine yönelik talepler karşısında bu şirketlerin de harekete geçeceği beklenmektedir.

## VI. SİBER GÜVENLİĞİN KAMUSAL YÖNÜ VE SİBER SİGORTAYA YÖNELİK MEVZUAT İHTİYACI

Siber güvenliğin her ne kadar işletmeleri ilgilendiren bir yönü bulunduğu düşünülse de en büyük piyasa aktörünün çoğu konuda devlet olduğu düşünüldüğünde ve serbest piyasa ekonomisinin hâkim olduğu ülkelerde dahi kriz anında devletin müdahale zorunluluğunun kaçınılmazlığı ortadadır. Hangi tür ekonomik politikalar benimsenmiş olursa olsun, piyasa regülasyonu konusunda kamu tarafına açık bir yükümlülük düşmektedir.

Çalışmanın ilk kısmında da belirtildiği üzere, siber güvenliği tehdit eden risklerin henüz standartlaştırılması ve daha keskin bir ifade ile siber riskin sınırlarının belirlenmesi mümkün olmadığından siber sigortanın gelişimi yavaş kalmaktadır.<sup>68</sup> Bu noktada, devletlerin piyasaya kural koyucu olarak müdahalesinin kaçınılmazlığı ortaya çıkmaktadır.

### A. Türkiye’de Siber Tehdide İlişkin Çalışmalar

Siber tehditlere karşı kamu tarafında alınacak önlem ve uygulamalara ilişkin 29 Aralık 2020 tarihli ve 31349 sayılı Resmi Gazete’de 2020/15 sayılı Cumhurbaşkanlığı Genelgesi

---

<sup>67</sup> Türk Reasürans A.Ş. 2020 Faaliyet Raporu, 39; Milli Reasürans T.A.Ş. 2020 Faaliyet Raporu, 52.

<sup>68</sup> Bara, Ćorić ve Jurišić, "The role of the Cyber Insurance", 40.

yayımlanmıştır. Genelge ile Ulaştırma ve Altyapı Bakanlığı koordinasyonunda hazırlanan ve ilk defa 2013 yılından itibaren politika metni haline gelen Ulusal Siber Güvenlik Stratejisi ve Eylem Planı da bu defa 2020 ilâ 2023 yılları arasında uygulanmak üzere resmîyet kazanmıştır.

Siber suçlarla mücadele, bilişim teknolojilerinin entegrasyonu, yeni nesil ağlar ve yerli teknolojilerin geliştirilmesi ve desteklenmesi gibi 8 ana başlıkta toplanan söz konusu strateji ve eylem planı metninde siber güvenliğe ilişkin de önlemlere yer verildiği görülmektedir.

Her ne kadar anılan eylem planında doğrudan siber sigortacılıktan bahsedilmemişse de risk yönetimi ve siber risk kavramlarına değinilerek siber risklerin getirdiği zararların önlenmesi ve giderilmesi amacıyla alınacak tedbirlerden bahsedildiği görülmektedir. İlkesel açıdan da siber güvenliğin güçlü hukuki temeller üzerine inşa edilmesinin amaçlandığı da belirtilerek bir kez daha bu alanda hukukçulara düşen görevin de altı çizilmiştir.<sup>69</sup>

Yine Eylem Planı çerçevesinde siber güvenliği sağlamaya katılacak her paydaşın temel hedefinin “siber tehditlerin, risklerin ve bunların etkilerinin en aza indirgenmesi”<sup>70</sup> hususundan bahsedilmesi de siber tehditlerle ortaya çıkan zararların giderilmesi veya en aza indirilmesi hususunda sigorta sektöründe yer alan paydaşların sorumluluğuna da işaret etmektedir.

---

<sup>69</sup> Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)*, 19.

<sup>70</sup> Ulaştırma ve Altyapı Bakanlığı, “Eylem Planı”, 20.

Siber vatan<sup>71</sup> olarak da ifade edilen kavramın eylem planında siber uzay olarak ifade edildiği görülmektedir.<sup>72</sup> Türk devleti yurttaşlarının özgür ve güvenli bir şekilde siber varlıklarını korumaları ve geliştirmelerini temin etmek amacıyla internet ortamında devletin siber egemenlik hakkı<sup>73</sup> olduğu ve bu hakkın sonuçları bakımından da gerekli önlemlerin alınması gerekliliği ortaya çıkmaktadır.<sup>74</sup>

06 Temmuz 2019 tarihli ve 30823 sayılı Resmi Gazete’de yayımlanan 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri ilan edilmişse de bu önlemlerin siber güvenliği sağlamaya yönelik olduğu ve ancak tazmine yönelik hükümler içermediği görülmektedir.

---

<sup>71</sup> Özgür Altuncu, “Siber vatan savunması,” *Hürriyet*, erişim tarihi: Mayıs 28, 2021, <https://www.hurriyet.com.tr/gundem/siber-vatan-savunmasi-41716074>; Söz konusu haberdan de görüleceği üzere ve Cumhurbaşkanlığı düzeyinde ifade edilen şekliyle, “siber vatan” egemenlik sınırlarının içinde tutulacaktır. “Uzay vatan”, kavramıyla birlikte yakın gelecekteki iki önemli başlıktan biri olacağı düşünülmektedir.

<sup>72</sup> Siber uzay kavramı, Varşova Zirvesi’nde NATO tarafından tanınmıştır ve gerek NATO üye ülkeleri ve gerek Avrasya tarafında yer alan ülkelerin bu konuda önlem olarak “siber ordular” yarattığı görülmektedir. Bkz: Cebeci, “Türkiye’de Siber Risk,” 164.

<sup>73</sup> Siber egemenlik hakkı kavram ilk kez 2014 yılında Çin’in Ciciang eyaletinde gerçekleştirilen Dünya İnternet Konferans’ında Çin Halk Cumhuriyeti devlet başkanı Şi Cinping tarafından dile getirilmiştir.

<sup>74</sup> Siber egemenlik kavram için, “Devletlerin, uyruklarını siber dünyadaki risklerden ve tehditlerden korumak adına tek taraflı tasarrufta bulunabilmeleri gücüne sahip olmalarıdır.” şeklinde bir tanım önerilebilir. Her ne kadar Türkiye’de bu kavramdan yaygın şekilde bahsedilmemekte ve egemenlik kavramının önemine zarar verdiği iddia edilmekte ise de dünya çapında yalnızca Çin tarafından değil, Fransa başta olmak üzere Avrupa ülkelerince de ciddi çalışmalar yapılmaktadır. Ancak bu çalışmalar siber egemenlikten öte üçüncü dünya ülkeleri üzerinde başlatılan siber sömürgecilik faaliyeti olarak görülerek eleştirilmektedir.

Bu vesile ile bireylerin siber riskler konusundaki farkındalıkları ile özellikle finansal okuryazarlık ve bilişim okuryazarlığı konularındaki birikimlerinin önem arz ettiğini de belirtmek gerekmektedir.<sup>75</sup> Bu noktada, görsel ve işitsel medyadan yararlanmak suretiyle bu konuda daha fazla çalışma yapılması önem taşımaktadır. Nitekim çalışmanın önceki bölümünde de belirtildiği üzere, siber saldırıların %40'ından fazlası kullanıcı hatası veya bilinçsizliğinden faydalanılması sayesinde ortaya çıkmaktadır. Siber egemenlik hakkını kullanan bir devletin de milletin eğitimi siber dünyadaki çıkarları koruyacak şekilde öncelik vermesi bu gibi risklerin azaltılmasını sağlayacaktır.

## B. Dijitalleşme Yolunda Mevzuat Adımları

Siber sigorta kavramının önemli bir ayağını teşkil eden kısmın dijital hizmetlerle ilgili olduğu açıktır. Dijital hizmetlere ilişkin olarak, 07 Aralık 2019 tarihli ve 30971 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 05 Aralık 2019 tarihli ve 7194 sayılı Dijital Hizmet Vergisi İle Bazı Kanunlarda Ve 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun ile birlikte Türk hukukunda dijital verginin yer almaya başlaması, dijital ortamda sunulan hizmetlerin vergiye

---

<sup>75</sup> Marsh'ın TÜSİAD için hazırladığı çalışmasında yer alan veriler ışığında 2019 yılında %22 olarak ölçülen dünya çapındaki farkındalığın, 2020 yılındaki araştırmaya göre Türkiye'de %9 olarak ölçülmesi örnek olarak gösterilebilir. Detaylı bilgi için bkz: Marsh ve TÜSİAD, 2020 Türkiye Siber Risk Algı Araştırması, 2. Ömürbek ve Altın'ın çalışmasında da ifade edildiği üzere, halkımızda ciddi bir kadercilik anlayışı hakimdir. Bkz: Nuri Ömürbek ve Fatma Gül Altın, "Sigortacılık Sektöründe Bilgi Teknolojilerinin Uygulanmasına İlişkin Bir Araştırma," *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 13, no. 3 (2008): 108. Ancak çizilen kötü manzaraya rağmen, sanal platformların günlük hayatın bir miktar daha dışında kalması ile, klasik yaklaşımların ve kaderci anlayışın bu alanda yaygın olmayacağı, bilgi ve tecrübe ile diğer alanlara kıyasen siber sigorta alanında gelişimin çok daha hızlı olacağı öngörülebilir.

tabi bir kazanç olduğunu yasal dayanak altına almıştır. O halde, vergilendirme tabi bir kazanç getiren faaliyetin varlığının doğası gereği riskler de barındırdığı ve sigorta teminatı altına alınabilmesi gerektiği de düşünülebilir. Hatta, siber sigorta poliçelerine yapılan ödemelerin vergiden düşürülmesi gibi teşviklerle bu iki alanın birbirini besler şekilde gelişimine imkân tanınabilir.

20 Mayıs 2021 tarihli ve 7319 sayılı Sigortacılık İle Diğer Bazı Alanlara İlişkin Kanunlarda Ve Bir Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun'un 12'nci maddesi ile 03 Haziran 2007 tarihli ve 5684 sayılı Sigortacılık Kanunu'nun 33/A maddesinde yapılan değişiklik ile kurulan Özel Riskler Yönetim Merkezi'nin sigorta veya reasürans teminatı altında olmayan ancak sigorta edilmesinde kamu yararı görülen risklerin yönetimi ve yürütülmesi yetkisi tanınmıştır. Bu kapsamda söz konusu merkezin siber riskin kamu menfaatini ilgilendiren bir tehdide dönüşmesi halinde kanundaki hükümler uyarınca siber sigorta teminatlarına yönelik çalışmada bulunabileceği düşünülebilir. En azından yürürlükteki mevzuat açısından bunun önünde bir engel gözükmemektedir.

Bu aşamada, siber sigortaya ilişkin meselelerde mevzuat çalışmalarının yapılarak sınırının çizilmesi, genel şartları ve siber sigortaya ilişkin standartların belirlenmesinin uygulama kolaylığı sağlayacağı hususu bir kez daha dikkat çekmektedir.

### **C. Standardizasyona Yönelik Çalışmalar**

Siber sigortanın birden çok kez ifade edildiği üzere karşılaştığı en önemli sorun siber risklerin çeşitliliği, poliçenin kapsama noktaları ve riskin ortaya çıkmasından öncesi ve sonrası için yapılan çalışmaların belli ve programlı olmasının zorluğudur.

OECD'nin bu zorlukların önüne geçilmesi için üye devletlerden beklentisi hükümetlerce yapılacak çalışmalar ile siber sigorta pazarının önünde duran engellerin kaldırılması ve

sektörün gelişimi için uygun mevzuat ve fırsat beklentilerinin yaratılmasıdır. Bunun önemli bir ayağı olarak, risklerin belirlenmesinde standardizasyon ve güvenlik politikalarının oluşturulması gelmektedir. Ayrıca, sektörle kamu arasında oluşturulacak bir ağ ile siber tehditlerle, vuku bulan siber risklere ilişkin yapılan ödeme taleplerine ilişkin istatistiksel bilgilerin hükûmetlere sunulması konusunda teşvik veya zorunluluk getirilmesi de eklenmektedir.<sup>76</sup>

OECD'nin bu yaklaşımına emsal nitelik gösteren bir uygulama Birleşik Krallık Hükûmetinden gelmiştir. 2014 yılından beri uygulamaya konulan "Siber Esaslar" isimli 10 adımdan oluşan siber güvenlik uygulaması önem taşımaktadır. Hükûmetin bu yaklaşımı ile, siber riskin belirsizliğinin ortadan kaldırılması amaçlanmaktadır. Esasların dikkat çeken yanının ise tüm büyüklükten işletmelerin uygulayabileceği temel önlemlerden ibaret olmasıdır.<sup>77</sup>

Benzer şekilde Amerika Birleşik Devletleri'nde de *Cybersecurity and Infrastructure Security Agency* - CISA (Siber Güvenlik ve Teknik Altyapı Güvenliği Ajansı) isimli kurumun 2018 yılında İç Güvenlik Bakanlığına bağlı bir müsteşarlık statüsünden çıkarılıp da müstakil bir federal ajans haline gelmesini takiben 2019 yılının Kasım ayında yayımladığı rehber ile yine işletmelere yönelik "Siber Esaslar" yayımlanmış ve 6 temel adımda işletmelerin siber güvenliklerini artırmaya yönelik ilkeler uygulamaya geçilmiştir.

Gerek Birleşik Krallıktaki ve gerek ise Birleşik Devletler'deki bu uygulamalar gözetilerek Türkiye'nin de "siber usul ve esasları" ortaya koyması ve Amerikan kurumuna benzer şekilde Türkiye'deki Siber Güvenlik Kurulu'nun, Türkiye Ulusal Siber Güvenlik Ajansına dönüştürülmesinin fayda

---

<sup>76</sup> OECD, "Supporting An Effective", 11-12; Aynı yönde bkz: PWC, "Insurance 2020 & beyond", 5.

<sup>77</sup> Bara, Ćorić ve Jurišić, "The role of the Cyber Insurance", 40.



sağlayabileceği görülmektedir. Böylelikle, alanında uzmanlaşmış bir otorite ile regülatif faaliyetlerin daha hızlı hayata geçişi beklenebilecektir.

#### **D. Kişisel Verilerin Korunması Kanunlarının Etkisi**

Amerika'daki siber sigorta piyasanın tarihsel süreç içerisinde her zaman Avrupa piyasasından ileride olduğu gözükmemektedir. Bunun en önemli nedeninin kişisel verileri korumaya ilişkin düzenlemelerin Amerika'da çok daha önceden başlaması gösterilmektedir. Öyle ki, Kaliforniya'da 2002 yılında hazırlanan ve 2003 yılında çıkan verilerin korunmasına ilişkin kanunun 2005 ve 2016 yılları arasında tüm eyaletlerde yayıldığı görülmekte iken, Avrupa'da ise *General Data Protection Regulation*'a (Genel Veri Koruma Tüzüğüne) ilişkin çalışmaların 2012 yılında başladığı ve ancak 2018 yılında yürürlük kazandığı görülmektedir.<sup>78</sup>

Türkiye'de de benzer şekilde 2010'lu yılların ikinci yarısına doğru kişisel verilere ilişkin çalışmalar hız kazanmış ve 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kabulü ile kanuni zemini oturmuştur. Ancak 2020'li yıllara gelinmesine rağmen veri siciline kayıtların uzatılması sebebiyle Kanun tüm çerçevesiyle uygulanmasının halen tam olarak başlamadığı da görülmektedir. Bu noktada, VERBİS kayıtlarının tamamlanmasına müteakiben siber sigortanın da Türkiye sahilinde de önem kazanacağı tahmin edilebilir.

Buradaki açıklamalara ek olarak, bilişim teknolojilerindeki gelişmelerin Amerika'da öncelikli olarak ilerlemesi ve Avrupa'nın yakın tarihsel süreçte bilişim alanında daha çok ileride olan değil de takip eden statüde oluşunun siber sigortanın gelişimi açısından etkili olduğunu ifade etmek

---

<sup>78</sup> Oxera, "The value of cyber insurance", 5-6.

mümkündür. Ancak her halükarda kaçınılmaz olan teknolojik gelişmelerin getirdiği *modern sorunlar modern çözümler gerektirir*.<sup>79</sup>

## VII. SİBER SİGORTA ZORUNLULUĞU HAKKINDA

Yaygın olarak tahmin edildiği şekilde, büyüklüğü fark etmeksizin çoğu işletme sahiplerince siber saldırılara maruz kalma riski altında oldukları bilinmemektedir. Üstelik gelecekte de böyle bir riskin artarak devam ettiği ve hatta belki de siber saldırıya çoktan uğramış olduklarından bihaber oldukları da düşünülmektedir.<sup>80</sup>

İşletmelerin yüksek risk altında olmalarının bertaraf edilmesi maksadıyla, siber sigortanın kanuni çerçevesinin çizildikten sonra küçük ve orta büyüklükteki işletmeler için zorunlu hale getirilmesi hususu düşünülmekte ve bu yönde talepler ortaya çıkmaktadır.<sup>81</sup> Ancak bu talebin yalnızca KOBİ'lere yönelik olması üzerine düşünmeyi gerektirmektedir.

Siber sigortanın, siber tehditlerle ortaya çıkan zararın giderilmesine yönelik teminatlar getirdiği ve bu sigortanın kendi

---

<sup>79</sup> "Modern problems require modern solutions" sözü aslında Amerikan komedyen Dave Chappelle'nin Chappelle's Show dizisinde geçmişse de internet ortamında "mim" haline gelerek yaygınlaşmıştır. Çalışma özelinde ifade edilebilir ki, yakın gelecekte buna benzer bir içeriğin NFT haline getirilmesi ihtimal dahilindedir.

<sup>80</sup> OECD, "Supporting An Effective", 3; Siber riskin gerçekleşmesi halinde aylarca ve hatta yıllarca tespit edilememesi ve bu süreç içerisinde kayıpların katlanması gibi riskler bulunmaktadır. Bkz: PWC, "Insurance 2020 & beyond", 9.

<sup>81</sup> Habertürk, "Siber güvenlik sigortası KOBİ'ler için zorunlu olmalı," erişim tarihi: Mayıs 24, 2021 <https://www.haberturk.com/siber-guvenlik-sigortasi-kobi-ler-icin-zorunlu-olmali-3023980-ekonomi>.

başına siber saldırıları engelleyemeyeceği hususu unutulmamalı ve işletmelerce siber güvenlik önlemleri muhakkak alınmalıdır.<sup>82</sup>

Zaten günümüz dünyasının geldiği nokta itibarıyla, önleyici hizmetlere ilişkin proaktif çalışmaların, zararın ortaya çıktıktan sonra giderilmesine yönelik geleneksel sürecin yerini yavaş yavaş almaya başladığı da gözlemlenmektedir.<sup>83</sup> Buna göre sigorta şirketleri, bilincin artırılması, risk ölçümlerinde ve tespit edilen risklerin azaltılması noktalarında müşterilerini cesaretlendirme ve teşvik etme şeklinde üç temel şekilde önleyici hizmetler sunabileceklerdir.<sup>84</sup> Ancak siber dayanıklılığın oluşması için tek rol yalnızca sigorta şirketlerine ve hükûmetlere düşmemektedir. Teknolojinin gelişimiyle birlikte, kişiler ve kültürel yaklaşımların da buna uygun olarak şekillenmesi ve bütüncül bir yapı ile risklere karşı mücadelede bulunması gerekmektedir.<sup>85</sup>

Öyle ki, siber tehditlerden kaynaklanabilecek risklerin ölçülmesi, karşılaşılabilecek muhtemel zararların önceden simule edilerek tespitinin yapılmaya çalışılması ve buna yönelik hazırlıkların tamamlanması önem arz etmektedir. Tehditlere karşı, olabilecek en kısa sürede güvenliğin sağlanmasına yönelik çalışmalar yapılması ve siber güvenlik şirketleri ile bu konuda iş birliğine gidilmesi gerekecektir. Sigorta şirketlerinin de müşterilerinin de bu ve benzeri sorumlulukları gerek iç

---

<sup>82</sup> Şekeroğlu ve Özüdoğru, "Dijital Dönemin Koruyucuları", 62; Aynı yönde: Çotak, "Sigortacılık Sektöründe", 66; Siber sigorta teminatı altına alınacak işletmeler açısından siber güvenlik önlemlerine ve risk yönetim politikalarına sahip olunması bir zorunluluk olarak da telakki edilmektedir. Bu husus hakkında bkz: Altuntaş, Kara, Soylu ve Kırkbeşoğlu, "Siber Sigortalar", 20.

<sup>83</sup> Bara, Ćorić ve Jurišić, "The role of the Cyber Insurance", 42; Aynı yönde bkz: Bul, "Sigorta Dağıtım Kanallarının Dijitalizasyonu", 5.

<sup>84</sup> OECD, "Supporting An Effective": 3.

<sup>85</sup> PWC, "Insurance 2020 & beyond", 5.

regülasyon yönünden ve gerek düzenli takibatı yönünden kontrollerinin eksiksiz yapılması ve tarafların birbirinin bilgilerini güncel tutması da yine risklerin azaltılması bakımından önemlidir.

Siber tehditlerin verinin kendisine yönelik olması sebebiyle, ilk bakışta işletme büyüklüğünün siber saldırılar açısından bir öneminin olmadığı düşünülmektedir. Ancak, küçük işletmelerin çevrimiçi hizmetler ve bulut servislerinin kullanımında büyük şirketlere kıyasen daha zayıf güvenlik tedbirlerinin aldığı ise genel olarak söylenebilir. Beri taraftan, KOBİ'lerdeki bu güvenlik zafiyetinin iş ortaklıkları kurdukları büyük şirketlerin verilerini de tehdit ettiği belirtilmelidir.<sup>86</sup> Tersine bir yorum ile Oxera'nın ifade ettiği şekilde, orman yangınlarının durdurulmasında olduğu gibi siber sigorta bilincinin artırılmasında diğer şirketlerin de dışsal yararı ortaya çıkacaktır. Nitekim, bir işletme kendini bu şekilde korumaya aldığı anda diğer işletme de bu korumadan yararlanmış olacaktır.<sup>87</sup>

KOBİ'lerle büyük şirketlerin siber sigortaya olan ilgisi kıyaslandığında elde edilen bir sonuç dikkat çekicidir: Büyük şirketlerin siber güvenliğe yaptığı yatırım KOBİ'lere kıyasen iki kattan daha fazla iken, siber saldırıların vuku bulması halinde KOBİ'lerin yaptığı harcama ise büyük şirketlere kıyasen beş kat daha fazla olmaktadır.<sup>88</sup> Siber sigortanın ve siber güvenlik politikalarının önemini göstermeye tek başına bu veri delil olabilecektir.

Her ne kadar KOBİ'lerin siber risklere karşı yeterli önlemleri almadığı ve farkındalığın düşük olduğu ifade edilmişse de<sup>89</sup>

---

<sup>86</sup> Bara, Čorić ve Jurišić, "The role of the Cyber Insurance", 37.

<sup>87</sup> Oxera, "The value of cyber insurance", 14.

<sup>88</sup> Oxera, "The value of cyber insurance", 4.

<sup>89</sup> Cebeci, "Türkiye'de Siber Risk", 166.

gerek ülkemizde ve gerek dünya çapında milyonlarca kullanıcısı olan şirketlerin veya sosyal medya paylaşım sitelerinin dahi siber saldırıların hedefi olduğu ortaya çıkmıştır. Beri taraftan, PWC tarafından 2013 ve 2014 yılları arasında yapılan araştırma, şirketin büyüklüğü arttıkça benzer şekilde şirketlere yapılan saldırıların giderilmesi için gereken harcamanın da arttığını göstermektedir.<sup>90</sup>

Bu denli büyük şirketlerin KOBİ'lere kıyasen çok daha fazla kişinin verilerini barındırdığı ve saldırılardan daha fazla etkilenebilecekleri düşünüldüğünde bu sigortanın yalnızca KOBİ'ler açısından zorunlu hale getirilmesinin ise nihayetinde haksızlık yaratacağı ve eşitlik ilkesine aykırı olacağı düşünülmelidir.

Siber varlığı ve siber risklere açık hizmetleri bulunan işletmelerin büyüklüğüne bakılmaksızın siber sigortanın zorunlu hale getirilmesi ise daha isabetli olabilecektir. Bu aşamada, teminat ve prim miktarlarının farklı tutarlarda öngörülmesi ve işletmelerin büyüklüğü ile güvenlik tedbirlerine uyumlu bir şekilde belirlenmesi gerekliliği ise tartışmasıdır. Sonuç olarak, riskin büyüklüğü yalnızca şirketin büyüklüğü ile ölçülemez. Şirketin büyüklüğüne ek olarak siber güvenlik önlemlerinin bir arada değerlendirilmesi sonucunda mümkün olduğu kadar yaklaşık risk tespitinin yapılması gerekmektedir. Bunun ardından, maktu fiyat politikasından ziyade, kişiselleştirilmiş fiyat tekliflerinin sunulması ve buna uygun prim toplanması gerekmektedir.

Çalışmanın önceki bölümünde belirtilen Birleşik Krallık Hükûmetinin 10 maddelik Siber Esaslar politikasında yer alan önlemlerin orta ve büyük işletmeler açısından %90'ları aşan şekilde uygunluk sağlanmasına kıyasen mikro ve küçük

---

<sup>90</sup> PWC, "Insurance 2020 & beyond", 8.

işletmelerde ise bu oran %50'lere kadar düştüğü görülmektedir.<sup>91</sup> Türkiye gibi Birleşik Krallık'ta da ticari hayatın %99'unun KOBİ'lerden oluştuğu düşünüldüğünde<sup>92</sup> siber sigortanın KOBİ'ler açısından halen istenen noktada olmadığı da dikkat çekicidir.

### VIII. NFT (NON-FUNGIBLE TOKEN)

Blokzinciri ve kriptopara teknolojisindeki gelişmelerle birlikte NFT'ler (Non-Fungible Token) ile üretilen sanat eserleri gündeme gelmiş durumdadır. "Değiştirilemez Jeton"<sup>93</sup> olarak adlandırılacak NFT'ler blokzincirinde yer alan harf ve rakamlarla şifrelenen emsalsiz ve biri diğerinin yerine geçemeyecek jetonlardır. Çalışmanın ilham kaynağı da bu jetonlarla üretilen sanat eseri gibi çeşitli içeriklerin sigortalanması imkânı hakkında düşündürmektir.

### IX. BLOKZİNCİRİ VE JETONLAR

Değiştirilemez jetonları anlayabilmek için öncelikle kabaca blokzinciri yapısının anlaşılması gerekmektedir. Blokzinciri, bir kayıt zinciri olarak düşünülebilir. Bu zincirler blok halinde birbirine bağlanarak büyüyen bir yapı oluşturur. Her blokta da şifreleme, zaman damgası ve işlem verileri bulunmaktadır. Kayıtların oluşması için sistemde bulunan tüm üyelerin doğrulama yapması gerekmektedir. Bu sebepten dolayı, kayıt listesini içerir veri yani blokzinciri uçtan uca şifreli hale gelerek

---

<sup>91</sup> Oxera, "The value of cyber insurance", 14.

<sup>92</sup> Oxera, "The value of cyber insurance", 14. Çatuk, "Siber Riskler Karşısında KOBİ'lerin Bilgi Güvenliği", 13.

<sup>93</sup> NFT'lerin Türkçeleştirilmesi açısından "değişmez im" anlamına gelecek şekilde "DİM" kısaltması kullanılabilir. Ancak TDK'nın bu aşamada henüz bir tercihi olmadığı görüldüğünden çalışma boyunca NFT ibaresinin kullanılması tercih edilmiştir.

merkezi olmayacak şekilde, sistemdeki tüm üyelerin bilgisayarlarında birer kopya oluşturur. Merkezi olmayan bu blokzinciri de belirli kişi veya grupların yönetimi altında kalmaz.<sup>94</sup>

Blokzincirinin en önemli avantajı, sonraki blokun kendinden önce gelen bloka bağlanması ve bu zincirin diğer kullanıcılar tarafından da görüldüğü için saldırganlarca sıralarının değiştirilemiyor oluşudur. İlaveten, tarih ve zaman damgası içerdiği için de olası herhangi bir değişiklik teşebbüsünde bunun bariz olması sonucunu doğuracaktır.<sup>95</sup>

### A. Sigorta Sektöründe Blokzinciri

Blokzincirinin oluşumu ile birlikte halihazırda zaten sigortacılık girişimlerinin azımsanmayacak bir ölçüde bu yapıya intibak etmeye başladığı söylenebilir. Öyle ki, *McKinsey*'in veri tabanına kayıtlı girişimlerin %10'unun sigorta sektörüne ilişkin olduğu not edilmiştir.<sup>96</sup>

Çalışma özelinde blokzincirinden NFT'ler oluşturulması ve bu ürünler üzerinde sigorta teminatlarına ilişkin bir inceleme söz konusu ise de, blokzincirinin diğer sigorta teminatları açısından da kullanılabilir olduğu belirtilebilir. Blokzincirinin maliyet avantajı sağlaması, güvenilir altyapı olanağı ve tazminat

---

<sup>94</sup> Tunca ve Sezen, "Sigorta İşlemlerinde Blokzincir", 14-16.

<sup>95</sup> Mahir Çipil, "'Blockchain' sigortacılığı nasıl etkileyecek?", *Dünya*, Erişim Tarihi: 31 Temmuz 2021. <https://www.dunya.com/kose-yazisi/blockchain-sigortaciligi-nasil-etkileyecek/344612>.

<sup>96</sup> Çipil, "'Blockchain' sigortacılığı nasıl etkileyecek?".

süreçlerinin hızlandırması gibi etkenlerle farklı şekillerde kullanıma konu edilebileceği ifade edilmektedir.<sup>97</sup>

Sayılan avantajlara yeni talep esnekliği, daha fazla kişiye ulaşma kolaylığı ve akıllı sözleşmelerin getireceği yeni modeller de eklenebilir. Özellikle akıllı sözleşmelerin piyasayı değiştireceği beklenmektedir. Ancak blokzinciri teknolojisine ilişkin tecrübelerin, deneyimsel olarak ilerlemesi hataların ortaya çıkması ve giderilmesi zaman aralığında dahi ciddi ekonomik zararlara sebep olabileceği kaçırılmamalıdır. Yakın gelecekte ise, blokzincirinin dijital iletişimin olduğu her yerde içerik üreticisi ve içeriği koruyucu olarak bulunması ihtimali de düşünülmektedir.<sup>98</sup>

Akıllı sözleşmeler açısından ayrıca, teminatın doğrulanması ve lehtarların sunduğu taleplerin teminat bilgileri ışığında karara bağlanması gibi süreçlerin de ayrıca doğrulama gerekmeksizin çözümleneceği düşünülmektedir. Yine ayrıca, akıllı sözleşmelerin portföy çeşitliliğini artırarak kişiselleştirilmiş hizmet deneyimi sunması konusunda avantaj sağlayacağı da beklenmektedir.<sup>99</sup>

Sigorta şirketlerinin bilişim altyapılarına bağımlı halde çalışmalarının siber risk açısından ciddi bir hedef olma ve

---

<sup>97</sup> Bu konu hakkında bkz: Duygu Kule, “Dijital Sigortacılıkta Hizmet Kalitesi”, (Yayımlanmamış yüksek lisans tezi, Kütahya Dumlupınar Üniversitesi, 2019), 18.

<sup>98</sup> Detaylı bilgi için bkz: İsmail Yıldırım, Eyyüp Ensari Şahin, “Insurance Technologies (Insurtech): Blockchain and Its Possible Impact on Turkish Insurance Sector”, *Journal of International Management, Education and Economics Perspectives* 6, no. 3, (2018): 18-21.

<sup>99</sup> Detaylı bilgi için bkz: Tunca ve Sezen, “Sigorta İşlemlerinde Blokzincir”, 18-19; Yeni ekonomik yapılar ile birlikte müşterilerin en iyi fiyat teklifinden ziyade kişiselleştirilmiş hizmet deneyimini önemsediklerine yönelik bir diğer görüş hakkında bkz: Sezal, “Türk Sigortacılık Sektöründe”, 135.



savunma zorluğu durumu yarattığı belirtilmektedir.<sup>100</sup> Ancak blokzincirindeki gelişmelerle bu durumun aşılacağı öngörülmektedir. Nitekim blokzincirinin değiştirilemez ve yok edilemez yapısı sayesinde veritabanları üzerindeki korumanın arttığı gözükmemektedir.<sup>101</sup> Açık kaynak kodu ile birden fazla yerde depolanarak merkeziyetçi yapıdan kurtulan bu sistem ile siber tehditlerin tek bir merkezi ele geçirilerek ciddi bir risk arz ettiği dönemler kapanabilecektir.

## B. Değiştirilebilir ve Değiştirilemez Jetonlar

NFT'yi anlamak için ayrıca değinilmesi gereken nokta, jetonların değişebilir niteliğinin ne olduğu hususudur. NFT'nin blokzincirinin altyapısını kullanmasına rağmen değiştirilemez içeriği diğer kripto varlıklardan ayrılması sonucunu doğurmaktadır. Buna göre, NFT'lerin biri diğeri ile eş olmayan kendine mahsus yapıları vardır. Ancak değişebilir jetonlarda (fungible token) tıpkı kağıt ve metal paralarda olduğu gibi değişebilir bir nitelik taşıması söz konusudur. Bununla ifade edilmek istenen 1 TL'lik bir metal paranın diğeri bir 1 TL'lik metal para yerine kullanılarak değiş-tokuşa aracılık etmesi gibi blokzinciri altyapısını kullanan Bitcoin gibi kripto paralarda da bu durumun geçerli olduğudur. Yani 1 Bitcoin yerine diğeri bir 1 Bitcoin geçebilmektedir. Dolayısıyla, değişebilir jetonların daha üretim aşamasında dahi karşılık buldukları bir değer bulunmaktadır.<sup>102</sup>

Ancak NFT'ler birbiri ile aynı değeri taşımayan ve fiyatı günden güne pazara olan talebe göre değişebilecek jetonlardır.

---

<sup>100</sup> Karayazgan, "Sigorta Sektöründe," 20.

<sup>101</sup> Tunca ve Sezen, "Sigorta İşlemlerinde Blokzincir," 15.

<sup>102</sup> Robyn Conti ve John Schmidt, "What You Need To Know About Non-Fungible Tokens (NFTs)," Forbes, erişim tarihi: Ağustos 27, 2021, <https://www.forbes.com/advisor/investing/nft-non-fungible-token/>.

Bu anlamda, birbirinden farklı resim, video, müzik ve benzeri içeriğe sahip NFT'ler aynı platformdan ihraç edilse dahi farklı fiyata sahip olabilmektedir.<sup>103</sup>

## X. NFT'İN GENEL ÇERÇEVESİ

Resimden müziğe, "twitlerden" video kliplere kadar birçok içerik NFT'ler vasıtası ile satışa çıkarılabilmektedir.<sup>104</sup> Kriptografi yöntemleriyle çeşitli içerikler akıllı sözleşmelere kilitlenerek satışa çıkarılmaktadır. NFT adı verilen bu içerikler özellikle NFT marketleri vasıtası ile kolay bir şekilde kriptopara karşılığında ticarete konu edilebilmektedir. Bir kez NFT'ye gömülen eserler, sahibinin fikri mülkiyeti altına girmektedir. Bu haliyle adeta, dijital bir bandrol altına alınmaktadırlar.<sup>105</sup>

Aslında NFT'lerin tarihi hemen hemen blokzincirinin ortaya çıkması kadar eskiye dayanmaktadır. Nitekim, ünlü simaların da kendilerine ait eşya veya sosyal medya paylaşımlarını bir süredir NFT aracılığı ile sattıkları basına da yansımıştır. BNP Paribas'ın yan kuruluşu L'Atelier'in raporuna göre 2020 yılında bir önceki yıla göre 4 kat artarak 338 milyon Dolarlık bir markete

---

<sup>103</sup> Conti ve Schmidt, "What You Need To Know".

<sup>104</sup> Bu çalışmanın yapıldığı günlerde bir NFT satışı daha gündeme gelmiştir. İnternet aleminde küçük kardeşinin parmağını ısırması ile bilinen "Charlie parmağımı ısırıldı" videosunun yaklaşık 760 bin Dolar'a NFT olarak satışı gerçekleşmiştir. Bu satışın ardından adı geçen videonun satımdan önce açık erişim şeklinde yer aldığı YouTube sitesinden kaldırılması beklenmektedir. NTV, "Charlie bit my finger" rekor fiyata NFT olarak satıldı", erişim tarihi: Mayıs, 24 2021, <https://www.ntv.com.tr/teknoloji/charlie-bit-my-finger-rekor-fiyata-nft-olarak-satildi,fhLOTQ5oaUi0ovQXwp5xQw>.

<sup>105</sup> Özgür Arkan, "NFT Sanat Eserleri ve Telif Hukuku," Fikri Mülkiyet, erişim tarihi: Mayıs 27, 2021, <https://fikrimulkiyet.com/nft-sanat-eserleri-ve-telif-hukuku/>.

ulaşan NFT satışlarının daha da büyüyeceği tahmin edilmektedir.<sup>106</sup>

NFT'lerin dünya çapında ses getirmesini sağlayacak olay ise, 2021 yılının ilk aylarında, bir sanat eserinin 69,3 milyon Dolar gibi astronomik bir fiyatla satımına aracılık etmesinin hemen ardından gerçekleşmiştir.<sup>107</sup>

## XI. NFT'NİN KAPSAMI VE HUKUKİ DEĞERİ

NFT'lerin hukuki statüsü hakkındaki belirsizlik NFT'lerin sigortalanması meselesinin yanı sıra, vergilendirilmesi noktasında da sorunlar yaratmaktadır. Bu bölümde, NFT'nin hukuki statüsü incelenerek yürürlükteki mevzuat açısından değerlendirilmesi yapılacaktır.

### A. Bir Eşya Olarak NFT

Her ne kadar blokzincirinde yer alan şeylerin somut olarak bir varlıkları olmasa da çeşit borca konu olamayan NFT'lerin Roma hukukundan beri gelen ayrıma istinaden biraz da geniş yorum yoluyla da olsa gayri misli eşya olarak adlandırılması mümkündür. Zira *Fungible* (değiştirilebilir) olarak üretilen jetonların aksine, NFT'lerin farkı önceden de belirtildiği üzere içinde gömülü olan içeriğin değiştirilemez oluşudur. Bu aşamada, NFT'lerin satım sözleşmesine konu edilmesi halinde bir parça borcu oluşacaktır. Söz konusu NFT içeriğinin çeşitli

---

<sup>106</sup> Nina Bambysheva, "BNP Paribas Subsidiary Helps Identify \$250 Million Leap In NFT Sales", Forbes, erişim tarihi: Mayıs 23, 2021, <https://www.forbes.com/sites/ninabambysheva/2021/02/15/french-banking-giant-bnp-paribas-details-explosion-of-new-crypto-sector-with-250-million-sales-volume/?sh=5ad59216412f>.

<sup>107</sup> Mehmet Çağrı, "NFT nedir? Kripto sanat çağı mı başlıyor?," TRT Haber, erişim tarihi: Mayıs 23, 2021, <https://www.trthaber.com/haber/kultur-sanat/nft-nedir-kripto-sanat-cagi-mi-basliyor-570069.html>.

sebeplerle yok olması durumunda sözleşme sona ereceğinden de bu aşamada gayri misli eşya olarak kabul edilmesi gerekmektedir.

NFT'ler ile içerik üretmenin en önemli faydası orijinal halinin devredilebilir bir şekilde koruma sağlamasıdır. Ayrıca bazı durumlarda Fikir ve Sanat Eserleri Kanunu'nun 45'inci maddesinde belirtilen sanat eserlerinin sonraki satışlarından pay verilmesi usulünün NFT'ler için kolaylıkla uygulama bulacağı da ifade edilmektedir.<sup>108</sup>

NFT'nin koruduğu bu hukuki değer yanında beri taraftan sanatçıların eserlerini ulaştırabilmesi noktasında eşitsizlik yarattığı, marketin kaosa neden olduğu, karbon emisyonu artırımı ile iklim değişikliğine katkı sağladığı ve nihayetinde emsalsiz bir kopya olarak hazırlanan eserin sanatın özüne ve ruhuna aykırı olduğuna yönelik iddialar da bulunmaktadır.<sup>109</sup>

NFT'lerin sanatın geleceğine ve çevreye yönelik olumlu veya olumsuz etkileri tartışılarsun, NFT'ler ile yapılan satışlarda içeriği üreten kimsenin sonraki satışlar için de komisyon alabilme fırsatı sağlamasının<sup>110</sup> dahi tek başına,

---

<sup>108</sup> Özgür Arıkan, "NFT Sanat Eserleri ve Telif Hukuku", Fikri Mülkiyet, Erişim Tarihi: 27 Mayıs 2021. <https://fikrimulkiyet.com/nft-sanat-eserleri-ve-telif-hukuku/>.

<sup>109</sup> Gregory Barber, "NFTs Are Hot. So Is Their Effect on the Earth's Climate," Wired, erişim tarihi: Mayıs 27, 2021. <https://www.wired.com/story/nfts-hot-effect-earth-climate/>; Cass Marshall, "NFTs are generating huge paydays for some artists, others feel under siege," Polygon, erişim tarihi: Mayıs 27, 2021. <https://www.polygon.com/22327806/nft-artists-online-theft-non-fungible-token>.

<sup>110</sup> Efe Öç, "NFT nedir: İnternette kolayca indirilebilen bir dijital eser, nasıl 70 milyon dolara alıcı buldu?," BBC, erişim tarihi: Mayıs 23, 2021, <https://www.bbc.com/turkce/haberler-dunya-56385962>; Beri taraftan, NFT'lerle yapılan satışlarda fiyatın inanılması güç bir hızla yükselmesinin

sanatçıları teşvik edeceği ve eserlerini bu yöntemle satma noktasında cesaretlendireceği ifade edilebilir.

Bu noktada, yer yer birbiriyle orantısız NFT fiyatları ortaya çıkabilmekte ise de fiziki sanat eserlerine benzer şekilde serbest piyasanın dengeyi bulacağı beklenmektedir.<sup>111</sup>

NFT'lerin blokzincirinde yer alan değiştirilemez yapısının yakın gelecekte sözleşmesel ilişkilerde de yaygın olarak kullanılabilmesi de mümkündür. Halihazırda Ethereum isimli kriptopara temelinde yer alan ve NFT olarak hazırlanan akıllı sözleşmelerin 19.000 sayısını aştığı da ifade edilmiştir.<sup>112</sup>

NFT'lerin hukuki olarak menkul kıymet olup olmadığı hususu ise henüz belli olmayıp konuya ilişkin olarak Amerikan mahkemelerinde yargılama devam etmektedir. Ayrıca, NFT'lerin teknolojik gelişmelerle birlikte *Fractional* (Bozukluk) halde üretilerek hisselerle ayrılması gibi meseleler de NFT'nin hukuki olarak nitelendirilmesini zorlaştırmaktadır. Beri taraftan, hemen aşağıda da değinileceği üzere yürürlükteki Türk mevzuatı açısından blokzincirinin bir ürünü olan bu yapının menkul kıymet olarak nitelendirme imkanı bulunmamaktadır.

---

dayanaksız ve olduğu ve çakılma riskinin bulunduğu da ifade edilmektedir. Her halükarda, sahte NFT'lere de dikkat edilmesi gerekir.

<sup>111</sup> Çağlar, yazısında NFT market fiyatlarının %50'sinin 200 Dolar altında olduğuna değinmektedir. Milyon dolar üzerinde satış yapan sanatçıların kriptopara topluluklarınca bilinen isimler olduğunu ifade etmekte, ortalama NFT fiyatının 2021 yılının Mayıs ayı itibarıyla 1400 Dolar olduğunu belirtmektedir. Deniz Çağlar, "NFT Sanat Pazarı: Finansal bir balon mu?," Habertürk, erişim tarihi: Mayıs 23, 2021. <https://www.haberturk.com/yazarlar/deniz-caglar/3057138-nft-sanat-pazari-finansal-bir-balon-mu>.

<sup>112</sup> Dilek Sarı, "Ethereum'daki (ETH) NFT Odaklı Akıllı Sözleşmeler Rekor Kırdı," Coinkolik, erişim tarihi: Mayıs 29, 2021. <https://www.coinkolik.com/ethereumdaki-eth-nft-odakli-akilli-sozlesmeler-rekor-kirdi/>.

## B. İlk NFT Davası – NFT, bir menkul kıymet midir?

NFT'lerin bu çalışmanın hazırlandığı sıralarda ciddi bir davayla karşı karşıya kaldığını not etmek gerekir. Dava, Ethereum blokzincirini kullanmakta iken, Flow adını verdikleri blokzincirini oluşturan ve önceden CryproKitties olarak bilinen Dapper Labs şirketine karşı açılmıştır. Şirket, NBA (National Basketball Association) ile ortaklaşa kurduğu "NBA Top Shot" isimli, Amerikan basketbol ligindeki kayda değer anları NFT'lere dahil ederek alım ve satım yapmaktadır. Ancak davacı tarafın iddiasına göre, bu ürünlerde makul bir kâr beklentisi ile yatırım söz konusu olduğundan menkul kıymet olarak satılması ve ulusal menkul kıymetler yasalarına uygun şekilde alım satım faaliyetinin yürütülmesi gerekmekte iken, kayıtsız şekilde yürütülen bu faaliyetin hukuka aykırı olduğu iddia edilmektedir. Virginia eyaletinde yaşayan davacının federal yasaların ihlal edildiğinden bahisle New York eyalet mahkemelerinde açtığı bu davanın yetki sebebiyle usulden reddi beklenmektedir. Yine de mahkeme henüz bir karar vermemiştir.<sup>113</sup>

Ancak, NFT'ler açısından kayda geçen ilk dava olmasının yanı sıra bu gibi davaların işbu çalışma özelinde de bir önem arz ettiğini belirtmek gerekir. Çünkü, bu veya buna benzer bir davanın kabulü ile hukuk literatüründe NFT'lerin makul bir kâr beklentisi niteliğini haiz olduğu ve menkul kıymet olarak adlandırılabilceği sonucu doğacaktır. Bunun ardından da söz konusu menkullerin taşıdığı riskin gerçek veya spekülâtif olup olmadığı noktasında bir değerlendirme de kaçınılmaz olacaktır. Zira, NFT'lerin spekülâtif risk taşıdığı ve zenginleşme beklentisinin yanı sıra piyasada oluşacak herhangi bir etkenle

---

<sup>113</sup> David Zaslowsky, "NBA Top Shot Sued Based on the Allegation That the Sale of NFTs Violated US Securities Laws Because they Qualify as Securities," Lexology, erişim tarihi: Ağustos 5, 2021. <https://www.lexology.com/library/detail.aspx?g=9617ec0c-4511-4223-9638-07c173438235>.

zarara neden olabileceği kabul edilirse, bu noktada sigorta kapsamına alınmayacağı net bir şekilde ifade edilebilir olacaktır.

Şayet, NFT'lerin spekülâtif risk taşıdığı kabul edilirse sigortanın genel ilkeleri açısından düşünüldüğünde NFT'ler açısından şöyle bir sorun söz konusu olabilecektir. Sezal'ın da çalışmasında belirttiği şekilde sigorta gerçek risklerle ilgilenir, zira zenginleşme aracı değil güvence aracı niteliğini taşımaktadır.<sup>114</sup> Buradan hareketle de söylenebilir ki, NFT'lerin zenginleşme aracı olarak bir menkul değer niteliği taşımasının yargı makamlarınca veya yasama organlarından çıkacak kanunlarca tespiti halinde sigorta poliçesine konu edilmesi mümkün olmayacaktır.

### C. NFT'nin Yürürlükteki Türk Mevzuatına Göre Konumu

İç hukuk bakımından yürürlükteki mevzuat açısından NFT'nin menkul kıymet olarak atfedilmesinin mümkün olmadığı açık bir şekilde ifade edilebilir. Zira kripto varlıkların kullanılmamasına ilişkin hazırlanan "Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmeliğin" 3'üncü maddesi ile getirilen tanımda kripto varlıkların "menkul kıymet ve sermaye piyasası aracı olamayacağı" hususu açıkça ifade edilmiştir.<sup>115</sup> Bu aşamada, Yönetmeliğin yürütücüsü olan Merkez Bankasının kanaati değişmedikçe hemen yukarıda yaptığımız açıklamalara istinaden ABD Mahkemelerince, blokzincirinin bir ürünü olan NFT'lerin, menkul kıymet olarak kabulünün iç hukuk açısından bir anlam ifade etmeyeceği de belirtilebilir. Ancak, Türkiye'nin de ardıl yaklaşımlarının

<sup>114</sup> Sezal, "Sigortacılık Sektöründe", 188.

<sup>115</sup> RG. 16.04.2021, S.31456. "Bu Yönetmeliğin uygulanmasında 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 varlıkları ifade eder."

NFT'lere ve genel olarak blokzinciri ile üretilen kriptoparalara menkul değer statüsü vermek yönünde değiştiğinde, bu defa bu ürünlerin sigorta kapsamından çıkarılması da gerekebilir. Son tahlilde, mevcut durum, NFT'lerin sigortalanmasında Türk hukuku açısından herhangi bir engel olmadığıdır. Bu sebeple, sigorta poliçesine konu edilerek teminat altına alınabilir.

Bu noktada, kripto varlıkların yürürlükteki mevzuat bakımından hukuki statüsünün belirsizliği gündeme gelmekle, Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmeliğin 3'üncü maddesinde "gayri maddi varlık" olarak ifade edilmesinden hareketle marka, patent, ticari sır gibi fikri veya sınai mülkiyete konu edilebilecek bir nitelik taşıdığı sonuç ve kanaatine ulaşılabilecektir. Bu haliyle de eşyaya ilişkin Türk Medeni Kanunu hükümlerinin uygulanmasının mümkün olmadığı ifade edilebilir.<sup>116</sup>

## XII. NFT'LERİN SİGORTALANMASI

Dünyanın hemen her yerinde siber sigorta hizmeti verilmesine karşın henüz NFT'ler için sunulan bir sigorta poliçesi bulunmamaktadır.

Bu yazının kaleme alındığı tarihte bilindiği kadarıyla tıpkı Türkiye gibi dünyada da henüz NFT'leri sigorta altına alan bir

---

<sup>116</sup> İşbu çalışma kapsamında daha önceden de ifade edildiği şekilde, kripto varlıkların dijital bandrol gibi bir fikri mülkiyete konu olması sebebiyle eşya üzerindeki mülkiyet kurallarının uygulanamayacağı ifade edilmekle birlikte; Özdemir'in çalışmasında kripto varlıkların ve özellikle kripto paraların günlük hayattaki sorunlarının çözülebilmesi için doğal güçlerin taşınır mülkiyetine konu olabileceğine dair Medeni Kanun düzenlemesinden hareketle kripto varlıklara eşya statüsünün verilmesinin bir ihtiyaç olduğu ifade edilmektedir. Konuya ilişkin anayasal dayanaklardan hareket eden bir çalışma olması sebebiyle ilgililer bakabilir: Gençer Özdemir, "Kripto Paraların Eşya Niteliği," *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 11, no. 1 (2021): 289-306.



şirkete ulaşılamamıştır. Ancak Hong Kong merkezli YAS MicroInsurance isimli sigorta şirketinin “NFTY” adını verdikleri NFT sigortası için İtalya merkezli Generali Sigorta ile iş birliğine gidilerek bu konuda birlikte çalışmalara başlandığı belirtilmektedir.<sup>117</sup> Türkiye’de de NFT alanında satış işlemlerinin başladığı ve yüksek tutarlara ulaşmaya yaklaştığı da gözetildiğinde Türk sigorta şirketlerinin de çağın gerisinde kalmamak adına bu alanda poliçe ve teminat hazırlıklarına girişeceklerini beklenebilir.

Beri taraftan NFT ürünlerinin, fiziksel ürünlerin banka kasalarında saklanması gibi saklanması amacıyla hizmet sunulmasına başlandığı da bildirilmektedir.<sup>118</sup>

Bu aşamada NFT’lerin yakın vakitte sigorta poliçelerine konu olacağı beklenmektedir. Böylelikle, teminat kapsamının belirlenmesi ve reasüransına yönelik işlemlerin başlatılması gerekmektedir.

### **XIII. NFT’LERİN TEMİNAT KAPSAMINA ALINMASI VE REASÜRANSI**

Çalışmanın ilk bölümünde de açıklandığı üzere, bir şeyin sigorta teminatı kapsamına alınabilmesi için karşılaşılabilecek risklerin ne olduğunun çok iyi bilinmesi gerekmektedir. Siber risklerin de bu açıdan bilinmesi gerekmele birlikte, aynı şekilde NFT’lerin de ne gibi tehditlerle karşı karşıya gelebileceği

---

<sup>117</sup> PR Newswire, “YAS Launches the World's First Microinsurance "NFTY" Covering NFT,” erişim tarihi: Mayıs 24, 2021. <https://www.prnewswire.com/news-releases/yas-launches-the-worlds-first-microinsurance-nfty-covering-nft-301269677.html>.

<sup>118</sup> Insured Finance, “Launching the First Insurance Vault for NFTs,” erişim tarihi: Mayıs 24, 2021. <https://insured.finance/launching-the-first-insurance-vault-for-nfts/>.

bilinmelidir. Nitekim blokzincirinin tartışmalı yapısı nedeniyle kişisel veri ihlallerine davetiye çıkarıp çıkarmadığının tespiti bu aşamada kritik düzeyde önem taşır. Zira, blokzincirinde yer alan tüm paydaşların kişisel verilerinin birbirleri arasında işlenmesi faaliyetleri de bulunabilecektir. Beri taraftan, veri sorumlusu ile uygulanacak yerel hukukun belirlenmesi ve açık rızanın geri çekilmesi gibi hususlar netleşmemektedir. Ancak bunların anonimleştirme gibi kişisel veri koruma mevzuatlarına uygun hale getirilmesinin de mümkün olduğu ifade edilmektedir.<sup>119</sup>

NFT'lerin fikri mülkiyet hakkına konu olması sebebiyle, siber sigortalarda veya geleneksel sigortalarda olduğu gibi teminat altına alınmasını olanaksız kılmaktadır. Oysa, siber casusluk gibi faaliyetlerle bu gibi fikri ürünlerin değerlerinin düşürülmesi ise ihtimal dahilindedir. Nitekim OECD'nin raporunda da bu hususun siber sigorta sektörünün gelişmesinin önünde bir engel olduğu mütalaa edilmiştir.<sup>120</sup> Bu noktada, daha önceden de ifade edildiği şekilde, sigorta şirketlerinin proaktif role bürünerek NFT içeriğinin güvenliğinin sağlanmasına yönelik teknolojik gelişmelerin eşzamanlı olarak poliçe sahipleriyle paylaşılması zorunluluğu ortaya çıkacaktır.

Sanal bir parmak izi gibi eşsiz<sup>121</sup> olan bu NFT'lerle satıma konu edilen eserlerin mali bir değer ifade ettiği açıktır. Bu değerın sanat eseri gibi mallarda fahiş fiyatlara kadar çıkması ile NFT'lerin hukuken geçerli ve korunması gereken bir menfaat olduğu ve bu sebeple teminat altına alınabilmesi gerektiği anlaşılmaktadır. Her ne kadar günümüz itibarıyla sigorta şirketlerince böyle bir poliçe söz konusu olmasa da ileriki

---

<sup>119</sup> Blockchain Türkiye, Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu, Türkiye Bilişim Vakfı, 78-84.

<sup>120</sup> OECD, "Supporting An Effective", 8.

<sup>121</sup> Tunca ve Sezen, "Sigorta İşlemlerinde Blokzincir", 16.

zamanlarda yapılacak bir sigortanın muhtemelliği ve büyük ölçüde kesinliği söz konusu olacaktır.

NFT'lerde ortaya çıkma ihtimali olan muhtemel zararlar gerek birinci taraf ve gerek üçüncü taraf teminatlarını ilgilendirir niteliktedir.<sup>122</sup>

NFT'lerin zarara karşı veya suça karşı olmak üzere iki farklı şekilde sigortaya konu olacağı ifade edilmektedir. Zarar sigortasının işçi zararlarına benzer şekilde kişisel bilgisayar veya başkaca bir şeyin blokzincirine yapacağı müdahaleden dolayı oluşan zararlardan dolayı teminat sağlayacağı ve diğer yandan hırsızlık veya mala zarar verme gibi hareketlerden veya üçüncü bir kişinin NFT içeriğindeki ürünün sahtesini piyasaya sürerek oluşturabileceği dolandırıcı faaliyetlerden dolayı ise suça karşı sigorta teminatı kapsamında tabi tutulabileceği ifade edilmektedir.<sup>123</sup> Suça karşı sigortalamak tanımının da iç hukukumuzdaki karşılığının sorumluluk sigortası ile daha uyumlu olduğu ifade edilebilir.

NFT teminatının sigorta lehtarları açısından asıl beklentisinin de NFT sahibinin dijital varlığın değeri hakkında önceden belirlenmiş bir bedelin ödenmesinin birinci taraf teminatlara kıyasen daha öncelikli olacağı da ifade edilebilir.<sup>124</sup>

---

<sup>122</sup> Aynı yönde bkz: Bethan Moorcraft, "How can we insure NFTs?", Insurance Business America, Erişim Tarihi: 29 Temmuz 2021. <https://www.insurancebusinessmag.com/us/news/breaking-news/how-can-we-insure-nfts-260576.aspx>.

<sup>123</sup> General Liability Insurance, "Non-Fungible Tokens Insurance (NFTs)," erişim tarihi: Mayıs 24, 2021. <https://generalliabilityinsure.com/non-fungible-tokens-insurance.html>.

<sup>124</sup> Bethan Moorcraft, "How can we insure NFTs?," Insurance Business America, erişim tarihi: Temmuz 29, 2021. <https://www.insurancebusinessmag.com/us/news/breaking-news/how-can-we-insure-nfts-260576.aspx>.

Ancak siber kişiliklerin ortaya çıkması ile birlikte üretilen içeriklerin ve işbu çalışma özelinde NFT'lerin bir eşya olarak kabul edilmesi halinde mal sigortası olarak kabul edilmesi gerektiği söylenebilir. Ancak NFT teknolojisi ile kayıt altına alınan eserlerin adeta çevrimiçi bir galeri gibi satışa çıkarıldığı pazarlar açısından ise mesleki sorumluluk sigortasına benzer sigorta ihtiyacı gündeme gelebilecektir. Nihayetinde sigortanın kapsamı ve lehtar bakımından çeşidinin değişeceği söylenebilir.

VHV Reasürans A.Ş.'nin sitesinde yer alan bilgiye göre, sanat sigortalarındaki pazarın artışı ve bununla eş şekilde artan reasürans ihtiyacına istinaden risk kabullerinin başladığı belirtilmiştir.<sup>125</sup> Bu aşamada, çok yakın gelecekte fiziksel sanat eserlerine getirilen söz konusu reasüre hizmetinin kapsamının NFT'ler açısından da genişletilmesi söz konusu olabilecektir.

#### **XIV. BOZUKLUK NFT'LER (FRACTIONAL NFTS)**

NFT'lere ilişkin olarak son güncellemelerden biri de bir NFT içeriği üzerinde paylı mülkiyete sahip olmaya olanak tanıyan Bozukluk NFT'lerdir. *Fraction* ya da *Fractional NFT*<sup>126</sup> olarak ifade edilen bu NFT çeşitleri içeriğin tümü üzerinde bir anda mülkiyet sahibi olamayan kullanıcılar için katkıda bulunulan hisse oranında parça temini sağlamaktadır. Kullanıcılar yalnızca bir NFT'nin parçalarını alabileceği gibi birkaç NFT'ye ait parçalardan farklı olanlarda alım yaparak kendi portföylerini de oluşturabilmektedirler.<sup>127</sup>

---

<sup>125</sup> VHV Reasürans, Sanat Sigortaları, erişim tarihi: Ağustos 26, 2021, <https://www.vhvre.com/tr-tr/sanatsigortalari>.

<sup>126</sup> Esasen "Fractional" ifadesinin fraksiyonel, parçalı, kısmi, oranlı veya hisseli gibi alternatif çevirileri yapılabilir ise de, blokzinciri ve kripto para teknolojisinin geleneksel para terimleri ile karşılanabileceği düşüncesinden hareketle "bozukluk" ibaresinin kullanımı bu çalışma kapsamında tercih edilmiştir.

<sup>127</sup> Fractional, "What is Fractional?," Medium, erişim tarihi: Ağustos 25, 2021, <https://medium.com/fractional-art/what-is-fractional-dd4f86e6458a>.

Bozukluk NFT'lerin oluşum mantığı ise, öncelikle NFT içeriğinin akıllı sözleşme içine kitlenmesi gerekmektedir. Bunun ardından, akıllı sözleşmeye kitlenen NFT içeriği için üretilecek toplam jeton sayısı belirlendikten sonra her bir jeton NFT içeriği olan bütünün parçaları halini almaktadır. Bunun ardından da her bir "Bozukluk" ayrı ayrı satım işlemine konu edilebilmektedir. Satımlardan diğer ortaklar etkilenmemekte ancak toplam fiyat artışından hisseleri oranında kazanç sağlamaları beklenmektedir. Bozukluk NFT'lerin bu yapısının, küçük yatırımcıyı koruyan ve paydaşları tasarrufta bulunmaya zorlamayan demokratik bir yapı getirdiği, tüm payların iktisabı ile adeta "Bütünleme" yapma olanağı tanıdığı hususları da ifade edilmektedir.<sup>128</sup>

Aslında Bozukluk NFT'lerin, NFT'nin bölünmezlik ilkesini<sup>129</sup> geçerek, yeniden değiştirilebilir bir hale geldiğini ifade etmek de mümkündür. Bu noktada, RFT (refungible tokens) olarak da ifade edilecek bozukluk NFT'lerinin aslında ilk düşüncede NFT olmadığı da değerlendirilebilir.

NFT'lerin "Bozukluk" haline alabilmesi yani hisselerle ayrılması ile menkul kıymet olarak nitelendirilip nitelendirilemeyeceği hususu bir kez daha önem kazanmaktadır. Çalışma özelinden hareketle, NFT sigortası açısından parça üzerinde teminat sağlanması imkanı daha büyük bir zorlukla karşılaşmaktadır. Kaldı ki, paydaşların tutum ve tasarrufları ile NFT içeriğinin bütününde sebep olabilecekleri özellikle yıkıcı etkiler açısından teminat sağlanamayacağı da düşünülebilir. Ancak yukarıda bahsedildiği gibi, Bozukluk NFT'lerin, yeniden değiştirilebilir jeton haline

---

<sup>128</sup> Cameron Robbins, "Fractionalized NFTs," Medium, erişim tarihi: Ağustos 25, 2021. <https://medium.com/the-zap-project/fractionalized-nfts-d3fa7458ae5>.

<sup>129</sup> "Gwyneth Iredale, "The Difference Between Fungible And Non-Fungible Tokens," erişim tarihi: Ağustos 27, 2021, <https://101blockchains.com/fungible-vs-non-fungible-tokens/>

getirildiğinin kabulü halinde zaten NFT olmadığı için sigorta kapsamında incelenmesine de gerek kalmayacaktır.

## **XV. İÇ HUKUK İMKANLARININ DEĞERLENDİRİLMESİ: ÖZEL RİSKLER YÖNETİM MERKEZİ**

Yazının bu kısmında NFT konusunda mevcut düzenlemelerde dahi sigorta faaliyeti yürütebilecek otoritelerden bahsedilecektir. Öyle ki, her ne kadar siber sigortacılık faaliyetine veya NFT'lere yönelik bir kurum teşekkül etmemiş ise de işler bir hukuk sisteminde eldeki imkanların elverişli bir şekilde kullanılması önem arz eder. Bu şekildedir ki, oluşabilecek ihtilaflara karşı gecikmeksizin ve mağduriyetleri önler şekilde müdahale edilebilecektir.

Özel Riskler Yönetim Merkezi olarak isimlendirilen kurumun teşekkülü ile sigorta sektörüne yeni bir soluk getirilmesi amaçlanmıştır. Öyle ki, bu merkezin AR-GE merkezi olacağı ve sektörün ihtiyaçlarına çözüm üreteceği de ifade edilmiştir.<sup>130</sup>

Öte yandan, Özel Riskler Yönetim Merkezi'nin teşkilatlanmasına ilişkin kanuni düzenlemesinde de bu amaçtan bahsedilmiştir. Nitekim, 7319 sayılı Kanun'un 12'nci maddesi ile değişik 5684 sayılı Sigortacılık Kanunu'nun 33/A maddesinin gerekçesinde "sigorta ve reasürans teminatı bulunamayan riskler ve özellik arz eden riskler için daha hızlı çözüm üretilebilmesi, ölçek ekonomisinden faydalanılmasının"<sup>131</sup> amaçlandığı ifade edilmiştir.

---

<sup>130</sup> Selva Eren'in açıklamalarından alıntılaman Umut Deniz Elçi, "Özel Riskler Yönetim Merkezi sektörün ihtiyaçlarına çözüm üretecek", Sigortacı Gazetesi, erişim tarihi: Ağustos 26, 2021, <https://sigortacigazetesi.com.tr/ozel-riskler-yonetim-merkezi-sektorun- ihtiyaclarina-cozum-uretecek/>.

<sup>131</sup> TBMM, 262 sıra sayılı Plan ve Bütçe Komisyon Raporu, 8.

Bu noktada, NFT'ler bakımından halihazırda bir sigorta veya reasürans teminatına yönelik bir düzenleme olmadığı hususu da dikkate alınarak, varsayımsal olarak söylenebilir ki, özellikle kamu yararlarını ilgilendiren bir tehdidin ortaya çıkması ile Merkezin gerekli önlemleri re'sen alabilme imkânı oluşacaktır.

## SONUÇ VE ÖNERİLER

Buraya kadar yapılan açıklamalarda da görüleceği üzere, siber sigorta sektörü halen çok genç ve niş bir alan olarak taliplilerini ve girişimcilerini beklemektedir. Özellikle büyük piyasa aktörleri şimdiden bu alanda hizmet sunumuna başlamış vaziyettedir. Ancak kamu tarafında ise adeta bir sessizlik hakimdir. Blokzincirinin gelişimi ile kripto para ve dijital varlıkların yadsınamaz bir noktaya varması halinde, kamu tarafındaki bu isteksizliğin de yerini peşi sıra regülasyonlara bırakacağını öngörmek zor değildir. Bu çalışmada DIM olarak kullanılması da önerilen NFT'ler için de gerek Türkiye'de ve gerek dünyada henüz bir sigorta hizmeti sunulmamaktadır. Ancak önce davrananın kârlı çıktığı günümüz dünyasında ilgisiz kalınan bu alanda yapılacak çalışmalar, müteşebbislerine yüksek menfaatler sağlayabilecektir.

Bu aşamada, çalışma kapsamında değinilen hususlara dair maddeler halinde hazırlanmış öneriler ise şu şekildedir:

- Siber risklere ilişkin çerçevenin hazırlanması siber sigortanın gelişimini kolaylaştıracaktır. Bu sebeple, *bilgi güçtür* ilkesi çerçevesinde özellikle beyaz şapkalı hackerler gibi grupların da yardımıyla mümkün olduğunca bilinmeyen risk kalmaması sağlanmalıdır.

- Siber güvenliğe ilişkin standardizasyon işlemleri hızlandırılarak işletme güvenliğinin artırılması yoluna gidilmelidir. Özellikle, siber risklerin azımsanmayacak derecede bir kısmının personel hatalarından ve bilgisizliğinden kaynaklandığı düşünüldüğünde, personelin bilişim

okuryazarlığı ve siber farkındalığının artırılmasına yönelik çalışmalara ağırlık verilmesi gerekmektedir.

- Siber güvenliğin sağlanmasına yönelik işletmelerce takip edilecek temel usul ve esasların belirlenmesi gerekmektedir ki, bu husus kamu tarafına düşen bir sorumluluktur. Söz konusu usul ve esasların belirlenmesi ile birlikte, siber sigorta poliçelerinin belirliliği de artacaktır.

- Kamu tarafına düşen ikinci bir yük ise, siber sigortaya ilişkin yasal düzenlemelerin netleştirilmesi ve mümkünse yalnızca siber güvenlik uzmanlaşacak ve bu çalışmadaki öneride bahsedildiği üzere Siber Güvenlik Kurulu yerine Türkiye Ulusal Siber Güvenlik Ajansına benzer bir şekilde regülatif kuruluşun teşekkülünün sağlanmasıdır. Bu şekilde, siber sigorta sektörünün de tek elden veya en azından bu yapılamayacaksa da sigortalara ilişkin diğer kamu kurum ve kuruluşları ile koordineli şekilde yönetimi sağlanabilecektir.

- Siber sigortanın vergilendirilmesine ilişkin teşviklerle sunulan poliçelere olan talebin artışı üzerine düşünmek hem siber sigorta hem de vergi branşı açısından birbirini besler şekilde etkisi olabileceği hususu üzerine düşünmekte fayda görülmektedir.

- Siber sigortanın zorunlu sigortalardan biri haline getirilmesine yönelik taleplerin değerlendirilerek bunun yalnızca KOBİ'ler açısından değil, avangart rolü görmeleri maksadıyla büyük şirketlerden başlanarak uygulamaya geçilmesi imkanının değerlendirilmesi gerekmektedir.

- NFT'ler açısından öncelikle, güncel ve küresel gelişmelerin de takibiyle birlikte menkul değer olarak bir anlam ifade edip etmediğinin kat'i suretle tespitinin yapılması gerekmektedir. Şayet bir yatırım aracı olarak görülecek ise de bu yönelik önlemlerin gecikmeksizin alınmasında fayda vardır. Her ne kadar Merkez Bankasının kripto paraların finansal işlemlerde kullanılmasının yasaklanmasına dair yönetmeliği olsa da



küresel gelişmelerin kulak tıkanarak engellenemeyeceği hususu da değerlendirilmelidir.

- NFT'ler de dahil olmak üzere, kripto varlıkların taşınır eşya statüsünün mümkünatı hususunun değerlendirilmesi gerekmektedir.

- NFT'lerin statüsünün tanınması ile sigortaya ilişkin soru işaretlerinin giderilmesinin yanı sıra eğer menkul değer olarak atfı kabil olacak ise yatırımcısına getireceği değer vergilendirilmesi imkanı üzerinde düşünmek gerekecektir.

- Doğrudan yatırım aracı olmayan ve özellikle sanat eseri niteliğini taşıyan koleksiyon ürünleri açısından, NFT sigortasının siber sigorta kapsamında olup olmayacağı veya münhasıran teklif olarak sunulması halinde yine hangi şartlara tabi olacağının belirlenmesi gerekmektedir.

---

**Hakem Değerlendirmesi:** Çift kör hakem.

**Finansal Destek:** Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

**Çıkar Çatışması:** Yazarlar çıkar çatışması bildirmemiştir.

**Etik Kurul Onayı:** Yazarlar etik kurul onayının gerekmediğini belirtmiştir.

**Peer Review:** Double peer-reviewed.

**Financial Support:** The authors have not declared whether this work has received any financial support.

**Conflict of Interest:** The authors have no conflict of interest to declare.

**Ethics Committee Approval:** The authors stated that ethics committee approval is not required.

---

## KAYNAKÇA

### Kıtap, Makale, Tez, Bildiri ve Raporlar

- Altuntaş, Eda, Emine Kara, Abdullah Buğra Soylu ve Erdem Kırkbeşoğlu, "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar." *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, no. 12 (Aralık 2018): 8-22.
- Bara, Daniel, Sanja Ćorić ve Goran Jurišić, "The role of the Cyber Insurance in managing and mitigating Cyber Security Risk (With special emphasis on the potential of Croatia and Serbia Cyber insurance market)", *Međunarodna naučno-stručna konferencija IKT bezbednost (Uluslararası Bilimsel-Profesyonel BİT Güvenliği Konferansı)*, (Ocak 2015): 35-44.
- Blockchain Türkiye, Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu, Türkiye Bilişim Vakfı
- Bul, Aycan. "Sigorta Dağıtım Kanallarının Dijitalizasyonu", 15. Ulusal İşletmecilik Kongresi Bildirileri, (26-28 Mayıs 2016). Erişim Tarihi: 09 Ağustos 2021. [https://www.researchgate.net/publication/313837149\\_SIGORTA\\_DAGITIM\\_KANALLARININ\\_DIJITALIZASYONU](https://www.researchgate.net/publication/313837149_SIGORTA_DAGITIM_KANALLARININ_DIJITALIZASYONU)
- Cebeci, İpek. "Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme." *Üçüncü Sektör Sosyal Ekonomi Dergisi* 56, no. 1 (2021): 163-188.
- Çatuk, Cüneyt. "Siber Riskler Karşısında KOBİ'lerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örnekleme." Yayımlanmamış doktora tezi, Hasan Kalyoncu Üniversitesi, 2018.
- Çotak, Alperen. "Sigortacılık Sektöründe Siber Güvenliği, Dünyada ve Türkiye'de Gelişmelerin İncelenmesi." Yayımlanmamış yüksek lisans tezi, Marmara Üniversitesi, 2019.
- Hazine ve Maliye Bakanlığı, 26 Ekim 2020 tarihi itibarıyla Sigorta ve Reasürans Şirketleri ile Emeklilik Şirketlerinin Ruhsat Sahibi Olduğu Branşları Gösterir Tablo, Erişim Tarihi: 24

- Ağustos 2021.  
<https://ms.hmb.gov.tr/uploads/2020/10/Sigorta-ve-Reas%C3%BCrans-%C5%9Eirketleri-ile-Emeklilik-%C5%9Eirketlerinin-Ruhsat-Sahibi-Oldu%C4%9Fu-Bran%C5%9Flar%C4%B1-G%C3%B6sterir-Tablo-26.10.2020.xlsx>.
- Karayazgan, Ahmet. "Hukuki Yönüyle Siber Sigorta ve Sessiz Siber Teminatının Çalışma Esasları", iç. Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Makalelerim Işığında), İstanbul: Legal Yayıncılık, 2020.
- Karayazgan, Ahmet. "Sigorta Sektöründe Siber Risk-Siber Sigorta", iç. Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Makalelerim Işığında), İstanbul: Legal Yayıncılık, 2020.
- Korkusuz, Ahmet. "Kurumlarda Siber Güvenlik ve Siber Riskler", Yayımlanmamış yüksek lisans tezi, Bahçeşehir Üniversitesi, 2020.
- Kubılay, Huriye ve Atakan Kubılay. "Sigortacılık Sektöründe Bilişim Teknolojilerinin Rolü." *Yaşar Üniversitesi E-Dergisi*, no. 8 (2013): 1819-1856.
- Kule, Duygu. "Dijital Sigortacılıkta Hizmet Kalitesi", Yayımlanmamış yüksek lisans tezi, Kütahya Dumlupınar Üniversitesi, 2019.
- Marsh ve Birleşik Krallık Hükûmeti, UK Cyber Security The Role of Insurance in Managing and Mitigating the Risk.
- Marsh ve TÜSİAD, 2020 Türkiye Siber Risk Algı Araştırması.
- Marsh, Global Insurance Markets: Pricing Increases Moderate in Second Quarter, (Temmuz 2021).
- Milli Reasürans T.A.Ş. 2020 Faaliyet Raporu.
- OECD, Supporting An Effective Cyber Insurance Market, OECD Report for the G7 Presidency, (Mayıs 2017).

- Oxera, The value of cyber insurance to the UK economy: Prepared for the Association of British Insurers, (Kasım 2020).
- Ömürbek, Nuri ve Fatma Gül Altın. "Sigortacılık Sektöründe Bilgi Teknolojilerinin Uygulanmasına İlişkin Bir Araştırma." *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 13, no. 3 (2008): 105-127.
- Özdemir, Gençler. "Kripto Paraların Eşya Niteliği." *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 11, no. 1 (2021): 289-306.
- PWC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience, (2015).
- Sezal, Levent. "Sigortacılık Sektöründe Karşılaşılan Riskler ve Etkin Risk Yönetimi." *Sosyal Bilimler Dergisi*, no.17, (Aralık 2018): 185-199.
- Sezal, Levent. "Türk Sigortacılık Sektöründe Mobil Teknoloji Uygulamaları." *Sosyal Bilimler Dergisi*, no. 19 (Ocak 2018): 130-143.
- Şekeroğlu, Sinan ve Haşim Özüdoğru. "Dijital Dönemin Koruyucuları: Siber Risk Sigortaları." 4. *International Research Congress on Social Sciences* (11-13 September 2019): 55-64.
- TBMM, 262 sıra sayılı Plan ve Bütçe Komisyon Raporu
- Tunca, Sezai ve Bülent Sezen. "Sigorta İşlemlerinde Blokzincir (Blockchain) Teknolojisi Uygulamaları." *Bankacılık ve Sigorta Araştırmaları Dergisi*, no. 14 (2020): 13-25.
- Türk Reasürans A.Ş. 2020 Faaliyet Raporu
- Ulaştırma ve Altyapı Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)
- Verizon, 2021 Data Breach Investigations Report
- Yıldırım, İsmail ve Eyyüp Ensari Şahin. "Insurance Technologies (Insurtech): Blockchain and Its Possible Impact on Turkish

- Insurance Sector." *Journal of International Management, Education and Economics Perspectives* 6, no. 3, (2018): 13-22.
- Yurdakul, Müberra ve Nilüfer Dalkılıç. "Sigortacılık Sektöründe Dijital Çağ." *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, no. 50, (Ekim 2016): 49-67.
- Zülfikar, Hamza. "Gündemi Meşgul Eden Sağlık Terimleri." *Türk Dili*, no. 821, (Mayıs 2020): 10-16.

### **İnternet Kaynakları**

- Acer, Fatih. "Sigorta sektörü InsurTech ile gelişecek." *Sigorta Medya*, Erişim Tarihi: Temmuz 31, 2021. <https://www.sigortamedya.com.tr/fatih-acer-sigorta-sektoru-insurtech-ile-gelisecek/>
- Altuncu, Özgür. "Siber vatan savunması." *Hürriyet*, Erişim Tarihi: Mayıs 28, 2021. <https://www.hurriyet.com.tr/gundem/siber-vatan-savunmasi-41716074>
- Arıkan, Özgür. "NFT Sanat Eserleri ve Telif Hukuku." *Fikri Mülkiyet*, Erişim Tarihi: Mayıs 27, 2021. <https://fikrimulkiyet.com/nft-sanat-eserleri-ve-telif-hukuku/>.
- Bambysheva, Nina. "BNP Paribas Subsidiary Helps Identify \$250 Million Leap In NFT Sales." *Forbes*, Erişim Tarihi: Mayıs 23, 2021. <https://www.forbes.com/sites/ninabambysheva/2021/02/15/french-banking-giant-bnp-paribas-details-explosion-of-new-crypto-sector-with-250-million-sales-volume/?sh=5ad59216412f>.
- Barlas, Mahmut. "Türk Hukukunda Siber Sigorta." *Fintechtime*, Erişim Tarihi: Mayıs 24, 2021. <https://fintechtime.com/tr/2020/09/turk-hukukunda-siber-sigorta/>.

- Conti Robyn ve John Schmidt. "What You Need To Know About Non-Fungible Tokens (NFTs)." Forbes, Erişim Tarihi: Ağustos 27, 2021. <https://www.forbes.com/advisor/investing/nft-non-fungible-token/>
- Çağlar, Deniz. "NFT Sanat Pazarı: Finansal bir balon mu?." Habertürk, Erişim Tarihi: Mayıs 23, 2021. <https://www.haberturk.com/yazarlar/deniz-caglar/3057138-nft-sanat-pazari-finansal-bir-balon-mu>.
- Çağrı, Mehmet. "NFT nedir? Kripto sanat çağı mı başlıyor?," TRT Haber, Erişim Tarihi: Mayıs 23, 2021. <https://www.trthaber.com/haber/kultur-sanat/nft-nedir-kripto-sanat-cagi-mi-basliyor-570069.html>.
- Çipil, Mahir. "'Blockchain' sigortacılığı nasıl etkileyecek?," Dünya, Erişim Tarihi: Temmuz 31, 2021. <https://www.dunya.com/kose-yazisi/blockchain-sigortaciligi-nasil-etkileyecek/344612>.
- Dünya, "Siber sigorta pazarı 15 milyar dolara gidiyor", Erişim Tarihi: Mayıs 24, 2021. <https://www.dunya.com/sectorler/sigortacilik/siber-sigorta-pazari-15-milyar-dolara-gidiyor-haberi-455727>.
- Elçi, Umut Deniz. "Özel Riskler Yönetim Merkezi sektörün ihtiyaçlarına çözüm üretecek", Sigortacı Gazetesi, Erişim Tarihi: Ağustos 26, 2021. <https://sigortacigazetesi.com.tr/ozel-riskler-yonetim-merkezi-sektorun- ihtiyaclarina-cozum-uretecek/>.
- Fractional, "What is Fractional?," Medium, Erişim Tarihi: Ağustos 25, 2021. <https://medium.com/fractional-art/what-is-fractional-dd4f86e6458a>.
- General Liability Insurance, "Non-Fungible Tokens Insurance (NFTs)", Erişim Tarihi: Mayıs 24, 2021. <https://generalliabilityinsure.com/non-fungible-tokens-insurance.html>.

- Habertürk, "Siber güvenlik sigortası KOBİ'ler için zorunlu olmalı", Erişim Tarihi: Mayıs 24, 2021. <https://www.haberturk.com/siber-guvenlik-sigortasi-kobiler-icin-zorunlu-olmali-3023980-ekonomi>.
- Insured Finance, "Launching the First Insurance Vault for NFTs", Erişim Tarihi: Mayıs 24, 2021. <https://insured.finance/launching-the-first-insurance-vault-for-nfts/>.
- Iredale, Gwyneth. "The Difference Between Fungible And Non-Fungible Tokens", Erişim Tarihi: Ağustos 27, 2021. <https://101blockchains.com/fungible-vs-non-fungible-tokens/>
- Moorcraft, Bethan. "How can we insure NFTs?", Insurance Business America, Erişim Tarihi: Temmuz 29, 2021. <https://www.insurancebusinessmag.com/us/news/breaking-news/how-can-we-insure-nfts-260576.aspx>.
- NTV, "Charlie bit my finger" rekor fiyata NFT olarak satıldı", Erişim Tarihi: Mayıs 23, 2021. <https://www.ntv.com.tr/teknoloji/charlie-bit-my-finger-rekor-fiyata-nft-olarak-satildi,fhLOTQ5oaUi0ovQXwpSxQw>.
- Öç, Efe. "NFT nedir: İnternette kolayca indirilebilen bir dijital eser, nasıl 70 milyon dolara alıcı buldu?", BBC, Erişim Tarihi: Mayıs 23, 2021. <https://www.bbc.com/turkce/haberler-dunya-56385962>.
- PR Newswire, "YAS Launches the World's First Microinsurance "NFTY" Covering NFT", Erişim Tarihi: Mayıs 24, 2021. <https://www.prnewswire.com/news-releases/yas-launches-the-worlds-first-microinsurance-nfty-covering-nft-301269677.html>.
- Robbins, Cameron. "Fractionalized NFTs", Medium, Erişim Tarihi: Ağustos 25, 2021. <https://medium.com/the-zap-project/fractionalized-nfts-d3fa7458ae5>.

- Sarı, Dilek. "Ethereum'daki (ETH) NFT Odaklı Akıllı Sözleşmeler Rekor Kırdı", Coinkolik, Erişim Tarihi: Mayıs 29, 2021. <https://www.coinkolik.com/ethereumdaki-eth-nft-odakli-akilli-sozlesmeler-rekor-kirdi/>.
- Sigorta Gündemi, "Siber risklere karşı Türkiye'nin ilk bireysel sigortası", Erişim Tarihi: Mayıs 24, 2021. <http://www.sigortagundem.com/haber/siber-risklere-karsi-turkiyenin-ilk-bireysel-sigortasi/1262619#ixzz52TtNbm84>.
- Sözcü, "Siber sigorta pazarı 9.5 milyar dolara ulaşacak", Erişim Tarihi: Mayıs 24, 2021. <https://www.sozcu.com.tr/2021/sigorta/siber-sigorta-pazari-9-5-milyar-dolara-ulasacak-6221265/>.
- Utkueri, Okan. "Dijital Sigortacılık ve Güven", Sigortacı Gazetesi, Erişim Tarihi: Mayıs 27, 2021. <https://sigortacigazetesi.com.tr/dijital-sigortacilik-ve-guven/>.
- VHV Reasürans, Sanat Sigortaları, Erişim Tarihi: 26 Ağustos 2021. <https://www.vhvre.com/tr-tr/sanatsigortalari>.
- Yeniova, Gözde. "Siber saldırılara karşı sigorta teminatı geldi", Ekonomist, Erişim Tarihi: Mayıs 24, 2021. <https://www.ekonomist.com.tr/teknoloji/siber-saldirilara-karsi-sigorta-teminati-geldi.html>.
- Zaslowsky, David. "NBA Top Shot Sued Based on the Allegation That the Sale of NFTs Violated US Securities Laws Because they Qualify as Securities", Lexology, Erişim Tarihi: Ağustos 25, 2021. <https://www.lexology.com/library/detail.aspx?g=9617ec0c-4511-4223-9638-07c173438235>.