SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 23.05.2024
Kabul | Accepted: 02.09.2024
doi 10.15337/suhfd.1488748

SİBER RİSK SİGORTASI:

ALMAN SİBER RİSK SİGORTASI GENEL ŞARTLARI ÇERÇEVESİNDE BİR İNCELEME

Doç. Dr. Aydın Alber YÜCE*

Öz

İnternet teknolojisi ve insan hayatında kapladığı alan, 2010'lu ve 2020'li yılların dünyasında, geçmiş on yıllara göre mukayese edilemeyecek derecede değişmiştir. Siber dünyanın gerçek dünya ile olan yoğun ilişkisi, işlenen suçların ve kişilerle işletmelerin hukuka aykırı fiiller sebebiyle karşı karşıya kaldıkları zararların siber ortama taşınmasına sebep olmuştur. O halde, sigorta hukuku açısından, gerçek dünyada olduğu gibi sanal dünyada da gerçekleşebilecek rizikolar teminat altına alınmalıdır. Bu ihtiyaca yönelik sigorta, siber risk sigortasıdır.

Uygulamada sıklıkla akdedilen siber risk sigortası sözleşmeleri için, ülkemizde genel şart niteliğinde bir düzenleme bulunmamaktadır. Bu çalışmada, Alman hukukunun hukuk sistemimize olan yakınlığı sebebiyle Alman Siber Risk Sigortası Genel Şartları, siber risk sigortasının açıklanması amacıyla incelenecektir.

* Doç. Dr. Öğr. Üyesi. Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi, Özel Hukuk Bölümü, Ticaret Hukuku Anabilim Dalı, Eskişehir, Türkiye ⚜⚜ Assoc. Prof. Dr., Eskişehir Osmangazi University, Faculty of Law, Department of Private Law, Commercial Law Department, Eskişehir, Türkiye.
aydinalberyuce@gmail.com • ORCİD 0000-0002-6178-9143.

Atıf Şekli | **Cite As**: **YÜCE,** Aydın Alber: "Siber Risk Sigortası: Alman Siber Risk Sigortası Genel Şartları Çerçevesinde Bir İnceleme", SÜHFD, C. 32, S. 3, 2024, s. 1611-1655.

İntihal | **Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. | This article has been scanned via a plagiarism software and reviewed by at least two referees.

Bu eser Creative Commons Atıf-Gayri Ticari 4.0 Uluslararası Lisansı ile lisanslanmıştır. | This work is licensed under Creative Commons Attribution-Non Commercial 4.0 International License.

Anahtar Kelimeler

•Sigorta Sözleşmesi •Sigorta Ettiren •Sigortacı •Siber Risk •Siber Risk Sigortası

CYBER RISK INSURANCE:

AN ANALYSIS IN THE CONTEXT OF THE GENERAL CONDITIONS OF GERMAN CYBER SECURITY INSURANCE

Abstract

Cyber technology and the space it occupies in human life have changed incomparably in the world of the 2010s and 2020s compared to previous decades. The dense correlation of the cyber world with the real world has caused the crimes committed and the damages faced by individuals and businesses due to unlawful acts to be transferred to the cyber environment. Hence, in terms of insurance law, the risks that may occur in the virtual world as well as in the real world should be covered. Insurance for this need is cyber risk insurance.

In Turkish law, there is no regulation in the nature of a general condition for cyber risk insurance contracts, which are frequently concluded in practice. This article will discuss the German General Terms and Conditions of Cyber Risk Insurance in order to explain cyber risk insurance due to the similarity of German law to our legal system.

Keywords

•Insurance Contract •Policyholder •Insurer •Cyber Risk •Cyber Security Insurance.

GİRİŞ

Siber risk sigortaları, siber rizikolara karşı sigorta ettireni korumayı amaçlar[1]. Siber risk teriminin anlaşılabilmesi için öncelikle siber sözcüğünün açıklığa kavuşturulmasında fayda vardır. İngilizce-Fransızca "cyber" sözcüğünden Türkçe'ye "siber" olarak aktarılan bu sözcük güncel Türkçe sözlüklerde, "genel ağa veya bilgisayara ait olan" şeklindeki karşılığıyla yer almaktadır[2]. İngilizcede "cyber" kelimesi, bilgisayarlara, bilgi

[1] **TEKİN**, Ufuk: "Hukukî Açıdan Siber Risk Sigortası", Genç Hukukçu Araştırmacılar Sempozyumu, 11-12 Ekim 2019, 2020, İstanbul, s. 675.

[2] https://sozluk.gov.tr/, Erişim Tarihi: 14/5/2024.

teknolojilerine ve sanal gerçekliğe ait olan anlamına gelir[3]. "Siber olay" ise, bilişim ve endüstriyel kontrol sistemlerinin, bu sistemler tarafından işlenen bilginin gizliliğinin, bütünlüğünün ya da erişilebilirliğinin ihlâl edilmesi veya buna teşebbüste bulunulması olarak tanımlanmıştır[4]. Siber saldırı da bilgisayar ortamında yahut internete bağlı mobil cihazlarda[5], bilgi teknolojileri kullanılarak bilgi işlem sistemlerinde saklanan verilere veya doğrudan bu sistemlere yönelik bir saldırıdır[6, 7].

Günümüz Türkiye'sinde, bireyler ve bireylerle kamu veya özel hukuk tüzel kişileri arasındaki hukukî ilişkilere ait veriler büyük oranda dijital ortamlarda saklanmaktadır. Hatta bu tür hukukî ilişkiler kâğıt formundan kurtarılmış olarak doğrudan internet ortamında başlamakta ve bitmektedir[8]. Dijitalleşmenin bu kadar yaygın olması siber saldırıların kişiler ve işletmeler üzerindeki tehlikesini artırmaktadır. Ülkemizde, siber

---

3 New Oxford American Dictionary, (Çevrimdışı Elektronik Sözlük); "cyber" sözcüğünün benzer bir açıklaması için bkz. https://www.duden.de/rechtschreibung/cyber_, Erişim Tarihi: 16/1/2022.

4 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, m. 3/1-e, RG, 11.11.2013/29059.

5 Siber saldırı ve siber güvenlik, çoğu zaman, internete bağlı bilgisayarlar ve bunlarla bağlantılı verilerle ilgili olarak düşünülse de aslında mobil teknolojiler de bunun bir parçası haline gelmiştir. Öyle ki bugün sayısı milyarları bulan akıllı telefonlar ın içindeki bilhassa bankacılık uygulamaları, bilgisayar korsanlarının hedefi haline gelmekte ve bu da bu cihazları da siber güvenlik sigortasının kapsamına sokmaktadır. Akıllı telefonlar yanında, internet teknolojisini kullanan taşınabilir nitelikteki her türlü diğer araç (örneğin, taşınabilir oyun konsolları) da bu bağlamda değerlendirilmelidir.

6 Siber saldırı, siber riske (tehdit) göre daha dar kapsamlı bir kavramdır. Zira siber tehdit, siber saldırı potansiyelini de içeren daha geniş bir anlam ifade eder. Bkz. **CEBECİ**, İpek: "Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme", Üçüncü Sektör Sosyal Ekonomi Dergisi-Third Sector Social Economic Review, S. 2021-56/1, s. 165. Bir kişi ya da işletme için salt siber riskin bulunması, mutlaka bir zararın da ortaya çıkacağı anlamına gelmez. Böyle bir halde, sigorta ettiren rizikonun gerçekleşmesine sebep olabilecek mevcut tehdidi ortadan kaldıracak tedbirleri almalıdır.

7 Siber riskin, işletmelerde bilgi teknolojilerinin kullanımından ve özellikle bu işletmelerin elektronik veri transferi imkânını kullanmasından ileri geldiği yönünde bkz., **SCHEUERMANN**, James E.: "Cyber Risks, Systemic Risks, and Cyber Insurance", Penn State Law Review, S. 2018-122/3, s. 616.

8 Benzer şekilde Almanya'da da bu yöndeki artan eğilimle ilgili değerlendirmeler için bkz., **ERICHSEN**, Sven: "Cyber-Risiken und Cyber-Versicherung: Abgrenzung und/oder Ergänzung zu anderen Versicherungssparten", CCZ-Corporate Compliance, S. 2015-06, s. 247, 248.

saldırıların en çok haberleşme, ulaşım, enerji, bankacılık, finans ve sağlık sektörlerini etkilediği bilinmektedir[9]. Almanya'da da yıllık yaklaşık doksan bin siber saldırının gerçekleştiği[10] ve bu saldırılarda her iki işletmeden birinin mutlaka etkilendiği ve sonuç olarak ülke ekonomisine yıllık yaklaşık elli beş milyar Euro zarar verildiği tahmin edilmektedir[11, 12]. Dünya ölçeğinde, konu daha çarpıcı bir görünüm arz etmektedir. Araştırmalara göre, siber saldırıların dünya genelinde sebep olduğu ekonomik zararların altı trilyon dolar olduğu düşünülmektedir[13].

İşte, işletmelerin siber saldırılara karşı bir acil durum planlarının bulunması ve siber rizikolar gerçekleştiğinde bunlardan olabildiğince az etkilenmeleri hatta mümkünse hiç zarara uğramadan kurtulmaları siber risk sigortasıyla mümkün olabilir[14]. Çünkü, sigorta şirketleri, gerçekleşen zararlar için teminat sağlamalarının yanında sigorta ettirene ve sigortalıya gerekli konularda profesyonel destek de sağlar.

---

9 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), Cumhurbaşkanlığı Genelgesi 2020/15, s. 1, RG, 29.12.2020/31349.

10 Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 9; örneğin 2014 yılında, Almanya'da sadece Ddos atağı şeklinde 32.000 siber saldırı gerçekleşmiştir. Bkz. **ERICHSEN**, s. 248. Ddos atağı, saldırının hedefi olan makinanın (örneğin, bir internet sitesini barındıran sunucunun, makinanın teknik kapasitesinin çok üzerinde iletişim isteğine maruz bırakılarak sonunda çevrimdışı hale gelmesine sebep olan bir siber saldırıdır (https://tr.wikipedia.org/wiki/Servis_dışı_bırakma_saldırısı, Eirişim Tarihi: 15/5/2024).

11 Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 7.

12 Bazı somut olaylarda, sadece bir kötü amaçlı yazılım (örneğin, NotPedya) tüm ekonomik sistem içinde on milyar dolar civarında zarara yol açabilir. Bkz. **MALEK**, Paul/**SCHÜTZ**, Camilla: "Cyberversicherung: Rechtliche und praktische Herausforderungen", r+s – recht und schaden, S. 2019-8, s. 421. Microsoft Windows tabanlı sistemlere saldıran bu şifreleyici kötü amaçlı yazılımla ilgili bilgi için bkz. https://en.wikipedia.org/wiki/Petya_(malware), Erişim Tarihi: 21/1/2022.

13 **FRENCH**, Christopher: "Insuring Against Cyber Risk: The Evolution of an Industry", Penn State Law Review, S. 2018-122/3, s. 608. Özellikle, Amerika Birleşik Devletleri, siber suçların kaynaklandığı ve bu suçların etkilerinin görüldüğü ülkelerin başındadır. Bkz. **VICEVICH**, David L.: "The Case for a Federal Cyber Insurance Program", Nebraska Law Review, S. 2018-97/2, s. 556. Bu sebeple, Amerikan hukukunda konu hukuk gündeminde önemli bir yerdedir. Hatta, biraz da ironik bir şekilde, Birleşik Devletler'de şirketlerin siber saldırıya uğrayanlar ve uğrayacak olanlar olmak üzere ikiye ayrıldığı vurgulanmaktadır. Bkz. **FRENCH**, s. 607.

14 Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 22.

Ülkemizde siber risk sigortalarının uygulaması yaygın olmakla beraber; bu tür sigortalar henüz genel şart düzeyinde bir düzenlemeye konu olmamıştır. Bununla birlikte, Almanya açısından da oldukça yeni olan siber risk sigortaları, Alman hukukunda genel şartla düzenlenmiştir[15]. Bu çalışmada, siber risk sigortaları, Alman Siber Risk Sigortaları Genel Şartları *(Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung, AVBC)* çerçevesinde incelenecektir.

I. SİBER RİSK SİGORTASININ KONUSU VE SİGORTA TÜRLERİ İÇİNDEKİ YERİ

1. Konusu

Siber risk sigortası *(Cyberrisiko-Versicherung)*, siber rizikolar sebebiyle ortaya çıkması muhtemel sonuçlara karşı teminat sağlar[16]. Bu sigorta teminatının konusu, bilgi güvenliğinin ihlâli sebebiyle ortaya çıkan malvarlığı zararlarıdır (AVBC, A1-1). Burada sigorta teminatı, ortaya çıkan tüm zararları değil; Genel Şartlar'da teminat kapsamında olduğu belirtilen zararları kapsar[17]. Ayrıca, bilgi güvenliğinin ihlâli ve ortaya çıkan malvarlığı zararları arasında uygun illiyet bağı bulunmalıdır[18].

Siber risk sigortası teminatı, münferit bir sözleşme ile ya da başka türden bir sigorta sözleşmesi içinde siber rizikolara yönelik klozlar ile sağlanabilir. Örneğin, deniz ticareti hukuku alanında siber rizikolar bu şekilde teminat altına alınabilmektedir[19].

---

15 2010'lu yılların sonu için Alman işletmelerinin % 34'ünün siber risk sigortası ile sigortalı olduğunu belirtilmektedir. Bkz. Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 26.

16 **SELBY**, Judy: "Understanding Cyber Insurance", International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, S. 2011-2/11, s. 21; Rüffer/Halbach/Schimikowski VVG, **ERICHSEN**, Vorbemerkungen, N. 5. Yeri gelmişken belirtmek isteriz ki hem ülkemizde hem de Almanya'da siber risk sigortası isteğe bağlı sigortalardandır. Almanya için bkz. Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 24.

17 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-1, N. 1.

18 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-1, N. 1.

19 **ALGANTÜRK LIGHT**, Didem: "Taşıma Sektöründe Siber Riskler ve Etkileri", Deniz Ticareti Hukukunda Yeni Sorunlar Sempozyumu I, 2019, İstanbul, s. 91.

2. Sigorta Türleri İçindeki Yeri

Siber risk sigortaları zarar sigortalarındandır[20]. Alman hukukunda zarar sigortaları, sigortacının riziko adı verilen bir olayın gerçekleşmesiyle, sigorta ettirenin ya da sigortalının malvarlığının aktif kısmında gerçekleşecek bir azalma ya da pasif kısmında meydana gelebilecek bir artıştan kaynaklanabilecek zararlarını karşılamayı sigorta sözleşmesine göre kararlaştırdığı sigortalardır[21]. Bu sigortalarda, sigorta sözleşmesinde kararlaştırılan sigorta bedeli, sigortacının ediminin üst sınırını oluşturur[22]. Böylelikle bu tür sigortalarda, sadece gerçekleşen (somut) zararların karşılanması amaçlandığından, sigorta tazminatının ödenmesiyle ortaya bir zenginleşmenin çıkması, zenginleşme yasağı kapsamında istenmeyen bir durumdur[23]. Alman hukukunda yapılan ayrıma göre, zarar sigortaları aktifin ya da pasifin sigortası şeklinde yapılabilir[24].

Türk hukukunda da zarar sigortaları, sigortalının para ile ifade edilebilen bir menfaatinde, rizikonun gerçekleşmesiyle ortaya çıkan zararlarının teminat altına alındığı sigortalardır[25]. Türk Ticaret Kanunu (TTK) hükümlerine göre zarar sigortaları mal sigortaları ve sorumluluk sigortaları olmak üzere ikiye ayrılır. Bu açıdan bakıldığında, sigorta sözleşmelerinin tasnifi açısından Alman hukuku ve Türk hukuku açısından büyük benzerlik olduğu görülmektedir. Dolayısıyla, siber risk sigortalarının sigorta türleri arasındaki yeri açısından, (AVBC'de yer alan özel hükümler bir kenara bırakılırsa) Alman hukuku bağlamında yapılacak genel değerlendirmeler Türk hukuku açısından geçerli olacaktır.

Yukarıdaki açıklamalar ışığında değerlendirildiğinde siber risk sigortaları, duruma göre hem mal sigortası hem de sorumluluk sigortası

---

20 **KARAYAZGAN**, Ahmet: Hukuk Gözüyle Siber ve Sigorta, 1. Bası, Aristo, İstanbul, 2021, s. 48.

21 **LORENZ**, Egon: "§ 1. Einführung", içinde: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 3. Auflage, C. H. Beck, 2015, München, N. 83.

22 **HÖRA**, Knut/**SCHUBACH**, Arno: "§ 1 Grundlagen des Privatversicherungsrechts", içinde: Münchener Anwaltshandbuch Versicherungsrecht, Höra/Schubach, 5. Auflage, C.H. Beck, 2022, München, N. 69.

23 **LORENZ**, N. 83.

24 **LORENZ**, N. 84.

25 **AYHAN**, Rıza/**ÇAĞLAR**, Hayrettin/**ÖZDAMAR**, Mehmet: Sigorta Hukuku Ders Kitabı, 3. Bası, Yetkin, Ankara, 2020, s. 9.

özelliği taşıyabilir[26]. Gerçekten bu sigortalarda sigorta ettiren, bir yandan sigortaya konu rizikonun bir siber saldırı sonucu gerçekleşmesiyle uğradığı zararların teminat altına alınmasını sağlar[27]. Diğer yandan sigorta ettiren anılan sigorta ile, sorumluluk sigortası anlamında bir hukukî koruma da talep edebilmektedir. Genel Şartlar'ın A3-1 hükmüne göre siber risk sigortası teminatı, sigorta ettirene sağlanan teminat için gerçekleşmesi gerekli rizikolar çerçevesinde, sigorta ettirenin (rizikonun gerçekleşmesi sebebiyle) zarara uğrayan bir üçüncü kişi tarafından sorumluluk hukuku anlamında dava edilmesi halinde de geçerlidir. Bu ihtimal, sigorta ettirenin veri güvenliğinin ihlâli sebebiyle üçüncü kişilere karşı bir tazminat yükümlülüğü altında kalması durumunda ortaya çıkar[28]. Öğretide "üçüncü taraf riskleri[29]" olarak adlandırılan bu halde, sigorta ettirenin genel hükümlere dayalı tazminat taleplerine karşı korunması sorumluluk sigortalarının özel bir görünümünü oluşturur[30]. Bu yüzden, siber risk sigortaları salt mal ya da sorumluluk sigortası olarak nitelendirilemez; aksine, siber risk sigortaları (sigorta ettirenin talep ettiği hukukî himayeye göre şekillenen) karma bir yapıdadır.

II. BİLGİ GÜVENLİĞİNİN İHLÂLİ KAVRAMI

1. Genel Olarak

Bilgi güvenliğinin ihlâli, sigorta ettirenin elektronik verilerinin veya meslekî faaliyetleri için kullandığı veri işleme sistemlerinin[31]

---

26 **TEKİN**, s. 677.

27 **TEKİN**, s. 677.

28 **ALTUNTAŞ**, Eda/**KARA**, Emine/**SOYLU**, Abdullah Buğra/**KIRKBEŞOĞLU**, Erdem: "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar", Bankacılık ve Sigortacılık Araştırmaları Dergisi, S. 2018-12, s. 13.

29 **ALTUNTAŞ/KARA/SOYLU/KIRKBEŞOĞLU**, s. 13.

30 **FORTMANN**, Michael: "Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen", r+s recht und schaden, S. 2019-8, s. 432; Prölss/Martin VVG, **KLIMKE**, AVBC, A3-1, N. 1; Rüffer/Halbach/Schimikowski VVG, **ERICHSEN**, A3-1, N. 1.

31 Veri işleme sistemi ya da bilgi işlem sistemleri kavramları geniş yorumlanmakta olup; sigorta ettirenin meslekî faaliyetlerinde kullanıldığı müddetçe, bilinen teknolojinin en güncel haline göre bütün bilgi teknolojileri altyapıları bu kapsamdadır. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 8. Bunlara örnek olarak, sunucular, cep telefonları, ağ bağlantılı üretim makineleri ve ağ bağlantılı yazıcılar sayılabilir. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 8. Home Office şeklindeki çalışmalar bakımından özel bilgisayarlar da bu kapsamdadır. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 9. Önemli olan, bu sistemlerin bir siber saldırıdan

kullanılabilirliğinin, *bütünlüğünün* ve *gizliliğinin* ihlâl edilmesidir (AVBC, A1-2.1). Bu açıdan, sigorta ettirenin elektronik verilerinin veya bu verilerin işlendiği sistemlerin, onun derhal müdahale edebileceği bir alanda olup olmamasının ya da sigorta ettirenin *harici* bir servis sağlayıcı kullanmasının önemi yoktur (AVBC, A1-2.2). Dolayısıyla, sigorta ettirenin örneğin mülkiyetinde bulunan ya da kiraladığı bilgi işlem sistemlerinin yanı sıra bu nitelikte olmayan aynı tür sistemler için de siber risk sigortası yapılabilir.

Bilgi güvenliğinin ihlâlini doğuran siber riskler açısından veri, önemli bir kavramdır. Veri, genel anlamda bilgileri ifade eder. Buna göre elektronik veri, elektronik olarak saklanan (örneğin, bir taşınabilir bellek üzerinde ya da Google Drive gibi bir bulut depolama alanında muhafaza edilen) verileri ifade eder[32]. Siber risk sigortası anlamında "veri", yazılım ve programları da kapsamaktadır (AVBC, A1-2.3). Fakat, siber risk sigortası anlamında bilgi güvenliğinin ihlâli kâğıt formundaki verileri değil; elektronik verileri kapsar[33]. Burada, elektronik veri kavramı geniş yorumlanıp yorumlanmayacağı tartışılabilir. Zira veri, doğrudan bilgi işlem sisteminde ya da kendisine doğrudan erişimin bulunmadığı CD ya da DVD gibi materyaller üzerinde de bulunabilir[34]. Alman hukukunda bizim de katıldığımız bir kanaate göre, siber risk sigortası, sadece okunması ve işlenmesi kendisi aracılığıyla sağlanabilen bilgi işlem sistemlerinde saklanan verileri kapsamalıdır[35]. Zira, sigorta ettirenlerin çoğunlukla, ellerinde bulundurdukları verilere ya da çalıştırdıkları bilgi işlem sistemlerindeki en son teknik gelişmelere aşina olmamaları sebebiyle sigorta korumasının kapsamının bu şekilde uygulanması, genel şart hükmünün geniş yorumlanması anlamına gelir[36].

Siber risk sigortalarında rizikonun gerçekleşmesine yol açan olgularla ilgili önceden kesin bir belirleme yapılamaz. Çünkü, bilgi

---

doğrudan etkilenebilir özellikte olmasıdır. Bkz. Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 5.

32 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 3.

33 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 6; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 4.

34 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 3.

35 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 3.

36 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 3.

teknolojileri son derece değişken dinamiklere sahiptir[37]. Ancak, siber riskin genel hatlarıyla tarif edilmesi ve ileride ortaya çıkabilecek teknik gelişmelere göre hukukî ve teknik tedbirler alınması mümkün olabilir. Bu doğrultuda, bilgi güvenliğinin ihlâli sayılan olaylardan bazıları, bir siber saldırı formunda gerçekleşirken (kötü niyetli eylem); bazı rizikoların herhangi bir kasıtlı davranış olmaksızın gerçekleştiği söylenebilir[38]. Özellikle işletmeler bakımından, sigorta teminatının sağlanması borcunu doğuran bu nitelikteki bazı rizikolar aşağıdaki şekilde gösterilebilir[39]:

	İşletme içi	**İşletme Dışı**
Rizikonun Gerçekleşmesine Yönelik Kötü Niyetli Eylemler	a- Aşağıdaki amaçlarla, verilere ve bilgi işlem sistemlerine kötü niyetli çalışanlar tarafından yapılan yetkisiz erişim; *i- Şirkete ait verilerin çalınması, yok edilmesi, şifrelenmesi* *ii- Şirketin bilgi işlem sistemlerine kötü amaçlı yazılımlar veya kodlar yerleştirmek* *iii- Gerçek olmayan işlemler ve hukuka aykırı para transferlerinde bulunmak*. b- Kötü niyetli çalışanların erişim	a- Aşağıdaki amaçlarla, verilere ve bilgi işlem sistemlerine, bilgisayar korsanı *(hacker)* gibi kişilerin yetkisiz erişimi; *i- Yazılım, donanım ya da verilerin çalınması, yok edilmesi, şifrelenmesi* *ii- İşletmenin bilgi işlem politikasını etkilemek için, bilgi işlem sistemlerine kötü amaçlı yazılım yüklenmesi* *iii- Gerçek olmayan işlemler yapılması*

37 **TEKİN**, s. 673.

38 **SCHEUERMANN**, s. 631.

39 Tablolar, **SCHEUERMANN**, s. 631-633'ten (seçilerek ve kısmen tercüme edilerek) naklen alınmıştır. Benzer bir sınıflandırma için bkz. **CEBECİ**, s. 165.

	izni olan alanlarda, bu izinlerini aşacak şekilde işlem gerçekleştirmeleri c- Verilerin hukuka aykırı olarak ele geçirilmesi ve saklanması	*iv- Fidye istenmesi, şantajda bulunulması.* b- Aşağıda sayılan eylemlerin bir neticesi olarak, istem dışı erişilebilir hale gelen verilere erişim, bu verilerin çalınması veya hukuka aykırı olarak ifşa edilmesi; *i- Bir bilgi işlem sisteminin, üçüncü kişilerin müdahalesine açık olacak şekilde yanlış yapılandırılması* *ii- Gizli verilerin şifrelenmeden veya güvenlik altına alınmadan transfer edilmesi.* c- Verilerin muhafaza edildiği bilgi işlem sistemlerine veya internet altyapılarına doğrudan saldırı.

	İşletme İçi	**İşletme Dışı**
Rizikonun Gerçekleşmesine Yönelik İstem Dışı Eylemler ve Durumlar	a- İşletme personelinin kimlik avı dolandırıcılığı gibi dış tehditler sonucu	a- Telefon ya da bilgisayar gibi cihazların kaybedilmesi ya da çalınması.

	operasyonel bir hata yapması. b- İşletmeye ait bir yazılımda ortaya çıkan fonksiyonel hata. c- İşletmenin bilgi işlem altyapısında bulunan ve üçüncü taraf bilgi işlem sistemlerine zarar veren hatalar. d- Haksız rekabet hükümlerine aykırı ya da sınaî mülkiyet haklarını ihlâl edici dijital içerik üretilmesi. e- İşletmenin donanımsal ve altyapısal eksikliklerinin sistem hatalarına yol açması. f- Verilerin istem dışı olarak hukuka aykırı elde edilmesi ve saklanması.	b- Üçüncü kişiler tarafından işletmeye ait bilgi işlem sistemlerine virüs gibi zararlı yazılımların bulaştırılması. c- Tedarik zincirinde virüs bulaşmış ürünlerin işletmeye girmesi. d- Satıcı ya da müşteri gibi kişilerin şirketin kritik verilerini istem dışı paylaşması. e- İşletmenin donanımsal ya da altyapısal bir kusuru bulunmaksızın, genel bir elektrik kesintisi ya da internet ağındaki bağlantı kopukluğunun sistem hatalarına yol açması.

2. Bilgi Güvenliğinin İhlâli Sayılan Olaylar

A. Genel Olarak

Siber risklerin ortaya çıkmasına yol açan hukuka aykırı eylemler, sırf zarar vermeye ve hedefin işletmesel faaliyetlerini sekteye uğratmaya yöneliktir[40]. Ayrıca, işletmelerden veri sızdırılması, fidye istenmesi ya da kişisel menfaatler doğrultusunda kullanmak amacıyla veri çalınması da rizikonun ortaya çıkmasına sebep olabilir[41]. Alman Siber Risk Sigortası Genel Şartları'na göre, siber risk sigortasıyla teminat altına alınan riziko, aşağıdaki olayların gerçekleşmesinden kaynaklanır[42] (AVBC, A1-2.4):

- Elektronik verilere veya bu verilerin işlendiği sistemlere yönelik siber saldırılar.
- Elektronik verilere yetkisiz olarak erişilmesi.
- Bilgi işlem sistemlerine yönelik müdahaleler.
- Sigorta ettirenin bir eylemi ya da ihmâli sonucu, verilerin korunmasına yönelik hukuk kurallarının ihlâli.
- Elektronik verilere ya da bu verilerin işlendiği bilgi işlem sistemlerine yönelik tehdit oluşturan virüs, trojan[43] gibi kötü amaçlı programlar *(malware*[44]*)*.

Aşağıda, bilgi güvenliğinin ihlâli olarak işaret edilen rizikoların verilerin tamamı için gerçekleşmesi ya da sayılan hallerin tamamının birden

---

40 **MEHRBREY**, Kim Lars/**SCHREIBAUER** Marcus: "Haftungsverhältnisse bei Cyber-Angriffen Ansprüche und Haftungsrisiken von Unternehmen und Organen", MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, S. 2016-2, s. 75.

41 **MEHRBREY/SCHREIBAUER**, (n 37) 75, 76.

42 Genel Şartlarda yapılan bu sayım sınırlayıcıdır. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 1. Bununla beraber, teknolojinin gelişimine göre başka rizikolar da siber risk sigortasıyla teminat altına alınabilir.

43 Trojan, kullanıcının bilgisayarına hukuka uygun yazılım kılığında (örneğin, bir ofis programı görünümünde) yüklenerek, bilgisayardaki verilere erişim elde ederek bunu başka bir hedefe aktarmaya yarayan programlara verilen genel bir addır (https://www.kaspersky.com.tr/resource-center/threats/trojans, Erişim Tarihi: 17/5/2024).

44 Malware, İngilizce *malicious software* (Türkçe, *kötü amaçlı yazılım*) kelimelerinin kısaltılmasından oluşan ve hukuka aykırı işlevleri olan bilgisayar programlarını ifade eden bir kavramdır. Bu yazılımlar, bilgisayarlarda istenmeyen reklamları göstermek, yetki bulunmayan verilere erişim sağlamak ya da bilgisayar veya mobil cihazların fonksiyonlarını bozmayı amaçlar (https://tr.wikipedia.org/wiki/Malware, Erişim Tarihi: 17/5/2024).

gerçekleşmesi gerekli değildir. Sigorta sözleşmesi bağlamında rizikonun gerçekleşmesi için olasılıklardan birinin verilerin bir kısmı için gerçekleşmesi yeterlidir[45].

B. Verilerin ve Sistemlerin Kullanılabilirliği, Bütünlüğü ile Gizliliği

Siber risk sigortasının teminat altına aldığı riziko, verilerin ve sistemlerin kullanılabilirliğinin, bütünlüğünün veya gizliliğinin zarar görmesidir. Verilerin ve bilgi işlem sistemlerinin *kullanılabilirliği*, sigorta ettirenin istediğinde bu verilere ulaşabilmesi ve bilgi işlem sistemlerinin amacına uygun olarak kullanabilmesidir[46]. Aşağıdaki hallerde verilerin veya sistemlerin kullanılabilirliği zarar görmüş ve riziko gerçekleşmiş demektir[47]:

- Verilerin sigorta ettirenin rızası dışında silinmesi.
- Verilerin sigorta ettirenin rızası dışında şifrelenmesi[48].
- Verilerin geçici veya sürekli olarak okunamaması.
- Bilgi işlem sistemlerinin arızalanarak fonksiyonlarını yitirmesi.

Verilerin ve bilgi işlem sistemlerinin *bütünlüğü*, bunların eksiksiz veya değiştirilmemiş olmasını gerektirir[49]. Bir veri yetkisiz olarak değiştirildiğinde veya bir bilgi işlem sistemine kötü amaçlı yazılım yüklendiğinde verilerin bütünlüğü bozulur[50]. Diğer bir ifadeyle, verilerin takip edilemeyecek şekilde değiştirildiği durumlarda verilerin bütünlüğünün bozulmasından söz etmek mümkündür[51].

---

45 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 4.

46 **MALEK**, Paul/**SCHILBACH** Dan: "Versichertes Risiko in der Cyber-Versicherung – Umfang und Grenzen des Deckungsschutzes", VersR-Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht, S. 2019-21, s. 1322; Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 3; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 12.

47 **MALEK/SCHILBACH**, s. 1322; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 12.

48 Uygulamada, özellikle muhasebe işletmelerinin sistemlerine yönelik siber saldırılarda mükelleflerin işletme ve şirketlerine ait verilerin şifrelendiği; ardından, bu şifrelerin çözülmesi karşılığında fidye istendiği bilinmektedir. Siber risk sigortası burada önemli bir ihtiyaca cevap vererek, verilere erişimin kaybolmasından doğan zararların giderilmesini sağlar. Bkz. **CEBECİ**, s. 66.

49 **MALEK/SCHILBACH**, s. 1322; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 13.

50 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 13.

51 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 3.

Verilerin *gizliliği*yle kastedilen, yetkisiz erişime karşı korunmadır[52]. Bir kişinin yetkisi bulunmadığı halde, gizli tutulması gereken verileri sadece okuması dahi rizikonun gerçekleşmesi demektir[53]. Bu noktada verilerin gizliliğinin bozulması açısından, verilere ulaşan kişinin kasıtlı hareket edip etmediği önem taşımaz[54]. Bu yüzden, verilerin gizliliğinin sağlanması bu verilere sadece yetkili kişilerin erişebilmesini ve veriler üzerinde çalışabilmesini gerektirir[55].

Rizikonun gerçekleşmesi için bu üç halden birinin ortaya çıkması (verilerin kullanılabilirliğinin, bütünlüğünün ya da gizliliğinin zarar görmesi) yeterlidir. Bununla beraber, sayılan olasılıklardan birinin gerçekleşmesi diğerlerinin gerçekleşemeyeceği anlamına gelmez[56]. Aksine, tipik bir siber saldırıda, sayılan her üç bilgi güvenliği ihlâlinin tamamı ya da bir kısmı gerçekleşmektedir[57]. Örneğin, kötü amaçlı bir yazılımın sigorta ettirenin bilgi işlem sistemlerine girmesi durumunda, bazı verilerin yok edilmesi ve başka bir bulut depolama alanına taşınması durumunda hem gizlilik hem de kullanılabilirlik zarar görür. Ayrıca, siber rizikonun gerçekleşmiş sayılması için mutlaka verilerin tamamen yok olması ya da bilgi işlem sisteminin tamamen çalışamaz duruma gelmesi aranmaz; kısmî fonksiyon ya da veri kaybı sonucu zarara uğranması da rizikonun gerçekleşmiş sayılması için yeterlidir[58].

3. Meslekî Kullanımın Gerekliliği

Sigorta teminatının kapsamı açısından, verilerin ya da bilgi işlem sistemlerinin sigorta ettirenin meslekî veya ticarî faaliyeti için kullanılıyor olması şarttır[59]. Diğer bir ifadeyle, sadece kişisel kullanıma özgü veriler ve sistemler siber risk sigortası kapsamında teminat altına alınmamıştır[60]. Bununla beraber, bazı sistem ve gereçlerin hem kişisel hem de meslekî

---

52 **MALEK/SCHILBACH**, s. 1322; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 14.

53 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 14.

54 **MALEK/SCHILBACH**, s. 1322.

55 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 3.

56 **MALEK/SCHILBACH**, s. 1322.

57 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 15; **MALEK/SCHILBACH**, s. 1322.

58 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 15; Benzer yönde bkz. **TEKİN**, s. 679.

59 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 7.

60 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 5; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 10.

veya ticarî amaçlar için kullanılması mümkündür. Örneğin, bir çalışanın kişisel bilgisayarını şirketteki görevleri kapsamında da kullanıyor olması mümkündür. Bu halde, siber risk sigortası teminatı kısmî işletmesel kullanımlar için de geçerlidir[61].

4. Harici Servis Sağlayıcıların Kullanılması

Harici servis sağlayıcı, sigorta ettirenin işletmesindeki bazı işleri yürütmede veya iş süreçlerini yönetmede dışarıdan yardım aldığı diğer bir işletmedir[62]. Örneğin, bir işletmenin müşterilerine ait verilerin saklandığı *(iCloud, Google Drive gibi)* bulut depolama alanları ya da haberleşmenin gerçekleştirilmesinde kullandığı *(Gmail, Outlook gibi)* bir e-posta hizmeti bu anlamda harici servis sağlayıcıdır. Yine, bir işletmenin güvenlik amacıyla, faaliyette bulunduğu mekanlarda kullandığı internet bağlantılı güvenlik kamera sistemlerini kuran ve bakımını yapan bir şirket de harici servis sağlayıcıdır.

AVBC, A1-2.2, ilk cümleye göre siber risk sigortası teminatı, sigorta ettirenin harici bir servis sağlayıcı kullanması durumunda da geçerlidir. Ancak sigorta teminatı, harici servis sağlayıcı tarafından sunulan hizmette bir arızanın ortaya çıkması ya da bu hizmetin kesilmesi gibi durumları kapsamaz. Burada teminat kapsamı sınırlandırılmaktadır. Zira böylelikle, örneğin bir bulut depolama alanını yöneten şirkete yönelik siber saldırılarda olduğu gibi, birçok başka şirketi etkileyebilecek böyle bir saldırının dolaylı sonuçlarının sigorta şirketini, altından kalkamayacağı tazminat yükümlülükleri ile karşı karşıya bırakmaması hedeflenmektedir[63]. Aksinin kabulü, sigorta sözleşmesiyle sigortacının harici servis sağlayıcının sigorta ettirene karşı edimini de temin etmesi anlamına gelir[64] ki bu şekilde bir rizikonun öngörülemeyecek sonuçları olduğu kuşkusuzdur.

---

61 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 10; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 8.

62 **MALEK/SCHILBACH**, s. 1327.

63 **MALEK/SCHILBACH**, s. 1327; Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 15; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 16.

64 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 16.

III. BİLGİ GÜVENLİĞİNİN İHLÂLİ BAKIMINDAN TEMİNAT ALTINA ALINAN RİZİKOLAR

1. Temel İlkeler

Riziko, sigorta sözleşmesi çerçevesinde sigortacının ödeme yükümlülüğünün doğmasına sebep olan gerçekleşmesi şüpheli bir olaydır[65]. AVBC, A1-4/I anlamında riziko ise, genel şartların "sigortanın konusu" başlıklı A1-1 hükmünde öngörülen tespit edilebilir ve doğrulanabilir malvarlığı zararlarının gerçekleşmesidir[66]. Alman hukukunda bu zarar, sigorta sözleşmesinin hüküm ve sonuçlarını ifade ettiği zaman dilimi içerisinde gerçekleşmiş olmalıdır (AVBC, A1-4/II).

Bahsedilen rizikoların gerçekleşmesiyle sigorta teminatının sağlanması, bir malvarlığı zararına uğranılmış olmasına, daha açık bir ifadeyle *fiilî zarar*ın varlığına bağlıdır[67]. Aksine, zararın gerçekleşmiş olabileceği yönündeki salt şüphe yeterli değildir[68]. Zarar, tespit edilebilir olmalıdır[69, 70]. AVBC A1-4'e göre, zararın varlığı konusundaki tespit, yeniden gözden geçirmeye imkân verecek şekilde kontrol edilebilir olmalıdır. Ayrıca, bilgi güvenliğinin ihlâline yol açan vakıanın (örneğin bir siber saldırının) değil; aksine sadece zararın tespit edilebilir olması gerekir[71].

---

65 **KARA**, Hacı, Sigorta Hukuku, Oniki Levha, İstanbul, 2021, s. 47; **YAZICIOĞLU**, Emine/**ŞEKER ÖĞÜZ**, Zehra: Sigorta Hukuku, 3. Bası, Filiz, İstanbul 2020, s. 74; **AYHAN/ÇAĞLAR/ÖZDAMAR**, s. 136.

66 Siber risklere çok sayıda örnek verilebilir. Bu konuda Alman Allianz sigorta şirketinin yaptırdığı bir araştırmaya göre siber risk sigortasıyla teminat altına alınan rizikolar nitelikleri itibariyle üç kategoridir: *Teknik hatalar* (donanım ve yazılım bakımından uygun olmayan araçların kullanılması, özellikle eski ve uyumsuz yazılımların kullanılması); *Operasyonel hatalar* (donanım ve yazılımın yanlış kullanımı, bir yazılımın yanlış yüklenmesi, yazılımcı hataları); *Siber saldırılar* (kötü amaçlı yazılımlar ya da bilgi işlem sistemlerine yetkisiz erişim), Allianz Risk Barometer, Top Business Risks for 2019, 12 vd., https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf, Erişim Tarihi: 25/5/2022.

67 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 4.

68 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 4.

69 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 5.

70 Siber rizikolara karşı önceden tüm olasılıkları öngörerek tedbir almak ve özellikle işletme içi tehditler (örneğin huzursuz çalışanlar) dolayısıyla, bir siber saldırı gerçekleştiğinde nasıl bir zarar gerçekleşeceğini önceden kesin olarak belirlemek güçtür. Bkz. **CEBECİ**, s. 165.

71 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 6.

Yoksa, bilgi güvenliğinin ihlâline yol açan sebebin başlangıçta ne olduğunun bilinmemesi, sigorta teminatının sağlanmasına engel değildir[72].

Zararın varlığı konusundaki tespiti, sigorta ettiren veya rizikonun gerçekleşmesiyle zarara uğrayan kişi ya da bir üçüncü kişi yapabilir[73]. Rizikonun gerçekleştiği ve bu olgunun aşağıda sayılacak vakıalara dayandığı yönündeki ispat yükü sigorta ettirenin üzerindedir[74].

2. Siber Risk Sigortası Bakımından Riziko Çeşitleri

Siber risk sigortasında rizikonun gerçekleşmesine yol açabilecek tehditler, kısa ve uzun vadeli tehditler olarak sınıflandırılabilir[75]. Kısa vadeli tehditler, kişi veya kurumların günlük faaliyetlerini etkilemeye yönelik dolandırıcılık, kimlik hırsızlığı gibi siber eylemlerdir[76]. Uzun vadeli tehditler de (millî güvenliğe tehdit oluşturan saldırılarda olduğu gibi) etkileri daha uzun müddet zarfında gözlenebilir olan ve daha geniş bir alanda (örneğin daha geniş insan topluluklarını etkileyen) etkisini gösteren tehditlerdir[77]. AVBC, A1-2.4 bendinde ise, bilgi güvenliğinin ihlâli oluşturan haller teminat altına alınmıştır. Bunlar, sigorta ettirenin bilgi güvenliği sistemlerine saldırı, sigorta ettirenin elektronik verilerine yetkisiz erişim, sigorta ettirenin bilgi işlem sistemlerine yapılan yetkisiz müdahaleler, bir yapma ya da yapmama şeklindeki fiil ile birlikte sigorta ettirenin verilerin korunmasına dair hükümlere aykırı davranmasına yol açmak, sigorta ettirenin verilerine ya da bilgi işlem sistemlerine zarar veren kötü amaçlı yazılım üretmek ve bunları çalıştırmaktır. Bu sayım sınırlayıcı olmakla birlikte[78], bir siber saldırının aynı zamanda birden fazla rizikonun[79] ortaya çıkmasına sebep olması da olasıdır. Dolayısıyla, yapılan sınırlayıcı sayıma dair olguların birbirinden soyut olarak ortaya çıkması

---

72 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 6.

73 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-4, N. 7.

74 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 27.

75 **CEBECİ**, s. 165.

76 **CEBECİ**, s. 165.

77 **CEBECİ**, s. 165.

78 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 18; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 26.

79 AVBC, A1-2.4 hükmünde belirtilmiş olaylar bu rizikolara örnek olarak gösterilebilir.

şart değildir[80]. Önemli olan, rizikonun gerçekleşmesiyle yapılan siber saldırı arasında uygun illiyet bağının bulunmasıdır[81].

Bilgi güvenliğine yönelik *saldırı*nın bilinçli bir eylem sonucu gerçekleşmiş olması gerekli olup; bunun için özel olarak bir malvarlığı zararının ortaya çıkması amacıyla hareket etmek şart değildir[82]. Bilgi güvenliğine zarar vermek için yapılan siber saldırı, belirli bir kişiye ya da kişi grubuna yönelmiş olabilir. Fakat bu şart değildir. Aksine, fidye talebine yönelik kötü amaçlı bir yazılımın internet ortamındaki lisanssız yazılımlara entegre edilmesinde olduğu gibi belirli olmayan bir kişi çevresine yönelik tehdit de mümkündür[83]. Bunun gibi, bilgi işlem sisteminin şifre ve veri çıkarılması amacıyla gözetlenmesi de rizikonun gerçekleşmesini tetikleyici bir saldırıdır[84]. Örneğin, bir siber saldırı sonucu internet hatlarında yaşanan kesintinin radar iletişimini etkilemesi ve bunun sonucunda bir çatma olayının yaşanmasında da bir (siber) saldırının varlığından pekâlâ söz edilebilir[85].

Sigorta ettirenin verilerine *yetkisiz erişim*, bu verilerin kopyalanması, başka bir veri taşıyıcıya aktarılarak taşınması ya da sadece bu veriler üzerinden not alınmasıyla gerçekleşebilir[86]. Yetkisiz erişim ile verilerin gizliliği ihlâl edildiğinden; ayrıca verilerin bütünlüğü ya da kullanılabilirliğinin de zarar görmesi şart değildir[87]. Ancak, verilere her türlü erişim, rizikonun gerçekleştiği anlamına gelmez. Aksine, erişimin yetkisiz olması gerekir. Yetkisiz erişim, erişim sağlayan kişinin hiçbir surette böyle bir yetkisinin olmamasından ileri gelebileceği gibi; yetkinin aşılması suretiyle de gerçekleşebilir[88]. Örneğin, sigorta ettirenin bir çalışanının yetkisini aşarak erişiminin mümkün olduğu verilere ulaşması, bunları

---

80 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 27.

81 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 18; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 28.

82 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 19; Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 29.

83 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 29.

84 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 19.

85 **ALGANTÜRK LIGHT**, s. 83.

86 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 30.

87 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 30.

88 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 31.

herhangi bir şekilde kullanması ya da sızdırılmasına sebep olması halinde durum böyledir[89, 90]. Burada, yetkisiz erişimde bulunan kişinin kusurlu olması şart değildir[91]. Ancak, rizikonun gerçekleşmesine yol açan eylemde kusur da bulunabilir. Örneğin, taşımacılık yapan bir kara taşıtının GPS sistemine yapılan bilinçli bir saldırı sonucu eşyanın tesliminde yaşanan gecikmelerden doğan zararlar için siber risk sigortası teminatı sağlanmış olabilir[92].

Sigorta ettirenin bilgi işlem sistemlerine yapılacak bir *yetkisiz müdahale* için de somut bir eylem gerekmektedir[93]. Örneğin, bir bilgisayar korsanının trafikte otonom olarak seyreden bir aracı işletene zarar verme kastıyla trafik altyapısına müdahale etmesi ve sonuç olarak bir zararın ortaya çıkması halinde bir yetkisiz müdahale söz konusudur[94]. Yine, otonom ya da internet teknolojisini kullanarak seyreden bir geminin -söz gelimi- Süveyş Kanalı'ndan geçerken devre dışı, çalışamaz duruma getirilmesi halinde hem doğrudan etkilenen gemiyi işleten kişinin hem de kanaldaki muhtemel tıkanıklık sebebiyle yaşanan gecikmelerden ötürü diğer kişilerin zararları ortaya çıkabilir[95]. Örneklerdeki gibi bilinçli müdahaleler dışında, doğa olayları sebebiyle ortaya çıkan elektrik kesintileri gibi aksaklıklar sigorta kapsamında değildir[96]. Yetkisiz müdahalenin rizikonun gerçekleşmesine sebep olmasındaki insan davranışının kasıt ya da

---

89 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 31; Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 20.

90 Almanya'da yapılan bir araştırmaya göre, siber saldırılar sonucu rizikonun gerçekleşmesinde etkili olan kişilerin yaklaşık %52'si, işletmenin halihazırdaki ya da eski çalışanlarıdır. Bu araştırmaya göre, organize suç şebekelerinin siber saldırılarda aldığı rol %11'de kalmaktadır. Bkz. Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 16.

91 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 31.

92 **ALGANTÜRK LIGHT**, s. 85.

93 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 32.

94 **BUĞRA**, Ayşegül: "Otomatik Yönlendirme Seviyesi Yüksek Kara Araçları ve Sigorta", Galatasaray Üniversitesi Hukuk Fakültesi-Sigorta Hukukunun İki Güncel Sorunu: İnsansız Araçlar, Sorumluluk ve Özel Sağlık Sigortalarında Birden Çok Sigorta Sempozyumu-18 Ocak 2019, Ed. Serap Amasya, 2020, İstanbul, s. 28.

95 **KARA**, Hacı: "Gemilerde Yapay Zekâ Kullanımı ve Buna Dair Hukuki Sorunlar", **Süleyman Demirel Üniversitesi Hukuk Fakültesi**, S. 2020-10/1, s. 27.

96 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 33.

ihmal ile ortaya çıkması önemli değildir[97]. Bu konuda bir görüşe göre, hatalı veya kötü amaçlı bir yazılım ya da donanımın bilgi işlem sistemine bağlanması sonucu ortaya çıkan zararlar da bilgi güvenliğinin ihlâli kapsamında sayılır[98]. Öğretide diğer bir görüşe göre ise, rizikonun gerçekleşmesi sonucu ortaya çıkan zarar bir kişiden değil de doğrudan hatalı bir yazılımdan kaynaklanmış ise, burada genel şartlar anlamında yetkisiz müdahale yoktur. Bu sebeple, siber risk sigortası bağlamında teminat altında olan bir rizikodan da söz edilemez[99]. Kanaatimizce, burada ikili bir ayrım yapılmak suretiyle ilk görüşe üstünlük tanımak gereklidir. Eğer, verilere ve bilgi işlem sistemlerine saldırı veya buralarda saklanan verilerin gizliliğinin ihlâli sistemin bir parçası sayılan yazılımlardaki fonksiyon eksikliğinden kaynaklanıyorsa sigorta teminatı söz konusu olmamalıdır. Buna karşılık, verilerin kullanılabilirliği, gizliliği ve bütünlüğü bir kötü amaçlı yazılım sebebiyle bozulmuşsa bu dışsal tehdide karşı sigorta teminatı sağlanmalıdır.

Siber risk sigortası anlamındaki bir diğer riziko, sigorta ettirene atfedilebilecek, *bilgi güvenliğini korumaya yönelik hükümlerin ihlâli* dir. İhlâl için gerekli olan, sigorta ettirenin yapma ya da yapmama şeklinde gerçekleşen kasıtlı veya ihmali fiilidir[100]. Örneğin, müşterilere ait gizli kalması gereken bilgilerin sigorta ettirene isnat edilebilecek bir eylem veya ihmâl sonucu hukuka aykırı olarak aleniyet kazanmasında durum böyledir[101]. Burada rizikoya sebep olan olgu, bir insan eylemi olup, kasıt ya da ihmâl ile ortaya çıkabilecek bu eylem, sigorta ettirenin gerekli tedbirleri almaması dolayısıyla icra edilebilmektedir[102]. Gerekli tedbirlerin alınmaması, işletmesel süreçlerin kişisel verilerin korunmasına dair mevzuata uygun hale getirilmemesinden ileri gelebilir[103,104]. Dolayısıyla, tüm dünyada

---

97 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 34.

98 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 35.

99 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 21.

100 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 24.

101 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 36.

102 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 37.

103 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 23.

104 Örneğin, yakın geçmişte, yemeksepeti.com isimli şirketin yaklaşık 22 milyon müşterisine ait verileri bir siber saldırı sonucu çalınmıştır. Şirket tarafından yapılan savunmada, bu veri gizliliği ihlâlinin "Yemek Sepetine ait bir web uygulama sunucusu

kabul edildiği üzere, müşterilerinin verilerini bilgi işlem sistemlerinde taşıyan, bu verileri kullanan işletmeler bu bilgilerin korunması ve gizli kalmasından da sorumludur. Bu anlamdaki tazminat sorumluluğuna ilave olarak, siber saldırıya uğrayan işletmeler, siber saldırının dolaylı etkileriyle karşılaşabilecek müşterilerini (ve kamuoyunu) saldırıdan haberdar etmeli, yetkili makamların konu ile ilgili yürüttüğü soruşturmalara yardım etmelidir[105].

Siber risk sigortasında rizikonun gerçekleşmesine yol açacak *kötü amaçlı yazılım*, üçüncü kişilerin verileri ve bilgi işlem sistemleri üzerinde istenmeyen değişikliklerin ortaya çıkmasına yol açan programlardır[106]. Dolayısıyla, burada rizikonun gerçekleşmesi doğrudan bir insana bağlı bir davranışı gerektirmemektedir[107].

3. Siber Risk Sigortasının Öncelikli Olarak Uygulanması

Bir siber riziko için birden fazla sigorta sözleşmesi ya da bu sözleşmelerde yer alan klozlar ile aynı zamanda teminat sağlanması ihtimaller dâhilindedir. Örneğin, bir tacir işletmesi için bir sigortacıyla (siber rizikoları da -bir ilave kloz ile- teminat altına alan) mesleki sorumluluk sigortası yaptırmış ve ardından, bu kez başka bir sigortacıyla, işletmesindeki bazı veya bütün siber rizikolar için ticarî siber risk sigortası sözleşmesi de akdetmiş olabilir. Siber risk sigortalarında bu ihtimal Genel Şartlar'da öngörülmüştür. Genel Şartlar'ın A1-12 hükmüne göre, bir siber riziko için AVB-Cyber anlamında bir poliçeye ek olarak başka bir poliçe ile de teminat sağlanmışsa, siber risk sigortasına ilişkin kurallar çerçevesinde zarar öncelikle siber risk sigortası kapsamında karşılanır.

Genel Şartlar A1-12'in bir amacı, aynı konuya ilişkin birbirinden farklı iki sözleşmenin çelişen hükümler içermesi sebebiyle ortaya

---

üzerinde bir açıklık bulunmasından ve bu açıklıktan yararlanılarak, uygulama kurulmasından ve komut çalıştırılmak suretiyle sunucuya erişilebilmesinden" ileri geldiği açıklanmıştır, https://www.kvkk.gov.tr/Icerik/6936/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Yemek-Sepeti-Elektronik-Iletisim-Perakende-Gida-Lojistik-AS, Erişim Tarihi: 28/12/2021; Ayrıca, konunun basında bulduğu yer ile ilgili örnek olarak bkz. https://shiftdelete.net/binlerce-yemeksepeti-kullanicisinin-verileri-calindi-iddiasi, Erişim Tarihi: 28/12/2021.

105 **FRENCH**, s. 609.

106 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-2, N. 38.

107 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-2, N. 25.

çıkabilecek hukukî güvenlik ilkesine aykırı belirsizliklerin önüne geçmektir[108]. Aynı zamanda bu kural ile, rizikonun gerçekleşmesi ihtimalinde sigortacıyı sürece olabildiğince erken dâhil etmek olanaklı olur[109]. Sigortacının sürece mümkün olan en kısa sürede katılmasıyla birlikte sigorta ettiren, zararın artmasının engellenmesi konusunda profesyonel bir desteğe kavuşur[110]. Dolayısıyla, AVBC A1-12 sigorta ettirenin menfaatinedir[111]. Hükmün amacı ve bu niteliği göz önünde bulundurulduğunda, birden fazla sigortacının aynı siber rizikonun gerçekleşmesiyle ortaya çıkan zararı birlikte karşılamasının yasaklanmamış olduğu sonucu da çıkarılabilir[112]. Ancak, sigorta hukukunun temel prensiplerinden olan zenginleşme yasağı burada da uygulama alanı bulur.

IV. SİGORTANIN KONUSU OLARAK MALVARLIĞI ZARARLARI

1. Genel Olarak

Zarar sigortalarında (ve bu kapsamda siber risk sigortalarında) sigortacının tazminat ödeme yükümlülüğünün doğması için sadece rizikonun gerçekleşmesi gerekmez; aynı zamanda bir zararın da ortaya çıkması gerekir[113]. Rizikonun, söz gelimi bilgi işlem sistemlerine yönelik bir siber saldırının gerçekleşmesine rağmen, güvenlik duvarı sayesinde bu saldırı zarara uğramaksızın atlatılmışsa, sigortacı tazminat ödemez[114]. Bu anlamda zarar, bir kişinin (sigorta ettirenin) malvarlığının, zarara yol açan olay (riziko) gerçekleşmeseydi içinde bulunacağı durum ile mevcut durumu arasındaki farktır[115]. Genel Şartlar ise, malvarlığı zararlarını

---

108 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-12, N. 1.

109 **SCHILBACH**, Dan: "Die Musterbedingungen des GDV für die Cyberrisiko-Versicherung", SpV-Spektrum für Verischerungsrecht, S. 2018-1, s. 3; Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-12, N. 3.

110 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-12, N. 3.

111 **ACHENBACH**, Matthias: "Die Cyber-Versicherung – Überblick und Analyse", VersR-Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht, S. 2017-24, 2017, s. 1498.

112 **ACHENBACH**, s. 1498.

113 **AYHAN/ÇAĞLAR/ÖZDAMAR**, s. 11.

114 **AYHAN/ÇAĞLAR/ÖZDAMAR**, s. 11.

115 **ANTALYA**, Osman Gökhan: Marmara Hukuk Yorumu-Borçlar Hukuku Genel Hükümler Cilt V/1, 2, 2. Bası, Seçkin, Ankara, 2019, s. 458; **DOĞAN**, Murat/**ŞAHAN**,

olumsuz bir sayım yaparak tanımlamıştır. Buna göre, sigorta teminatı kapsamındaki malvarlığı zararları; ölüm, yaralanma ya da insan sağlığının herhangi bir şekilde zarar görmesi gibi kişisel zararlar yahut hasar veya eşyanın zıyaı gibi eşyaya bağlı zararlar veya bu tür zararlarla doğrudan bağlantılı *olmayan* zararlardır (AVBC, A1-3/I).

Kapsam dışı tutulan zararlar, aynı zamanda sigorta teminatının dışındadır. Zira, genel şartların ilk maddesi, (aslında AVBC, A1-3/I'de tanımlanan) malvarlığı zararlarının sigorta teminatı içinde olduğunu belirtmektedir. Ayrıca, elektronik veriler, genel şartlar kapsamında eşya sayılmaz. Her ne kadar bir eşyanın doğrudan uğradığı zararlarla bağlantılı zararlar AVBC, A1-3/I anlamında sigorta teminatı içinde sayılmasa da eşyanın yok olması sonucu veri kaybı sigorta teminatı içindedir (AVBC, A1-3/II). Görüldüğü üzere Genel Şartlar, yalnızca saf malvarlığı zararlarının teminat altına alınmasını öngörmektedir[116]. Bunun dışında, kişisel ya da eşyaya bağlı zararlar ile bunlarla bağlantılı dolaylı zararlar teminat kapsamında olan zararlar değildir[117].

2. Sigorta Teminatı İçinde Yer Alan Malvarlığı Zararları ve Eşya Kavramı

Klasik anlamda eşya, kişiliğin unsurları ile bağlantısı bulunmayan, para ile ölçülebilir bir değer üzerinden ifade edilebilen, üzerinde fiilî veya hukukî hakimiyet kurulabilen maddî varlıktır[118]. Elektronik verilerin ise, Genel Şartlar anlamında eşya olmadığı özellikle belirtilmiştir; çünkü, aksinin kabulünde, bir siber risk sigortası sözleşmesinden beklenen yarar sağlanamaz[119]. Zira elektronik verilerin eşya kavramına dâhil kabul edilmesi, tipik bir siber saldırı sonucunda zarar görecek unsurların kapsamının oldukça daraltılmış olmasından dolayı sigorta teminatını zayıflatır[120].

Gökhan/**ATAMULU**, İsmail: Borçlar Hukuku Genel Hükümler, 2. Bası, Seçkin, Ankara, 2021, s. 201.

116 **ACHENBACH**, s. 1497; **SCHILBACH**, s. 3.

117 **ACHENBACH**, s. 1497; **SCHILBACH**, s. 3.

118 **AYAN**, Mehmet: Eşya Hukuku I-Zilyetlik Tapu Sicili, 13. Bası, Seçkin, Ankara, 2016, s. 40; **ANTALYA**, Osman Gökhan/**TOPUZ**, Murat: Marmara Hukuk Yorumu-Eşya Hukuku Cilt: IV/1, 3. Bası, Seçkin, Ankara, 2019, N. 38.

119 Prölss/Martin VVG, **KLIMKE**, AVBC, A.1-3, N. 2.

120 Prölss/Martin VVG, **KLIMKE**, AVBC, A.1-3, N. 2.

Genel şartlarda sigorta teminatı bir başka açıdan daha genişletilmiştir. Buna göre, bir eşyanın yok olması veri kaybına yol açıyorsa bu durumda da sigorta teminatı vardır. Örneğin, bir USB belleğin kaybolması ya da bilgisayarın çalınması durumunda, bu veri taşıyıcılardaki verilere erişim sağlanamamasında durum böyledir[121]. Ancak, bir veri taşıyıcının fiziksel olarak parçalanması veya yok edilmesi sonucu veri kaybı yaşanırsa sigorta teminatı yoktur[122]. Yine, bir eşyanın yok olması sonucu yaşanan iş kesintisi gibi dolaylı sonuçlar da sigorta teminatı dışındadır[123].

V. SÖZLEŞME SONA ERDİKTEN SONRA SİGORTACININ SORUMLULUĞU

Siber risk sigortası genel şartlarına göre (AVBC, A1-5), bazı durumlarda sigorta ilişkisi sona ermesine rağmen sigorta teminatı devam eder[124]. Özellikle, rizikonun gerçekleşmesiyle zararın ortaya çıkması arasında geniş bir zaman dilimi varsa, sonraki sorumluluğun kabul edilmesi işlevseldir[125]. Sigortacının sözleşmenin sona ermesinden sonraki sorumluluğunun kabulü için, sigorta ettirenin rizikonun gerçekleştiğini bilmiyor olması gerekir[126]. Bu doğrultuda, sigorta ilişkisinin, teminat altına alınan rizikonun tamamen ya da kalıcı olarak sona ermesi sebebiyle veya bu ilişkinin sigortacı ya da sigorta ettiren tarafından sona erdirilmesi

---

121 Prölss/Martin VVG, **KLIMKE**, AVBC, A.1-3, N. 3.

122 Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-3, N. 3; Prölss/Martin VVG, **KLIMKE**, AVBC, A.1-3, N. 4. Bu özellikteki bir veri taşıyıcının kötü amaçlı bir yazılım sebebiyle fizikî olarak zarar görmesi de eşyaya bağlı bir zarar niteliğinde olup; sigorta teminatı dışındadır. Bkz. Rüffer/Halbach/Schimikowski VVG, **PAWIG-SANDER**, A.1-3, N. 1.

123 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-3, N. 4.

124 Genel Şartların bu hükmü, amacı bakımından TTK m. 1484/2 hükmüne benzer. Anılan TTK hükmüne göre, sigorta ilişkisinin sona ermesi, zarar görene karşı ancak, sigortacının sözleşmenin sona erdiğini veya ereceğini yetkili mercilere bildirmesinden bir ay sonra hüküm doğurur. Sorumluluk sigortaları bakımından sigortacının rizikoyu taşıma yükümlülüğünün süre bakımından kapsamını artıran bu kural, zarar göreni korumayı hedefler. Bkz. **ÜNAN**, Cilt II, s. 424; **HACIÖMEROĞLU**, Abdülhamid Oğuzhan: "Zorunlu Sorumluluk Sigortacısının Sonraki Sorumluluğu", BATİDER, S. 2020-36/2, s. 167.

125 **MALEK/SCHÜTZ**, s. 426.

126 **MALEK/SCHÜTZ**, s. 426.

halinde[127] sigorta teminatı bazı koşullarla, gerçekleşen zararlar bakımından devam eder. Bunun için, sigorta sözleşmesinin geçerli olduğu zaman dilimi içinde bir bilgi güvenliğinin ihlâli gerçekleşmiş olmalıdır. Fakat, sigorta ilişkisi sona erdiği anda henüz tespit edilememiş malvarlığı zararları için söz konusu sonuç, aşağıdaki koşullarda ve ölçüde geçerlidir:

- Sigorta teminatı, sigorta ilişkisinin sona erdirildiği andan itibaren başlamak üzere, sigorta poliçesinde kararlaştırılan süre boyunca devam eder.

- Sigorta teminatı, sigorta ilişkisinin sona erdirilmesine dair şartlar çerçevesinde sözleşmenin sonra ermesinden sonraki sorumluluk için belirlenen zaman dilimi boyunca da geçerlidir. Ancak bu teminat, sigorta ilişkisinin sona erdiği yıl için geçerli olan ancak kullanılmamış bulunan sigorta bedeli kadar güvence sağlar.

AVBC, A1-4/II hükmüne göre riziko, sigorta sözleşmesinin hüküm ve sonuçlarını ifade ettiği zaman dilimi içinde gerçekleşmelidir. Bu hükme göre sigorta sözleşmesinin sona ermesi, sigorta teminatının kesilmesine sebep olur. Fakat, sigorta ettirenin, bilgi güvenliğinin ihlâline yönelik fiillerin devam eden sonuçlarından da korunması gerekli olduğundan, sigorta sözleşmesi kapsamında sigortacının devam eden sorumluluğu kabul edilmiştir[128]. Bu anlamda sonraki sorumluluğun kabul edilmesi, sigorta ettirenin malvarlığında sigorta sözleşmesinin sona ermesinden sonra ortaya çıkabilecek olan zararların da belirli koşullarla teminat altına alınmasını sağlar[129]. Böylece, örneğin, sigorta sözleşmesinin süresi içinde gerçekleşmiş ancak fark edilmemiş ve malvarlığına zarar verici etkisi daha sonra ortaya çıkmış olan siber saldırıların sonuçlarından da sigorta ettireni korumak mümkün olur[130].

---

127 Sigorta sözleşmesinin sona ermesine yönelik bu sayım sınırlayıcıdır. Dolayısıyla, sözleşmenin iptal sebebiyle sona ermesi durumunda anılan sonraki sorumluluk söz konusu olmaz. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A.1-5, N. 2.

128 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-5, N. 1.

129 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-5, N. 1.

130 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-5, N. 2.

VI. SİGORTA ETTİREN VE SİGORTALI

1. Sigorta Ettiren

Sigorta sözleşmesinin tarafları, sigortacı ve sigorta ettirendir. Zarar sigortalarında (ve bu kapsamda siber risk sigortalarında) sigorta ettiren, belirli bir prim karşılığında, kendisinin para ile ölçülebilir bir menfaatine, riziko (inceleme konusu bakımından siber risk) dolayısıyla gelebilecek zararların teminat altına alınması konusunda sigortacıyla sözleşme yapan kişidir[131]. Genel Şartlar'a göre sigorta teminatı, sigorta poliçesinde adı geçen sigorta ettiren ve yine aynı yerde belirtilen işletmeler için geçerlidir (AVBC A1-7/I).

2. Sigortalı

Genel olarak sigortalı, rizikonun gerçekleşmesiyle zarar görme ihtimali olan ve sigorta sözleşmesinden doğan hakların sahibi olan kişilerdir[132]. Sigorta ettiren, başkasının menfaatini de (başkası hesabına sigorta şeklinde) sigorta ettirebilir. Dolayısıyla, sigorta ettiren ve sigortalı, aynı şahıslar olabileceği gibi; farklı kişiler de olabilir[133]. Bununla bağlantılı olarak, siber risk sigortası anlamında sigortalı kişiler, sigorta ettirene ya da sigortalı işletmeye bir iş ya da hizmet sözleşmesiyle bağlı olarak çalışan işçiler ve geçici işçi pozisyonundaki kişilerdir. Ayrıca, usulüne uygun olarak seçilmiş ve görevlendirilmiş organ üyeleri de bu anlamda sigorta kapsamına dâhil kişiler arasındadır[134] (AVBC A1-7/II).

Rizikonun gerçekleşeceği işletmeler çeşitli büyüklükte olabilir. Sadece büyük şirketlerin siber saldırıların hedefi olabileceği söylenemez. Aksine, büyük şirketler topluluklarından tek kişi işletmelerine kadar birçok kategorideki işletmeler siber saldırıların hedefi olabilir[135]. Bununla birlikte, çalışan sayısı yüz ila beş yüz arasında olan işletmelerin daha sık

---

131 **AYHAN/ÇAĞLAR/ÖZDAMAR**, s. 130.

132 **KENDER**, Rayegan: Türkiye'de Hususi Sigorta Hukuku, 14. Bası, Oniki Levha, İstanbul, 2014, s. 220; **YAZICIOĞLU/ŞEKER ÖĞÜZ**, s. 89; **KARA**, Sigorta Hukuku, s. 146.

133 **KENDER**, s. 220.

134 Dolayısıyla, sahip oldukları pay oranına göre şirket yönetiminde etkili olan ve fiilî organ sıfatına sahip kişiler bu kapsamda değildir. Bkz. Prölss/Martin VVG, **KLIMKE**, AVBC, A1-7, N. 2.

135 Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 19.

bu saldırıların hedefi olduğu ve siber risk sigortasına ihtiyaç duyduğu da bir gerçektir[136].

Sigorta sözleşmesinde sigorta ettiren için geçerli olan tüm sözleşme hükümleri, sigortalı işletme ya da kişiler için de uygun düştüğü ölçüde geçerlidir (AVBC A1-8/I). Dolayısıyla, hem sigorta ettirenin elektronik verileri ve bilgi işlem sistemleri hem de sigortalılara ait veri ve sistemler sigorta teminatı kapsamındadır[137].

VII. SİGORTACININ ZARARI TAZMİN BORCUNUN MUACCELİYETİ

1. Üçüncü Kişilerin Talepleri

Sigorta ettirenin, bilgi güvenliğinin ihlâli sebebiyle gerçekleşen riziko dolayısıyla üçüncü bir kişiye karşı bir özel hukuk hükmü gereğince sorumlu olması mümkündür. Üçüncü kişiye ait bir zararın ortaya çıktığı bu hallerde de sigorta teminatı söz konusudur (AVBC A3). Bu doğrultuda, sigortacı, üçüncü bir kişinin sigorta ettireni yerine getirmek zorunda bırakan talebinin bir kesin hüküm, kabul veya uzlaşma ile tespit edildiği tarihten itibaren iki hafta içinde sigorta ettireni söz konusu üçüncü kişinin talebinden kurtarmalıdır. Talepte bulunan üçüncü kişi, sigorta ettiren tarafından tatmin edilmişse; sigortacı, üçüncü kişiye ödeme tarihinden itibaren iki hafta içinde gerekli tazminatı sigorta ettirene öder (AVBC A1-13.1[138]).

2. Sigorta Ettirenin Zararının Karşılanması

Sigortacının tazminat ödeme borcu, sigortacının zararın karşılanması talebine dair sebep ve miktar yönünden tespitleri tamamlandığında muaccel olur. Sigorta ettiren, rizikonun gerçekleştiğine ve zararın ortaya çıktığına dair bildirimden bir ay sonra, duruma göre en az ödenmesi gerekli tutarı bir avans ödemesi olarak talep edebilir (AVBC A1-13.2).

3. Zararların Tazmini İçin Yapılacak Ödemelerin Ertelenmesi

Sigortacı, aşağıdaki koşulların gerçekleşmesi halinde zararların tazmini için gerçekleştirilecek ödemeleri erteleyebilir (AVBC A1-13.3):

---

136 Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 19.

137 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-8, N. 1.

138 Karş. VVG §100.

- Sigorta ettirenin zararın tazmini için yapılacak ödemeleri alma konusundaki hakkı ile ilgili şüpheler varsa.

- Sigorta ettiren veya temsilcisi hakkında, sigortaya konu rizikonun gerçekleşmesiyle ilgili idari veya cezai bir takibatın yapılıyor olması durumunda.

4. Tazminat Talebinin Temlik Edilebilirliği

Siber saldırılar sonucu zarara uğrayan işletmelerin, üretim ya da tedarik zincirinin bozulması sebebiyle üçüncü kişilere karşı olan yükümlülüklerini yerine getirememeleri ve sonuç olarak bu kişilere karşı sözleşme uyarınca sorumlu olmaları mümkündür[139]. Bu sorumluluk, sigorta ettireni üçüncü kişiye karşı konusu belirli bir miktar paranın ödenmesi yükümlülüğü altına sokabilir. *Sigorta ettirenin üçüncü kişilere karşı yerine getirmek zorunda olduğu bu tür talepler*den kurtarılma hakkı[140] bazı şartlarla temlik edilebilir. Buna göre, kurtarılma yönündeki talebin kapsam ve sınırları kesin olarak tespit edilmeden önce bu hak, sigortacının onayı olmaksızın, başkasına devredilemeyeceği gibi rehnedilmesi de mümkün değildir. Fakat, sigortalı sorumluluk teminatı kapsamında sigortacıya karşı sahip olduğu bu hakkını zarar gören üçüncü kişiye temlik edebilir (AVBC A1-14.1[141]).

Sigortacıdan tazminat ödenmesini talep etme hakkı, muacceliyetten önce sadece sigortacının muvafakatı ile devredilebilir. Sigorta ettiren açısından haklı sebeplerin varlığı halinde bu muvafakat verilmek zorundadır (AVBC A1-14.2). Görüldüğü üzere, AVBC A1-14.1 ile 14.2 arasında, sigortalının zarar gören üçüncü kişilerin taleplerinden kurtarılma hakkı ile ve kendisinin uğradığı zararlar için tazminat talep hakkının temliki bakımından ayırım yapılmıştır.

VIII. SİGORA TEMİNATINI SINIRLANDIRAN ŞARTLAR

1. Muafiyet

Rizikonun gerçekleşmesi ihtimalinin yüksek olduğu durumlarda, belirli bir muafiyet tutarının öngörülmesiyle, sigortacının yüksek tutarlarda tazminat ödeme ihtimali ile karşı karşıya kalmasından doğabilecek

---

139 **MEHRBREY/SCHREIBAUER**, s. 80.

140 Bu hak, AVBC A3 uyarınca sigortacıya karşı ileri sürülebilir.

141 Karş. VVG §108.

dezavantajlı durumun önüne geçilmeye çalışılır[142]. Siber risk sigortasına konu rizikoların coğrafi olarak kaynaklanabileceği alanların ve çeşitlerinin geniş kapsamlı olması ve tamamen kontrol edilemezliği de sigorta şirketlerinin bu sözleşme kapsamında bir risk havuzu oluşturmasını güçleştirmekte[143] ve bu sigorta türünün olabildiğince yaygınlaşmasını engellemektedir[144]. Bu sebeple, siber risk sigorta sözleşmesinde sigortacıyı koruyan özel şartların bulunması doğaldır. Bu düşüncelerle, sigorta hukukunda, sigortacıyı korumaya yönelik muafiyet prensibi kabul edilmiştir. Bu prensibe göre, sigorta ettiren, özel olarak kararlaştırılmış olması kaydıyla, rizikonun gerçekleşmesi halinde AVBC A2-A4 hükümleri doğrultusunda ve her seferinde sigorta poliçesinde gösterilmiş olan tutar kapsamında, zararın muafiyet tutarı veya oranındaki kısmına kendisi katlanır. Başka türlü kararlaştırılmamış olduğu müddetçe, sigortacı bu halde de haksız tazminat taleplerine karşı koruma yükümlülüğü altındadır. Gerçekleşen zararın sigorta bedelinden yüksek olduğu durumlarda, muafiyet tutarı gerçekleşen zarar tutarından düşülür.

2. Seri Zarar Klozu

Sigortanın hüküm ve sonuçlarını ifade ettiği bir zaman dilimi içerisinde gerçekleşmiş rizikolar, aşağıdaki koşulların ortaya çıkması şartıyla, seri zararlar bağlamında ve ilk rizikonun gerçekleşmesi anında vuku bulmuş tek bir riziko sayılır:

- Rizikoların,

o bilgi güvenliğinin ihlâli anlamında *aynı* olguya (örneğin, farklı zamanlarda gerçekleşen rizikoların tek bir siber saldırıya dayanması) ya da

o bilgi güvenliğinin ihlâli anlamında *benzer* ve özellikle zamansal ve nesnel açıdan aynı bağlam içinde bulunan olgulara dayanıyor olması (örneğin, bir merkezden idare edilen ancak farklı zamanlarda ortaya çıkan aynı amaçlı *malware*, *phishing*[145] ya da *ddos* gibi siber saldırıların bulunması).

---

142 **GÜNAY**, M. Barış: Sigorta Hukuku, 3. Bası, Seçkin, Ankara, 2021, s. 161.

143 **MALEK/SCHÜTZ**, s. 421.

144 **VICEVICH**, s. 557; **ALTUNTAŞ/KARA/SOYLU/KIRKBEŞOĞLU**, s. 12.

145 *Phishing* (oltalama), kullanıcıların e-posta adreslerine, onları maddî açıdan cezbedici şekilde hediye, ödül ya da ikramiye vermek gibi sahte vaatlerle kandırarak kişisel veriler başta olmak üzere kullanıcıya ait bazı bilgilerin elde edilmesini hedefleyen

Seri bir şekilde gerçekleşen zararların varlığını ispat yükü sigortacının üzerindedir[146].

IX. SİGORTA ETTİRENİN RİZİKONUN GERÇEKLEŞMESİNDEN ÖNCEKİ TEKNİK YÜKÜMLÜLÜKLERİ (AVBC A1-16)

Sigorta hukukuna dair temel ilkelerden biri de sigorta ettirenin, sigorta sözleşmesinin kurulmasından sonraki aşamada, süreklilik oluşturacak şekilde sigortacının aleyhine ve rizikonun gerçekleşmesi ihtimalini artırıcı davranışlardan kaçınması yükümlülüğüdür[147]. Zira, sözleşmenin başlangıcındaki prim ve riziko dengesi o anki şartlara göre kurulmuştur[148]. Rizikonun gerçekleşmesine yol açacak şekilde durumun kötüleşmesi sigortacının aleyhinedir. Konuyu ele alan TTK m. 1444'e göre sigorta ettiren, sözleşmenin yapılmasından sonra, sigortacının izni olmadan rizikoyu veya *mevcut durumu ağırlaştırarak tazminat tutarının artmasını etkileyici davranış ve işlemler*de bulunamaz. Bu bağlamda sigorta ettiren, rizikonun gerçekleşmesinden önce, üzerine düşen tüm sözleşmesel yükümlülükleri yerine getirmek zorundadır. Bunun için özellikle, bilgi işlem sistemlerinin bireysel kullanıcıları ve dijital hiyerarşisi arasında ayrım yapmış olması gereklidir. Bunun gerçekleşmesi, *tüm kullanıcıların* bilgi işlem sistemlerine yeteri kadar karmaşık parolalarla korunan bir erişimini gerektirir. Tüm gerçek kişi kullanıcılar için tek bir erişim çiftinin (kullanıcı adı-parola) tanımlanması artan bir risk anlamına geleceğinden; tüm gerçek kişiler için ayrı ayrı kullanıcı adı ve parola belirlenmesi, sigorta ettirenin rizikonun gerçekleşmesinden önceki yükümlülüklerindendir[149]. Bu anlamda yönetici erişimi, yalnızca yöneticiler *(administrators)* için ve yönetimsel faaliyetlerin icrası için saklı tutulmalıdır.

Sigorta ettiren aynı zamanda bilgi işlem sistemlerini, bu sistemler artan bir riske maruz kaldıklarında yetkisiz erişime karşı ilâve bir koruma

---

bir siber saldırı türüdür, https://it.bilgi.edu.tr/tr/guvenlik/phishing/, Erişim Tarihi: 22/05/2024.

146 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-15, N. 11.

147 **YAZICIOĞLU/ŞEKER ÖĞÜZ**, s. 149.

148 **ÜNAN**, Samim: Türk Ticaret Kanunu Şerhi, Altıncı Kitap-Sigorta Hukuku, Cilt I, Oniki Levha, İstanbul, 2016, s. 464.

149 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-16, N. 7.

ile donatmak zorundadırlar. Örneğin, internet üzerinden erişilebilir cihazlarda ya da internet erişimine sahip mobil cihazlara yönelik bu manada artan bir risk var demektir. Oysa, internet erişiminin bulunmadığı iş istasyonları için artan bir risk yoktur ve sigorta ettirenin bunlar için ek tedbirler alması gerekmemektedir[150]. Artan risklerden korunmak adına alınabilecek ek koruma tedbirleri şunlar olabilir: Cihazların güvenlik duvarı ile korumaya alınması; sunucular bakımından iki faktörlü kimlik doğrulama sisteminin getirilmesi; seri taşıyıcı ve mobil cihazların şifrelenmesi; hırsızlığa karşı koruma önlemleri.

Sigorta ettiren bilgi işlem sistemlerini otomatik olarak güncellenebilen ve kötü amaçlı yazılımlara karşı koyabilen koruyucu yazılımlarla muhafaza etmelidir. Bu tür yazılımlar şunlar olabilir: Virüs tarayıcı programlar; kod imzalama sertifikaları[151]; uygulama güvenlik duvarları[152].

Sigorta ettirene ait bilgi işlem sistemleri, gerekli ve ilgili güvenlik yamalarını derhal sisteme entegre ederek yükleyebilen bir yapıda olmalıdır. Bilgi teknolojileri dünyasında bilinen güvenlik açıklarına sahip sistemler ve uygulamalar, bu güvenlik açıklarına yönelik uygun ek güvenlik tedbirleri olmaksızın kullanılmamalıdır.

Sigorta ettiren, bilgi işlem sistemlerini haftada en az bir kez yedekleme işlemine tabi tutmalıdır. Bu sayede veriler ayrı olarak ve fizikî bir şekilde taşınma imkânına sahip olur. Böylelikle, sigorta sözleşmesine konu riziko gerçekleştiğinde orijinal ve yedek kopyalara aynı anda erişilememiş olunur ki bu, verilerin manipüle edilmesi ya da yok edilmesinin engellenmesi demektir. Sigorta ettiren, söz konusu yedekleme sürecini periyodik olarak yönetir.

---

150 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-16, N. 10.

151 Kod imzalama sertifikaları, bir yazılımcının yaratmış olduğu kodların, imzalama tarihinden itibaren değiştirilmemiş ya da bozulmamış olduğunu garanti etmeye yarayan belgelerdir, https://en.wikipedia.org/wiki/Code_signing, Erişim Tarihi: 22/05/2024.

152 Güvenlik duvarı (*firewall*), internet kullanıcısının siber saldırılardan korunması için gerekli ilk savunma mekanizmasını oluşturan ve kötü amaçlı bir yazılım veya bir siber korsanın internet kullanıcısına ait kişisel verileri ele geçirmesini engelleyen donanım ya da yazılımlardır, https://www.mcafee.com/tr-tr/antivirus/firewall.html, Erişim Tarihi: 22/05/2024.

Sigorta ettiren ayrıca, bütün yasal, idarî ve sözleşmesel güvenlik hükümlerine uymak zorundadır. Sigorta ettiren, sigortacının talebi üzerine, tehlike arz eden durumları makul bir süre içinde ortadan kaldırmak durumundadır. Hasarla sonuçlanması muhakkak bir durum tehlikeli sayılır. Fakat, her iki tarafın sigorta sözleşmesi çerçevesindeki karşılıklı menfaatleri değerlendirildiğinde bu tür tedbirlerin alınması beklenemez ise anılan gereklilikten söz edilemez.

X. TEMİNAT DIŞI HALLER (AVBC A1-17)

Sigorta sözleşmesine konu olan rizikonun herhangi bir istisna tanınmaksızın tamamen teminat altına alınması, akdedilen birçok sözleşme vesilesiyle, sigortacıyı altından kalkılamayacak tazminat yükleriyle karşı karşıya bırakabilir[153]. Bu sebeple, sigorta sözleşmelerinde her bir özel sigorta konusuna göre teminat dışında olan durumlar özel olarak belirtilir. Genel Şartlar'a göre de bazı hallerin gerçekleşmesi bu hallerin gerçekleşmesine sebep olan olgular dikkate alınmaksızın sigorta teminatını ortadan kaldırır[154]. Bir hususun sigorta teminatı dışında olduğu konusundaki ispat yükü sigortacıdadır[155]. Zira bu vakıadan kendi lehine (sigorta tazminatından sorumlu olmama yönünde) hak çıkaran taraf sigortacıdır.

Genel Şartlar'a göre aşağıdaki haller sigorta teminatı dışındadır:

1. Sözleşme Öncesi Bilgi Güvenliği İhlâlleri

A. Kural

Sigorta sözleşmesinin yapıldığı sırada zaten gerçekleşmiş olan ya da gerçekleşme ihtimali bulunmayan bir riziko sigorta edilemez[156]. Böyle

---

153 **KENDER**, s. 296.

154 Sigorta teminatının istisna klozlarıyla sınırlandırılarak, sigortacının teminat sağlama borcunun kapsamının daraltılması eğilimi uluslararası hukukta da söz konusudur. Örneğin, bu manada, denizcilik sigortalarında kullanılan CL380 klozu ile sigortanın; bir bilgisayarın, birden fazla bilgisayardan oluşan bir sistemin, bir yazılımın, kötü niyetli kodun, bilgisayar virüsünün veya bilgisayarda yapılmış bir işlemin ya da başka bir elektronik sistemin doğrudan ve bizzat zarar verme aracı olarak kullanılmasından kaynaklanan zararları kapsamayacağı belirtilmiştir. Konu ile ilgili ayrıntılı bilgi için bkz. **KARAYAZGAN**, Ahmet: Hukuki Yönüyle Siber Sigorta ve Sessiz Siber Teminatının Çalışma Esasları, Legal Hukuk Dergisi, C. 18, S. 215, Y. 2020, https://legalbank.net/belge/hukuki-yonuyle-siber-sigorta-ve-sessiz-siber-teminatinin-calisma-esaslari/4281775, E.T. 1.09.2024.

155 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-17, N. 2.

156 **YAZICIOĞLU/ŞEKER ÖĞÜZ**, s. 74.

bir riziko sigorta edilmiş olsa dahi sözleşme imkânsızlık sebebiyle geçersizdir[157]. Geçmişe etkili sigortayı düzenleyen TTK m. 1458 hükmü de bu doğrultudadır. Zira bu hükme göre, sigorta, sigorta koruması sözleşmenin yapılmasından önceki bir tarihten itibaren sağlanacak şekilde yapılabilir. Ancak, rizikonun gerçekleştiğinin bilindiği veya gerçekleşme ihtimalinin ortadan kalkmış olduğu, sözleşmenin yapılması sırasında, sigortacı ile sigorta ettiren ve sigortadan haberi olmak şartıyla, sigortalı tarafından biliniyorsa *sözleşme geçersiz* dir. Bu doğrultuda, siber risk sigortası sözleşmesinin akdedilmesinden önceki dönemde ortaya çıkan bilgi güvenliği ihlâllerinden kaynaklanan zararlar da teminat dışındadır. Bununla beraber, siber saldırıların ne zaman gerçekleştiği yönündeki kesin tespit güç olduğu için, yine de yüz seksen günlük bir periyodun bir siber saldırının varlığının anlaşılması için yeterli olabileceği ifade edilmektedir[158]. Siber saldırının gerçekleşme zamanı ile ilgili kesin bir belirlemenin yapılamadığı hallerde, gerçekleşen zararın teminat dışında olduğu ileri sürülemez[159].

B. Geçmişe Etkili Koruma

Genel şartlarda, teminat dışı bırakılan hallerin bazıları için sözleşmeyle teminat sağlanması imkânı getirilmiştir[160]. Özellikle, geçmişte gerçekleşmiş ancak uzun süre fark edilememiş siber saldırıların etkilerini sonradan göstermesinden kaynaklanan zararlar da sigorta teminatı altına alınmış olur[161]. Buna göre, AVBC A1-17.1 hükmünden farklı olarak, sigorta sözleşmesinin akdedildiği sırada tespit edilememiş olan (bilinmeyen), sigorta poliçesinde belirtilen zamandan (geçmişe etki tarihinden) sonra ortaya çıkan ve aynı zamanda sigorta sözleşmesinin başlangıcından önce (teminat başlangıcı ile geçmişe etki tarihi arasındaki geçmişe etki süresinde) gerçekleşen bilgi güvenliği ihlâllerinden kaynaklanan zararlar da teminat kapsamındadır (AVBC A1-6). Sigorta ettirene ya da onunla

157 **ÜNAN**, Cilt II, s. 77.

158 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-17, N. 1'de dn. 1.

159 **FORTMANN**, s. 432.

160 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-6, N. 1.

161 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-6, N. 1.

bağlantılı bir üçüncü kişiye atfedilebilecek müspet vukuf, hükmün uygulanmasını engeller[162].

2. Savaş

Rizikonun gerçekleşmesi veya zararın ortaya çıkması bir savaş yüzünden ise sigorta teminatı yoktur. Bu anlamda savaş, iki ülkenin silahlı kuvvetlerinin çarpışması, işgal, iç savaş, ayaklanma, devrim, isyan ve sivil ya da askeri darbe girişimlerini içeren geniş bir kavramdır.

Teknolojinin sağladığı imkânlarla sanal dünyada yapılan siber savaşların da *(Cyberkrieg)* bu anlamda savaş kavramı içinde değerlendirilip değerlendirilemeyeceği akla gelebilir. Öncelikle, bu türden bir savaşın sigorta teminatı dışında bırakılması isteniyorsa mutlaka sigorta sözleşmesinde bu yönde bir istisna hükmüne ihtiyaç olduğu belirtilmektedir[163]. Kanaatimizce, siber savaş olarak nitelendirilecek çapta geniş bir sanal (ve büyük olasılıkla yasadışı) mücadelenin genel şartlarla bir istisna hükmü olarak belirlenmesi, yasadışı bir zeminde gerçekleşen aksiyonların etki ve sonuçlarının kapsamının belirlenmesinde yaşanabilecek güçlükler sebebiyle taraflar arasındaki hukukî uyuşmazlıkları artırabilecek niteliktedir. Dolayısıyla, resmî makamların "savaş" olarak nitelendirmediği mücadelelerin sigorta teminatına istisna edilmemesi gerekir. Zaten, aksinin kabulü halinde, sigortacının bir siber saldırının yabancı bir devletten kaynaklandığını ispatı gerekir ki bunun güçlüğü de ortadadır[164]. Bu yüzden, siber savaşın gerçekleşebileceği zeminde bulunacak kadar kritik ve geniş çaplı işletmeler için de sigorta teminatının sağlanması ve sözleşmelerde bu yönde istisnai hükümlere yer verilmemesi isabetli olur. Elbette, rizikonun niteliğine göre sigorta priminin miktarının değişebileceği de göz ardı edilmemelidir.

3. Siyasî Kargaşa ve Tehditler

Rizikonun gerçekleşmesi veya zararın ortaya çıkması düşmanca eylemlere, bir iç isyana veya iç kargaşaya, genel veya yasadışı greve dayanıyorsa sigorta teminatı bulunmamaktadır.

---

162 Prölss/Martin VVG, **KLIMKE**, AVBC, A1-6, N. 3.

163 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-17, N. 1.

164 **MALEK/SCHÜTZ**, s. 427.

4. Terör Eylemleri

Rizikonun gerçekleşmesine ya da zararın ortaya çıkmasına yol açan olgu bir terör eylemi ise bu hâl sigorta teminatı dışındadır. Genel Şartlar'a göre terör eylemi; politik, dinî, etnik ya da ideolojik amaçlara ulaşmak için yapılan yasadışı faaliyetlerdir. Ancak bu faaliyetlerin terör eylemi sayılabilmesi için söz konusu faaliyetlerin, toplumun tamamı ya da bir kısmında korku ve dehşet yaymaya, böylelikle devlet kurumları üzerinde etki yaratmaya yönelik ve buna uygun olması gerekir.

5. Kusurlu Altyapı

Eksik ve hatalı altyapının bulunması gerçekleşen rizikoyu teminat dışı bırakır. Gerçekten de sigortacının, ilgili bölgedeki genel bir elektrik kesintisine dayanan ve bundan kaynaklanan bir bilgi güvenliğinin ihlâli eylemine karşı sorumluluğunu sınırlandırmakta özel bir yararı vardır[165]. Çünkü sigortacı, eksik ya da hatalı altyapı bağlantılı tek bir olayın gerçekleşmesiyle çok sayıda etkilenmiş işletmenin tazminat talebi ile karşı karşıya kalabilir ve böylelikle sigorta şirketinin finansal yapısı sarsılabilir[166]. Bu olumsuz durumdan kurtularak, gerçekleşen olayın teminat dışında olduğunu iddia edebilmek amacıyla altyapıda bir noksanlıktan bahsedebilmek için aşağıdaki koşulların gerçekleşmesi gerekli ve yeterlidir:

- Ülkenin belirli bir bölgesini oluşturan çeşitli büyüklükteki mülkî idarî amirliklerin ya da bunların il, ilçe, belediye veya köy gibi önemli kısımlarının rizikoya yol açan eksiklikten etkilenmiş olması.
- Bölgelerarası bilgi transferine imkân sağlayan telefon, internet ya da radyo ağları gibi yapıların söz konusu eksiklikten etkilenmiş olması.
- Toplumun genel yararına hizmet eden kurum ve kuruluşların aşağıdaki hizmetlerinin altyapı eksikliğinden etkilenmiş olması:
  - Katı atık tahliye sistemleri.
  - İçme suyu temini.
  - Atık su tahliyesi.
  - Elektrik ve doğalgaz temin sistemleri.
  - Kısa ve uzun mesafe toplu taşıma sistemleri.
  - Sair altyapı işletmeleri.

---

165 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-17, N. 9.

166 **FORTMANN**, s. 434.

6. Taşıtlarla İlgili Riziko ve Zararlar

Kara, hava, demiryolu ya da denizyolu taşıtlarıyla ilgili riziko ve zararlar teminat dışındadır. Bu kural aynı zamanda hava sahası, trafik gözetim, yönlendirme ve idare sistemleri için de geçerlidir.

7. Fidye ve Şantaj

Kötü amaçlı yazılım kullanılarak siber saldırıya hedef olan kişiden fidye istenmesi ya sistemin tamamen kilitlenmesi suretiyle ya da belirli dosyaların şifrelenmesi suretiyle gerçekleştirilir[167]. Bu kilitleme ya da şifrelemenin çözülmesi için siber saldırıdan zarar gören kişiden belirli miktar parayı bir hesaba aktarması istenir ve aktarımın ardından kilitleme ya da şifrelemenin çözüleceği vaat edilir[168].

Fidye istenmesi ve şantaj yapılması sonucu ödenen paralar (ve bitcoin gibi diğer ekonomik değerler[169]) sigorta teminatı dışındadır. Teminat dışında olan ve fidye konusunu oluşturan edim parasal bir edim olup; sigorta ettireni (örneğin belirli bir malın belirli bir süre için tedarik edilmemesine yönelik edimlerde olduğu gibi) belirli bir biçimde davranmak zorunda bırakan, konusu para dışında olan fiiller sigorta teminatı içindedir[170].

8. Finansal Piyasa İşlemleri

Kıymetli evrakın, emtianın, türev araçların, dövizin, tahvilin ve benzeri yatırım araçlarının her türlü alımı ve satımı sebebiyle veya bu işlemlerle bağlantılı olarak ortaya çıkan zarar veya rizikolar teminat dışındadır. Çünkü, finansal piyasalarda (muhtemel) sigorta ettirenin karşılaşabileceği zarar rizikosu ile kâr beklentisi birbirini dengeler ve zarar rizikosunun teminat altına alınması sigorta sözleşmesinden beklenen bir yarar olamaz[171].

9. Varlık Akışı

Bir bilgi güvenliğinin ihlâliyle bağlantılı olarak sigortalıya ait olan malvarlığı değerlerinin (örneğin bir hırsızlık sebebiyle) dışarı akışından

---

167 **BEUKELMANN**, Stephan: "Cyber-Attacken – Erscheinungsformen, Strafbarkeit und Prävention", NJW-Neue Juristische Wochenschrift Spezial, S. 2017-12, s. 376.

168 **BEUKELMANN**, s. 376.

169 **FORTMANN**, s. 434.

170 **FORTMANN**, s. 434.

171 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-17, N. 18.

ötürü ortaya çıkan riziko ve zararlar teminat kapsamı dışındadır. Bununla beraber, uygulamada birçok sigorta şirketi özel klozlar ile siber hırsızlıklara karşı sigorta ettirenlere teminat sunmaktadır[172].

10. Bir Yükümlülüğün Kasıtlı İhlâli

Bir kanun hükmüne, karara, temsile yönelik bir yetkilendirme işlemine ya da talimata kasıtlı olarak veya (sonucunu öngörmeyerek de olsa) bilinçli bir davranış sonucu aykırı davranarak zarara ya da rizikonun gerçekleşmesine sebep olan kişilerin sigorta sözleşmesine ilişkin talepleri teminat dışındadır.

11. Kamusal Tedbirler ve Cezalar

Aksi kararlaştırılmış olmadıkça, sigorta ettirene karşı uygulanan kamusal icraî işlemler ve emirler, özgürlüğü kısıtlayıcı cezalar ya da para cezaları gibi yaptırımlardan kaynaklanan riziko veya zararlar teminat kapsamında değildir.

12. Fikrî Mülkiyet Haklarının İhlâli

Aksi kararlaştırılmış olmadıkça, Marka, patent, telif hakkı gibi fikrî mülkiyet unsurlarına ilişkin hakların; lisans veya lisans ücretine ilişkin hakların, rekabet ve haksız rekabet hukukuna ilişkin kuralların; kişilik haklarının ihlâlinden kaynaklanan ya da bunlarla bağlantı içinde olan zararlar veya rizikonun gerçekleşmesi olgusu teminat dışındadır.

13. Nükleer Enerji

Nükleer enerji, radyasyon ya da radyoaktif maddelerin etkisiyle ortaya çıkan zararlar veya rizikolar da teminat dışındadır.

14. Ayrımcılık

Özellikle Genel Eşit Davranma Yasası'na *(Allgemeinen Gleichbehandlungsgesetz)* dair hükümler olmak üzere, ayrımcılığın ortadan kaldırılmasına dair hükümlere aykırı davranılması sebebiyle ortaya çıkan zarar veya rizikolar teminat kapsamı dışındadır.

XI. TÜRKİYE'DE SİBER GÜVENLİK SİGORTASI ÖRNEKLERİ

Ülkemizde siber risk sigortası, henüz gelişim aşamasındadır. Türkiye'de 2024 yılı ortaları itibariyle siber risk sigortasına dair genel şart şeklinde bir düzenlemenin bulunmadığı görülmektedir[173]. Fakat

---

172 Rüffer/Halbach/Schimikowski VVG, **SALM**, A.1-17, N. 20.

173 Siber risk sigortaları için Meslekî Sorumluluk Sigortası Genel Şartları'nın (RG, 26.5.2013/28658) geçerli olacağı belirtilmektedir. Bkz.

uygulamada, siber risk sigortası sözleşmelerinin yaygın olarak yapıldığı görülmektedir. Siber risk sigortalarının, "*Dijital Güvenlik Sigortası*[174]", "*Risk (Veri Koruma) Sigortası*[175]", "*Siber Sorumluluk Sigortası*[176]", "*Bireysel Siber Güvenlik Sigortası*[177]", "*Ticarî Siber Güvenlik Sigortası*[178]" ve "*Siber Koruma Sigortası*[179]" adları altında yapıldığı görülmektedir[180, 181].

Türkiye özelinde ele alındığında, siber risk sigortalarıyla teminat altına alınan rizikoların genel itibariyle aşağıdaki gibi olduğu söylenebilir[182]:

ALTUNTAŞ/KARA/SOYLU/KIRKBEŞOĞLU, s. 12. Ancak, anılan genel şartlar sorumluluk sigortalarını konu edinmektedir. Yukarıda da ifade edildiği üzere, siber risk sigortaları hem zarar hem de sorumluluk sigortaları şeklinde yapılabilir. O halde, bu sigorta türüne özel bir genel şart düzenlemesi gereklidir.

174 https://www.somposigorta.com.tr/dijital-guvenlik-sigortasi, Erişim Tarihi: 8/1/2022.

175 https://phillipsigorta.com.tr/siber-risk-veri-koruma-sigortasi/, Erişim Tarihi: 8/1/2022.

176 https://www.allianz.com.tr/tr_TR/urunler/diger-urunler/sorumluluk-sigortalari/finansal-sigortalar.html, Erişim Tarihi: 8/1/2022.

177 https://www.anadolusigorta.com.tr/urunler/size-ozel-sigortalar/bireysel-siber-guvenlik-sigortasi, Erişim Tarihi: 8/1/2022.

178 https://www.dogasigorta.com/urunler/ticari-siber-guvenlik-sigortasi, Erişim Tarihi: 8/1/2022.

179 https://www.aksigorta.com.tr/urunler/kurumsal-urunler/diger-sigortalar/siber-koruma-sigortasi, Erişim Tarihi: 8/1/2022.

180 Siber risk sigortasıyla ilgili uygulamada, Almanya'da kullanılan terimler de farklılık göstermektedir. Bu kavramlardan bazıları şunlardır: "*Cybercrime-Versicherung*, *Cyberrisiko-Versicherung*, *Computer-Missbrauch-Versicherung*, *Hacker-Versicherung*, *Anti-Hacker-Versicherung*, *Datenschutz-Versicherung*, *Elektronik-Versicherung*, *IT-Versicherung*, *Web-Versicherung*, *Online-Schutz-Versicherung*, *Multimedia-Versicherung*, *Cyber-Space-Versicherung*". Bkz. Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, **GEBERT/KLAPPER**, N. 2'den naklen.

181 Bu noktada, öğretideki bireysel/ticari siber risk sigortası ayrımının uygulamaya da yansımış olduğu söylenebilir. Söz konusu ayrım için bkz. **TEKİN**, s. 676.

182 Teminat altına alınan rizikolar açısından bu yönde bkz. https://www.aksigorta.com.tr/urunler/kurumsal-urunler/diger-sigortalar/siber-koruma-sigortasi, https://www.anadolusigorta.com.tr/urunler/size-ozel-sigortalar/bireysel-siber-guvenlik-sigortasi, https://www.isbank.com.tr/siber-guvenlik-sigortasi, https://www.turkiyesigorta.com.tr/urunlerimiz/diger-sigortalar/finansal-siber-koruma-sigortasi, https://www.yapikredi.com.tr/bireysel-bankacilik/sigorta-ve-emeklilik/siber-guvence-sigortasi, https://www.raysigorta.com.tr/kendim-ve-ailem-icin/diger-sigortalar/cyberella-siber-guvenlik, https://www.halkbank.com.tr/tr/bireysel/sigorta/diger/finansal-siber-koruma-sigortasi.html, Erişim Tarihi: 23/5/2024.

- Tüketici ekonomisine yönelik rizikolar ve özellikle,

o İnternet alışverişlerinde karşılaşılacak ödeme problemleri.

o Kredi kartı ve benzeri araçların izinsiz kullanımı.

o Kişisel teknolojik cihazlarda yaşanabilecek teknik sorunlar.

o Siber saldırılar sonucu kişisel hesaplardaki tutarların başka hesaplara aktarılması.

- Kişisel bilgilerin güvenliğine dair rizikolar ve özellikle,

o Sigorta ettirene ya da sigortalıya ait sosyal medya hesaplarının siber saldırıya uğraması.

o Sigorta ettirene ya da sigortalıya ait bilgisayar ve bilgi işlem sistemlerindeki verilerin izinsiz olarak çalınması, yayılması ve değiştirilmesi.

o Sigorta ettirene ya da sigortalıya ait kişisel bilgilerin deep web ve dark web olarak da isimlendirilen, internetin derin ve yasadışı katmanlarında alınıp satılması.

o Sigorta ettirene ya da sigortalıya ait kişisel şifrelerin çalınması.

- İşletme ekonomisine yönelik rizikolar, zararlar ve özellikle,

o Siber saldırı sonucu iş durmasından kaynaklanan zararlar.

o Bir siber saldırıyla bağlantılı fidye talepleri.

o İşletmeyle ilgili müşteri çevresi, plan ve hesap gibi gizli kalması gerekli bilgilerin bir siber saldırı ile çalınması.

o Verilerin muhafazası için kullanılan bilgi işlem sistemlerine verilen hasarlar.

- Sorumluluk hukuku anlamında karşılaşılabilecek rizikolar ve özellikle,

o Bir kamu otoritesine karşı ödenmek durumunda kalınan para cezaları.

o Verilerin hukuka aykırı olarak ele geçirilmesi sebebiyle karşılaşılan tazminat talepleri.

- Kişisel haklara ve saygınlığa ilişkin rizikolar ve özellikle,

o Kişisel verilerin çalınması sonucunda bilhassa dijital dünyadaki marka itibarına ve kişisel saygınlığa zarar verilmesi.

Bir sigorta ilişkisinde en kritik noktalardan biri, sigorta teminatının kapsamıdır. Başka bir deyişle, sigortacının ortaya çıkan zararı karşılama borcu için teminat dışı hallerin neler olduğunun tespiti sigorta

ilişkisinden beklenen yararın sağlanması için önemlidir. Uygulamada, siber risk sigortası kapsamında akdedilen sözleşmelerde bu konuda yeknesak ya da birbirine yakın veya benzer bir uygulamanın sağlanması için AVB-Cyber benzeri bir genel şart düzenlemesinin ortaya konması sigorta şartlarındaki yeknesaklığı artırarak muhtemel hukukî uyuşmazlıkları azaltacaktır[183].

SONUÇ

İşletmelerin müşterilerine sundukları malların ya da hizmetlerin önemli bir kısmının internet üzerinden ve bilgisayar teknolojileri kullanılarak arz edilmesi, bu işletmeleri siber saldırıların açık hedefi haline getirmektedir. Özellikle müşterilerine ait kişisel verileri sistemlerinde muhafaza eden şirketler bakımından, bu verilerin hukuka aykırı olarak ifşası halinde üçüncü kişilere (müşterilere) karşı sorumluluk da söz konusu olabilir.

Çeşitli kamusal, ticari ve bireysel gereklilikler sebebiyle, özellikle kişisel verilerin internet ortamında saklanması zorunluluğu göz önünde bulundurulduğunda, siber saldırıların sadece işletmeleri değil, aynı zamanda bireyleri de tehdit ettiği söylenebilir. Bilhassa, bireylerin sosyal medya kullanımlarının, devletlerle olan ilişkilerinin kısmen internet ortamına kaymasının etkisiyle, bireyler de siber saldırı tehdidinin muhatabı haline gelmiştir.

Siber rizikolara karşı sigorta ettireni korumayı amaçlayan sigorta türü ise siber risk sigortalarıdır. Siber risk sigortaları, ülkemizde ve Almanya'da yaygın olarak kullanılmakta ise de Almanya'nın aksine ülkemizde siber risk sigortaları için bir genel şart düzenlemesi bulunmamaktadır. Oysa, siber rizikoların bilinemezliği, gerçekleşen zararın kapsamını belirlemenin zorluğu ve tarafların bu zararlar karşısındaki hukukî durumlarını anlamak etmek bakımından ilgili sözleşme bakımından hak ve borç dağılımını net olarak tespit etmek son derece önemlidir. Siber risk sigortası genel şartlarının belirlenerek uygulamaya konulması, ülkemizde de bu alanda akdedilen sözleşmelerdeki yeknesaklığı sağlayacaktır. Siber risk sigortaları açısından bugün gelinen nokta bir yana, geleceğe

---

183 Alman hukuku açısından bu yöndeki bir tespit için bkz. Rüffer/Halbach/Schimikowski VVG, **ERICHSEN**, Vorbemerkungen, N. 2.

yapılacak kısa bir bakışta, bu tür sigorta sözleşmelerinin sayısının katlanarak artacağı söylenebilir. Zira, sadece ülkemizde değil tüm dünyada bilgisayar ve internet teknolojilerinin kullanımı asla azalmayacak, belki insan hayatının yüzde yüzünü işgal ediyor olacaktır. O halde, hukuk gelişen ihtiyaçlara cevap vermesi gereken bir araç olduğundan ötürü, ülkemiz de dünyadaki gelişmeleri takip etmeli, belki de bu ilerlemeye öncülük etmelidir. Bu bağlamda, çalışmamızın inceleme konusunu oluşturan genel şartlar benzeri bir düzenleme ivedilikle ve muhakkak gerçekleştirilmelidir. Alman Siber Risk Sigortası Genel Şartları bu konuda Türk hukukunda yapılması düzenlemeler açısından bir örnek niteliğindedir.

Alman Siber Risk Sigortası Genel Şartları'nın içeriği incelendiğinde bu sigortaların zarar sigortaları içinde tasnif edilebileceği görülür. Bu değerlendirme, Türk ve Alman sigorta hukukları arasında sigorta hukukunun temel prensipleri açısından söz konusu olan benzerlik göz önünde tutulduğunda Türk hukuku açısından da geçerlidir. Dolayısıyla, Türk hukukunda mevcut durumda genel şartlar olmaksızın uygulanan siber risk sigortaları zarar sigortaları arasındadır.

Alman hukukunda siber risk sigortaları, zarar sigortalarından mal ve sorumluluk sigortalarına ait teminatlar sunmaktadır. Bu durum Türk hukuku açısından, mevcut durumda genel şartlar olmaksızın sigorta şirketleri tarafından sunulan poliçe içeriğine göre değişir. Türk hukukunda, sigorta genel şartları anlamında ileride yapılması muhtemel bir düzenlemede, sorumluluk sigortaları anlamında teminatlar sunulması ihtimali de göz önünde tutulmalıdır. Çünkü, özellikle veri güvenliğinin ihlali sebebiyle sigorta ettirenlerin karşılaşması olası olan tazminat talepleri bu suretle genel şart hükümlerine tabi olarak teminat altına alınabilir.

KAYNAKÇA

ACHENBACH, Matthias: "Die Cyber-Versicherung – Überblick und Analyse", VersR-Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht, S. 2017-24, 2017, s. 1493-1500.

ALGANTÜRK LIGHT, Didem: "Taşıma Sektöründe Siber Riskler ve Etkileri", Deniz Ticareti Hukukunda Yeni Sorunlar Sempozyumu I, 2019, İstanbul, s. 83-95.

Allianz Risk Barometer, Top Business Risks for 2019, https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf, (Erişim Tarihi 25/5/2022).

ALTUNTAŞ, Eda/**KARA**, Emine/**SOYLU**, Abdullah Buğra/**KIRKBEŞOĞLU**, Erdem: "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar", Bankacılık ve Sigortacılık Araştırmaları Dergisi, S. 2018-12, s. 8-22.

ANTALYA, Osman Gökhan: Marmara Hukuk Yorumu-Borçlar Hukuku Genel Hükümler Cilt V/1, 2, 2. Bası, Seçkin, Ankara, 2019.

ANTALYA, Osman Gökhan/**TOPUZ**, Murat: Marmara Hukuk Yorumu-Eşya Hukuku Cilt: IV/1, 3. Bası, Seçkin, Ankara, 2019.

AYAN, Mehmet: Eşya Hukuku I-Zilyetlik Tapu Sicili, 13. Bası, Seçkin, Ankara, 2016.

AYHAN, Rıza/**ÇAĞLAR**, Hayrettin/**ÖZDAMAR**, Mehmet: Sigorta Hukuku Ders Kitabı, 3. Bası, Yetkin, Ankara, 2020.

BEUKELMANN, Stephan: "Cyber-Attacken − Erscheinungsformen, Strafbarkeit und Prävention", NJW-Neue Juristische Wochenschrift Spezial, S. 2017-12, s. 376-377.

BUĞRA, Ayşegül: "Otomatik Yönlendirme Seviyesi Yüksek Kara Araçları ve Sigorta", Galatasaray Üniversitesi Hukuk Fakültesi-Sigorta Hukukunun İki Güncel Sorunu: İnsansız Araçlar, Sorumluluk ve Özel Sağlık Sigortalarında Birden Çok Sigorta Sempozyumu-18 Ocak 2019, Ed. Serap Amasya, 2020, İstanbul, s. 1-35.

CEBECİ, İpek: "Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme", Üçüncü Sektör Sosyal Ekonomi Dergisi-Third Sector Social Economic Review, S. 2021-56/1, s. 163-188.

DOĞAN, Murat/**ŞAHAN**, Gökhan/**ATAMULU**, İsmail: Borçlar Hukuku Genel Hükümler, 2. Bası, Seçkin, Ankara, 2021.

ERICHSEN, Sven: "Cyber-Risiken und Cyber-Versicherung: Abgrenzung und/oder Ergänzung zu anderen Versicherungssparten", CCZ-Corporate Compliance, S. 2015-06, s. 247-250.

FORTMANN, Michael: "Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen", r+s recht und schaden, S. 2019-8, s. 429-444.

FRENCH, Christopher: "Insuring Against Cyber Risk: The Evolution of an Industry", Penn State Law Review, S. 2018-122/3, s. 607-612.

GÜNAY, M. Barış: Sigorta Hukuku, 3. Bası, Seçkin, Ankara, 2021.

HACIÖMEROĞLU, Abdülhamid Oğuzhan: "Zorunlu Sorumluluk Sigortacısının Sonraki Sorumluluğu", BATİDER, S. 2020-36/2, s. 165-192.

HÖRA, Knut/**SCHUBACH**, Arno: "§ 1 Grundlagen des Privatversicherungsrechts", içinde: Münchener Anwaltshandbuch Versicherungsrecht, Höra/Schubach, 5. Auflage, C.H. Beck, 2022, München.

KARA, Hacı: "Gemilerde Yapay Zekâ Kullanımı ve Buna Dair Hukuki Sorunlar", Süleyman Demirel Üniversitesi Hukuk Fakültesi, S. 2020-10/1, s. 17-51.

KARA, Hacı: Sigorta Hukuku, Oniki Levha, İstanbul, 2021. (Anılış: Sigorta Hukuku)

KARAYAZGAN, Ahmet: Hukuk Gözüyle Siber ve Sigorta, 1. Bası, Aristo, İstanbul, 2021.

KARAYAZGAN, Ahmet: Hukuki Yönüyle Siber Sigorta ve Sessiz Siber Teminatının Çalışma Esasları, Legal Hukuk Dergisi, C. 18, S. 215, Y. 2020, https://legalbank.net/belge/hukuki-yonuyle-siber-sigorta-ve-sessiz-siber-teminatinin-calisma-esaslari/4281775.

KENDER, Rayegan: Türkiye'de Hususi Sigorta Hukuku, 14. Bası, Oniki Levha, İstanbul, 2014.

LORENZ, Egon: "§ 1. Einführung", içinde: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 3. Auflage, C. H. Beck, München, 2015.

MALEK, Paul/**SCHILBACH**, Dan: "Versichertes Risiko in der Cyber-Versicherung – Umfang und Grenzen des Deckungsschutzes", VersR-Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht, S. 2019-21, s. 321-1330.

MALEK, Paul/**SCHÜTZ**, Camilla: "Cyberversicherung: Rechtliche und praktische Herausforderungen", r+s – recht und schaden, S. 2019-8, s. 421-429.

MEHRBREY, Kim Lars/**SCHREIBAUER**, Marcus: "Haftungsverhältnisse bei Cyber-Angriffen Ansprüche und Haftungsrisiken von Unternehmen und Organen", MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, S. 2016-2, s. 75-82.

PRÖLSS/MARTIN, Versicherungsvertragsgesetz: VVG-mit Nebengesetzen, Vertriebsrecht und Allgemeinen Versicherungsbedingungen, 31. Auflage, München 2021. (Anılış: Prölss/Martin VVG, Yazar)

RÜFFER, Wilfried/**HALBACH**, Dirk/**SCHIMIKOWSKI**, Peter: Versicherungsvertragsgesetz**,** 4. Auflage, Baden-Baden 2020. (Anılış: Rüffer/Halbach/Schimikowski VVG, Yazar, A-, N.-)

SCHEUERMANN, James E.: "Cyber Risks, Systemic Risks, and Cyber Insurance", Penn State Law Review, S. 2018-122/3, s. 613-644.

SCHILBACH, Dan: "Die Musterbedingungen des GDV für die Cyberrisiko-Versicherung", SpV-Spektrum für Verischerungsrecht, S. 2018-1, s. 2-4.

SELBY, Judy: "Understanding Cyber Insurance", International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, S. 2011-2/11, ss. 21-24.

TEKİN, Ufuk: "Hukukî Açıdan Siber Risk Sigortası", Genç Hukukçu Araştırmacılar Sempozyumu, 11-12 Ekim 2019, 2020, İstanbul, ss. 671-683.

ÜNAN, Samim: Türk Ticaret Kanunu Şerhi, Altıncı Kitap-Sigorta Hukuku, Cilt II, Oniki Levha, İstanbul, 2016. (Anılış: Cilt II)

ÜNAN, Samim: Türk Ticaret Kanunu Şerhi, Altıncı Kitap-Sigorta Hukuku, Cilt I, Oniki Levha, İstanbul, 2016.

VEITH, Jürgen/**GRÄFE**, Jürgen/**GEBERT**, Yvonne: Der Versicherungsprozess-Ansprüche und Verfahren Praxishandbuch, 4.

Auflage, Baden-Baden 2020. (Anılış: Veith/Gräfe/Gebert, Der Versicherungsprozess, §24, Yazar, N. -)

VICEVICH, David L.: "The Case for a Federal Cyber Insurance Program", Nebraska Law Review, S. 2018-97/2, s. 555-605.

YAZICIOĞLU, Emine/**ŞEKER ÖĞÜZ**, Zehra: Sigorta Hukuku, 3. Bası, Filiz, İstanbul 2020.