International
SMART JOURNAL
International SOCIAL MENTALITY AND RESEARCHER THINKERS Journal
e-ISSN: 2630-631X
Smart Journal 2021; 7(50) : 2449-2455
Doı : http://dx.doi.org/10.31576/smryj.1081
Arrival : 15/07/2021
Published : 23/09/2021
Original Article

SİGORTACILIKTA DİJİTALLEŞME VE SİBER GÜVENLİK İHLALLERİ

Digitalization In The Insurance And Cyber Security Breaches

Dr. Öğretim Üyesi. Serhat SOYŞEKERCİ
Çanakkale Onsekiz Mart Üniversitesi, Çanakkale,/TÜRKİYE
ORCID: https://orcid.org/0000-0002-8427-0184

Cite As: Soyşekerci, S. (2021). "Sigortacılıkta Dijitalleşme ve Siber Güvenlik İhlalleri", International Social Mentality and Researcher Thinkers Journal, (Issn:2630-631X) 7(50): 2449-2455

ÖZET

Sigorta güvence demektir. Sigortacılık sektörü ise teknolojide meydana gelen değişimlere bağlı olarak siber riskleri ve beraberinde güvenlik önlemlerini de karşımıza çıkarmaktadır. Teknoloji ile paralel olarak siber saldırılara karşı risk ve güvenlik de artmaktadır. Son yıllarda sıkça duyulmaya başlayan siber risk, doğal afet risklerinden öndedir. Bu da insanların geleneksel güvenlik anlayışında değişimi zorunlu kılmakta, sigorta şirketlerinin çıkardıkları siber risk sigortaları ile dünyada ve Türkiye'de teminatı ve işleyişi sağlayan uygulamalar hâline gelmektedir. Günümüzde dünyada yaklaşık 6 milyar akıllı cihaz bulut üzerinden birbirine bağlanırken, 2020'de bu rakam yaklaşık 20 milyarı bulmuştur. Buna rağmen gelişmiş ülkelerde siber güvenlik ihlallerine karşı sigortalı olanlar %31'i geçmemektedir. Bu oran gelişmiş ülkelerde geniş bir pazar payı olarak görülse bile, gelişmekte olan ülkelerde siber risklere karşı güvence sağlamada tecrübe eksikliği önemli risk unsuru hâlini almaktadır. Bu çalışma, günden güne dijitalleşen sigortacılık sektöründe güvenlik önlemleri ve olası riskleri, güvenlik ihlalleri bağlamında ele almaktadır.

Anahtar Kelimeler: Sigorta, siber risk sigortası, siber güvenlik, siber ihlaller.

ABSTRACT

The means of insurance is a guarantee. The insurance sector on the other hand, faces cyber risks and security measures due to technological changes. But in parallel with technology, the risk and security against cyber attacks also increases. Cyber risk, which has become common in recent years, is ahead of natural disaster risks. This, in turn, necessitates a change in people's traditional understanding of security, with Cyber risk Insurance issued by insurance companies, as well as practices that provide coverage and functioning in the world and in Turkey. In today's world about 6 billion smart devices are connected to each other via the cloud, while in 2020 this figure is about 20 billion. Despite this, those insured against cyber security breaches in developed countries do not exceed 31%. Although this ratio is seen as a wide Sunday share in developed countries, lack of experience in providing security against cyber risks in developing countries is an important risk element. This study examines security measures and possible risks in the insurance sector, which is digitizing day by day, in the context of security violations.

Keywords: Insurance, cyber risk insurance, cyber securaty, cyber violations.

1. GİRİŞ

Sigorta, Lâtincede *güvenlik* anlamına gelen *securitas* teriminden gelmektedir. *Cura* kökenine sahip bu terim; emniyet, koruma, göz kulak olma ve kaygı kelimelerinin de karşılığıdır (Çotak, 2019: 4). 6272 sayılı Türk Ticaret Kanunu'nun 1263. maddesinde yapılan tanıma göre; "Sigorta bir akittir ki bununla sigortacı bir prim karşılığında diğer bir kimsenin para ile ölçülebilir bir menfaatini halele uğratan bir tehlikenin meydana gelmesi hâlinde tazminat vermeyi yahut bir veya birkaç kimsenin hayatlarında meydana gelen belli birtakım hadiseler dolayısıyla bir para ödemeyi veya sair edalarda bulunmayı üzerne alır." (Yayar ve Daşçı, 2019: 11). Sigorta, "aynı ya da benzer risklere maruz bulunan kişiler topluluğunda risklerin gerçekleşmesi sonucu ortaya çıkan ihtiyaçların belli bir prim karşılığında giderilmesine yönelik sözleşme" (Çetintaş ve Biçen, 2012: 125) olduğu için *güvence* ve *teminat* kelimelerini de karşılamaktadır.

Dünyada sigortacılığa benzer ilk uygulamalara günümüzden yaklaşık 4000 yıl önce Babil'de rastlanmaktadır. Zamanın ticaret durumundaki Babil'de, kervan tüccarlarına borç veren sermayedarlar, kervanların soyulması veya fidye ödeme durumunda karşılaşmaları hâlinde tüccarların borçlarını silmekte, buna karşılık borcu tüccarlardan geri aldıkları zaman taşıdıkları riskin karşılığı olarak ana borcun miktarı üzerinden bir miktar para almaktaydılar. Bu olay sonraları Hammurabi Kanunları olarak yasallaştı. Bu kanunların en büyük özelliği, haydutların saldırısına uğrayan kervanların zararlarının bütün diğer kervanlar arasında paylaşılmasını öngörmesiydi. (Taş, 2015: 135; Başkır, 2015: 21). Günümüzdeki yapıya daha yakın olan "prim esaslı" sigorta ise milattan sonra 1250 yıllarında Venedik, Floransa ve Cenova şehirlerinde görülmüştür. Sigortacılığın gelişmesindeki en önemli faktör, bu yıllardan itibaren ekonomik koşulların değişmesi ve deniz ticaretindeki gelişmelerdir. 17. yüzyılda gemi ve yükünün sigorta edilebilmesi, kaptan, yolcular ve tayfaların da sigorta edilebilmesi fikrini doğurmuştur. Dünyada sigortacılığın gelişimi eski

tarihlere dayanmakla birlikte, Türkiye'de 19. yüzyılın ikinci yarısından önce sigortacılıktan söz etmek mümkün değildir. 19. yüzyılın ikinci yarısında İstanbul'da meydana gelen *Büyük Pera Yangını*'ndan sonra, burada ikamet etmekte olan kişilerin, yabancılarla ekonomik ilişkileri zengin kişiler olması, Türkiye'de sigortacılığın gelişimini hızlandırmıştır (Çetintaş ve Biçen, 2012: 125). 1872 yılında İngiliz sigorta şirketleri, açtıkları temsilciliklerle Türkiye'de ilk sigortacılık faaliyetlerini başlatmışlardır (Başkır, 2015: 21). Avrupa'da sigortacılık yaygın ve gelişmiş bir sektördür. Hâlihazırda Avrupa'da sigorta pazarı Türkiye'nin iki katıdır ve bu da Türk sigorta sektörünün %100 büyüme potansiyeline ihtiyaç duyduğunu göstermektedir (Özyalçın, 2017: 68). Swiss Re'nin yayınlamış olduğu *2013 Dünya Sigorta Raporu*'na göre, Avrupa ülkelerinin tamamının 2013 yılında ürettikleri toplam prim üretimi 1.631.699 milyon dolar, pazardan aldıkları pay ise %35,16 olarak gerçekleşmiştir. 2013 yılı verilerine göre, Avrupa sigorta endüstrisi küresel sigorta pazarında %35'lik pay ile dünyanın en büyük piyasasıdır. Türkiye ise 2013 yılında, 12.460 milyon dolarlık üretimiyle Avrupa ülkeleri arasında toplam prim üretiminde 19.sırada yer almıştır. Bu yönüyle Türk sigorta sektörü, toplam prim üretiminde gelişmiş birçok Avrupa ülkesine kıyasla geride kalmıştır (Taş, 2015: 140). *2019 Dünya Sigorta Raporu*'ndaki verilere göre, Avrupa ülkelerinin toplam prim üretimi 1.796.772 dolardır ve pazardan aldıkları pay ise %28.55'tir. 2019 yılı verilerine göre, dünyada en büyük pazar payına sahip ülke %39,10 pazar payı ile Birleşik Devletler'dir. Ülke bazında ikinci sırada %9,81 pazar payı ile Çin, üçüncü sıradaysa %7,30 payı ile Japonya yer almaktadır. Yine aynı raporun verilerine göre, 2019 yılında kişi başına düşen prim üretimi dünya ortalaması 818 dolardır. Türkiye'de ise kişi başına düşen prim üretimi 131 dolardır. Bu verilere göre Türkiye'de sigortalılık oranının düşük, sigorta pazarının büyümeye açık olduğu görülmektedir (Engin ve Karakuş, 2020: 181).

Türkiye'de sigortacılık yeni bir uygulama alanına sahiptir. *Sigorta Acenteleri Dünya Uygulamaları Araştırma ve 2023 Vizyonu Belirleme Raporu* verilerine göre, Türk müşterisinin dijital ortamdan sigorta poliçesi satın alma eğilimi düşüktür. Sigorta poliçesini İnternet üzerinden alanların oranı ise %8'dir (Ünlenen, 2018: 52). Ne var ki toplumlar dijitalleşme seviyelerine bağlı olarak, bilgi odaklı yaşamlarını sürdürdükleri ölçüde siber tehditlere de açık hâle gelmektedirler (Cebeci, 2021: 164). Dahası, bir ülkenin gelişmişlik düzeyi, siber risklere aynı oranda açık olduğunu gösterir. Her şeyden önce risk, anlam bakımından ikiye ayrılır. Bunlardan birincisi spekülatif risktir ve bu risk, gerçekleşip kayıplar doğurabileceği gibi, gerçekleşmemesi durumunda kişiye kâr sağlar. İkinci olarak gerçek risk, ekonomik ya da maddi açıdan kesin zarar getirebilen risktir ve bu anlamda sigortanın konusu değildir (Çotak, 2019: 6).

Sigortacılık bir hizmet sektörüdür. Müşterilerin tamamı somut ürüne dayalı satış ve pazarlama değil, soyut bir hizmet alır. Bu yüzden sigortacılığın temelinde sosyal güvenlik vardır ve bu da risklerden korunma güdüsüdür. Bu güdü, günlük hayatın akışında olası risklerden korunma düşüncesine dayanır (Karaman, 2018: 29-35). Özellikle satılan malın soyut bir ürün olması, kullanım zamanının belirsizliği ve kullanım hâlinde karşılıklı güvenin büyük önem taşıması, sigorta sektörü açısından güveni ön plana çıkarmaktadır (Yazıcı ve Yanık, 2010: 8). 2000'lerden sonra dijitalleşmenin giderek yaygınlaşmasıyla siber saldırılar ve bu alandaki riskler yükselmiş ve bu her geçen gün daha sofistike ve daha yıkıcı olmaya başlamıştır. Bunun için şirketler kendilerine "asla başımıza gelmez" diyebilme gibi bir alışkanlıktan kurtulmak zorundadırlar. Çünkü genelde örgütler, özelde ise şirketler, siber saldırılara karşı henüz bağışıklık kazanabilmiş değildir (Güler ve Arkın, 2019: 18). Dünyada yılda 556 milyon siber saldırı gerçekleşmekte ve Türkiye, en çok siber saldırıya uğrayan ülkeler arasında 9'uncu sırada yer almaktadır (Altuntaş vd., 2018: 10). Her geçen gün daha fazla şirket, verilerini ve markalarını tehdit eden riskleri asgari düzeye indirmek için sigorta güvencesi arama yoluna gitmektedir. Ancak dijitalleşmeyle beraber riskler artmakta, sigorta şirketleri ise dijital çözümler geliştirmek için müşteri beklentilerini anlamaya çalışmaktadır. Bu anlamda pek çok sigorta müşterisi acente ya da brokerlara gitmeden önce İnternette araştırma yaparak sosyal medya sitelerini ve blog yazıları rehber olarak değerlendirmektedir (Yurdakul ve Dalkılıç, 2016: 50).

2. SİGORTACILIKTA DİJİTALLEŞME

Sigortacılıkta dijitalleşme ya da dijital sigortacılık, "sigortacılıkla ilgili finansal hizmetlerin dijital çözümler yardımıyla uygulanması ve kullanılması" (Yurdakul ve Dalkılıç, 2016: 50; Ünlenen, 2018: 51) anlamına gelir. Dijital çözümler içinde sigorta hizmetinin satın alınması, poliçelerin uygulanması, hasar tazminat taleplerinin gerçekleştirilmesi ve kişiselleştirilmiş bilgilere erişim gibi işlemler söz konusudur. Dijital sigortacılık, sigorta poliçesinin pazarlanması sürecinde, sigorta şirketlerinde geçtiği aşamaların en az birinin elektronik ortamda yapılmasıdır (Ünlenen, 2018: 51). Sigorta sektörü, elektronik ya da dijital gelişmelere uyum sağlamaya çalışırken; bulut teknolojisi, akıllı mobil teknolojiler, giyilebilir cihazlar, dijital platformlar, yapay zekâ ve insansız hava araçları gibi teknolojinin diğer yeniliklerine de ayak uydurmaya çalışmak zorundadır. Örneğin bulut teknolojisi, herhangi bir kurulum gerektirmeyen, web tabanlı uygulamalarda

operasyonel kolaylık sağlayan en basit çevrimiçi depolama hizmetidir. Böylece büyük verilerin İnternet üzerinden depolanması ve kolaylıkla verilere erişimi mümkündür (Gönen vd., 1146). Dolayısıyla 2015 yılından sonra dünya genelinde çoğu sigorta şirketinin odak noktası teknoloji olmuştur. Örneğin 2015 yılında kurulan ve Almanya merkezli bir dijital sigorta girişimi olan *Getsafe*, başlangıçta Y kuşağını hedefleyen bir dijital sigortacı olarak kendisini tanıtmıştı. Şirketin kısa sürede Allianz ve Axa gibi oturmuş şirketlerden daha fazla poliçe satması, yeni ürünler kullanmasıyla öne çıktığını ve bu konuda başarılı olduğunu göstermektedir. Türkiye'de, benzer şekilde *Vodafone*, müşterilerine dijital ortamda teklifler sunmak amacıyla Vodafone Sigorta Aracılık Hizmetleri A.Ş.'yi kurmuş ve geniş bir müşteri ağı oluşturmuştur (webrazzi.com).

Yukarıdaki örnekler dikkate alındığında, şirketlerin son yıllarda ürün sınıflandırma ve müşteri ilişkilerini güçlendirmek için dijital platformlarda yatırım yapmaya başladıkları görülmektedir. Bütün bunlar veri ihlallerini de beraberinde getirmekte ve teknolojinin iki uçlu kılıç olduğunu göstermektedir (Özyalçın, 2017: 2-10). Buna rağmen bugün gelişmiş ülkelerde siber güvenlik ihlallerine karşı sigortalı olanların oranı %31'i (Altuntaş vd.,2018: 9) geçmemektedir. Aslında bu oranın düşük olması, sigortacıkta dijitalleşmenin isteneni veremediğine dair önemli bir soruna da temas eder. Bugün dünyada Siber Güvenlik Uzmanı adıyla bir işkolu söz konusudur ki şu anda Türkiye'de bir Siber Güvenlik Uzmanı maaşı 8.500 TL iken, en düşük 3.500 TL ve en yüksek 17.800 TL olarak değişebilmektedir (haberall.com). Her şeyden önemlisi dijitalleşme, değişen ve çeşitlenen müşteri beklentilerine yanıt vermek amacıyla çevrimiçi ekosistemin bir parçasıdır. Ancak sigorta sektörü, düşük yatırım maliyeti, düşük aracı ve hizmet maliyeti, bilgiye kolay ulaşım, gerçek kullanıcı yorumları, yüksek ürün çeşitliliği, kolay satın alma ve hızlı destek gibi temel parametreler dikkate alındığında, bu parametrelerin dijital sigortacılıkta zayıf yanlar olarak öne çıktığı söylenebilir (sigortastrateji.com).

2.1. Siber Saldırılar, Siber Güvenlik, Risk ve Sigorta

Siber [*İng*. Cyber] kelimesi sanal gerçeklik, İnternete ait olan ve İnternet ağlarına bağlı olan anlamına gelir. Başka bir tanıma göre, "İnternet, bilgisayar sistemleri, iletişim ağları ve kontrol birimlerini içeren teknolojik altyapının meydana getirdiği birbirine bağlı ağların oluşturduğu alana verilen isimdir (Şekeroğlu ve Özüdoğru, 2019: 56). Bununla beraber siber, saldırılara karşı bir risk unsurudur ve çoğu sektörde olduğu gibi, sigortacılık sektörü için de bir tehdittir (Özyalçın, 2017: 65). Bu anlamda teknoloji, siber alana gömülü bir mantığı ifade etmekte ve siber terörizm olarak nitelenen yeni tür terörizmi ortaya çıkarmaktadır (Terzi, 2019: 214). Siber alanlar 1980 ve 1990'larda teknoloji ve İnternetin yaygınlaşmasıyla hızla gelişmiş ve bu da yeni sorunları beraberinde getirmiştir. Siber ortamın sağladığı kolaylıklar kişi ve kurumları bu ortama bağlarken, bu ortamın korsanları olan hackerlar tarafından saldırılara maruz kalmaktadır. Örneğin çoğu siber işgalci, İnternette web etki alanlarının tescilini almakta ve bunu kurulu başka şirketlere ya da marka sahiplerine satmayı amaçlamaktadır. Siber suçlular, tanınmış bir şirkete ait gibi görünen bir web sitesinin tescilini alarak ziyaretçileri siteye çekerek tuzağa düşürebilmektedir. Dolayısıyla kişi, sektör, kurum ve ülke çapında saldırıların artmasıyla, siber ortamda güvenliğin yeri ve önemi de tartışılır hâle gelmektedir.

Günümüzde çok çeşitli türde siber saldırılar gerçekleşmektedir. Bu saldırılardan en bilinenleri; fidyeleme (ransomware), nesnelerin İnterneti (the Internet of things), sosyal mühendislik (social engineering), oltalama (phishing), kırma (cracking), ortadaki adam saldırısı (man-in-the-middle attack) şeklindedir (Cebeci, 2021: 166). *Fidyeleme*, bir cihazı kilitleyebilen ya da sahibinden para koparmak amacıyla içeriklerini şifreleyen kötü amaçlı yazılımlardır. *Nesnelerin İnterneti*, birbirine bağlanarak bilgi akışı sağlayan, belirli haberleşme kanalları vasıtasıyla ağ oluşturan cihazlar sistemidir. *Sosyal mühendislik*, kişileri maniple ederek belirli eylemleri yaptırmayı hedefleyen veya kişiye özel bilgileri açığa çıkarmaya çalışan eylemdir. *Oltalama,* kurbanı aldatan saldırganın kurbana ait gizli bilgileri (şifre, kredi kartı, banka hesap numarası bilgileri gibi) ele geçirmesidir. *Kırma*, kişinin bütün finansal bilgilerini ele geçirmektir. *Ortadaki adam saldırısı* ise saldırganın kullanıcı ile sunucu arasında geçen iletişimi dinleyerek bunu ele geçirmesidir (Cebeci, 2021: 171). Yapılan araştırmaya göre şu ana dek en ses getiren siber saldırı 12 Mart 2017 tarihinde Avrupa ülkelerinde etkisinin görüldüğü "WannaCry" adlı bir siber saldırıdır. Uzmanlar bu saldırıyı bu tarihe kadar gerçekleştirilmiş en yaygın ve en büyük siber saldırı olarak değerlendirilmiştir. Hastaneler başta olmak üzere pek çok kurumu etkilemiştir (Selimoğlu ve Altunel, 2019: 7). Böyle bir siber saldırı, teknoloji ve yazılım alanında gerçekleşmiş olan gerçek bir virüs salgınıdır ve tıbbi cihazlar da dâhil olmak üzere tüm cihazları şifrelemiş, bazı fabrikaların üretimlerini durdurmaya zorlamıştır. Kuşkusuz bununla birlikte, "NotPetya" gibi küresel düzeyde etkisi olan ve birçok şirketi etkileyen siber bir saldırının gerçekleşmesi de, bu tür saldırıların devamının gelebileceği konusunda fikirler ortaya atılmasına sebebiyet vermektedir (Çotak, 2019: 1). Diğer yandan, çalışma sistemi aynı olmakla birlikte, maliyetiyle en yüksek salgın unvanına sahip olan "WannaCry" değil, "NotPetya" olmuştur. Siber alanda güvenli bilgi akışının sağlanması, verilerin kontrol altında güvenli

şekilde saklanması, kişi ve şirket bilgilerinin gizliliği hususunda güvenlik açısından farklı ve yeni yollar aransa da, gelişen teknoloji, korsanların birçok strateji ile kişisel veya kurumsal sisteme sızma yollarını arttırmaktadır. 2027 yılına kadar küresel temelde hesaplanan siber güvenlik harcama bütçesinin 10 milyar doların üstünde olacağı tahmin edilmektedir. Muhtemelen bu bütçe, 10 milyar dolar olan "NotPetya" siber saldırısının yol açtığı bir maliyetin baz alınmasıyla oluşturulmuştur. Bu konuda NATO, kendisine yeni güvenlik gündemi oluşturarak ilerleyen dönemlerde güvenlik gündemine *siber risk ve tehditleri* eklemesi, inşa sürecinin gündelik olarak devam ettiğini ya da bu sürecin uluslararası ilişkilerin hızlı değişen yapısına bağımlı olarak hareket ettiğini göstermektedir (Erendor, 2016: 118).

Ponemon Enstitüsü tarafından 2012 yılında yapılan bir çalışmada, son üç yılda haftalık başarılı siber saldırı sayısı ortalamasının 50'den 102'ye çıktığı, ortalama saldırılardan kurtarma süresinin 12'den 24 güne çıktığı, şirket başına yıllık ortalama kayıp maliyetinin ise 5,5 milyondan 8,9 milyon dolara çıktığı belirtilmiştir. Buradan da anlaşılacağı üzere, siber güvenliği elektronik ve bilgisayar bilimi yanında, ekonomik açıdan da ele almak bir zorunluluk hâline gelmektedir (Şentürk vd., 2016: 40). Siber saldırıların yarısından fazlası küçük şirketlere yöneliktir. Bunun sebebi, bu şirketlerin siber tehditleri önemsemeyip, siber güvenlik için harcanacak meblağı gereksiz harcama olarak görmesinden kaynaklanmaktadır (Şekeroğlu ve Özüdoğru, 2019: 57). Ayrıca küçük şirketler siber tehditlere karşı koyabilecek yetkin bir işgücü ve kaynağa da sahip değildir. *Bilgi Güvenliği İhlali Anketi* (2015) sonuçlarına göre, büyük ve kurumsal şirketlerin %90'ı bilgi güvenliği suçu raporlarken, küçük ve orta büyüklükteki şirketlerin %74'ü bilgi güvenliği suçu raporlamıştır. Yine anket sonuçlarına göre, büyük şirketlerdeki suçların %75'i çalışanlarla ilgilidir. Ayrıca bu anketi yürüten siber güvenlik direktörü, anketi yanıtlayan 10 şirketten 9'unun şirketinde siber suçu raporladığını belirterek, şirketlerin siber suçlarla nasıl mücadele edeceğinin bilinmesi gereğinden bahsetmiştir (Kurt ve Uysal, 2015: 2). Siber saldırılara maruz kalan şirketlerin finansal zararlarının yanı sıra, itibarlarının zedelenmesi negatif sonuçlar doğurmakta, şirketler bu zarara karşı sigorta poliçeleriyle korunabilmektedir. Sigorta poliçeleri, kurumsal ya da kişisel veri ihlali sebebiyle ortaya çıkacak zararları ve itibar kaybını önlemek için yapılması gereken masrafları ve riskten doğan zararları karşılamaktadır (Şekeroğlu ve Özüdoğru, 2019: 61).

Sigorta, varlığı bilinmeyen, ileride meydana gelme ihtimali bulunan tehlikelere karşı bireyleri ve varlıkları yaşanacak tehlikelerden doğan zararların giderilmesi için önceden yapılan ödemeye dayalı bir güvenceyi kapsar (Taş, 2015: 134). Bu yönüyle, sigorta ile risk arasında çok yakın bir ilişki vardır. Üstelik siber güvenlik açıklıkları çoğunlukla belirsizdir. Bu nedenle, saldırıya açık bir platform olmasından ötürü risk barındırır (Gönen vd., 2021: 1147). Bu bağlamda siber risk sigortası veya siber güvenlik sigortası, bilişim sektöründe faaliyette bulunan şirketler ve bu sektörün ortaya çıkardığı yazılımları kullanan firmalar, veri depolarken üzerlerine aldıkları riskleri bu poliçeler aracılığıyla ortadan kaldırabilirler. Siber risk sigortaları; şirketler, müşterilerin kredi kartı, hesap numarası, adres ve benzeri kişisel bilgilerini bazı yazılımlarla depolamaktadırlar. Bu verilerin güvenliğinden sorumlu olan şirketler, depolanan verilerin çeşitli yasa dışı yöntemlerle yetkisiz şahısların eline geçmesinden dolayı oluşacak zararları bu tür özel poliçelerle karşılayabilmektedirler (Cebeci, 2021: 172). Bu yönüyle siber poliçe, sigortalı olanlara yönelik kimlik hırsızlığı, ödeme araçlarını hileli ve kötüye kullanma gibi olumsuzluklara karşı güvence oluşturmaktadır.

2.2. Siber Risk Sigortası

Dünya üzerinde pek çok şirket, siber saldırılara karşı teminat oluşturmak için daha fazla siber risk sigortasına yönelmektedir (Selimoğlu ve Aktunel, 2019: 7). Şirketlerin siber güvenlik riski nedeniyle oluşabilecek veri koruma hasarları, iş faaliyetlerinin durmasından kaynaklanan zararlar, idari para cezaları, siber fidye masrafları, bilgi güvenliği, gizlilik sorumluluğu ve veri ihlali masrafları, siber risk sigortası kapsamında değerlendirilmektedir. Birleşik Devletler'de 2013 yılı itibariyle siber sigorta hizmeti sağlayan otuzun üzerinde sigorta şirketi olduğu, mevcut sigorta primlerinin genellikle 10 bin dolar ile 25 bin dolar arasında olmakla beraber, kapsama durumuna göre 50 milyon dolara kadar çıkabildiği, poliçe kapsamlarının birbirinden farklılık gösterdiği belirtilmiştir (Şentürk vd., 2016: 43). Türkiye'de İnternet kullanımın yaygınlaşmasıyla birlikte siber risk sigortasının da artacağı tahmin edilmektedir. Şöyle ki, Türkiye İstatistik Kurumunun 19.09.2017 tarihinde yayınladığı *Hanelerde Bilişim Teknolojileri Kullanımı Araştırması Raporu'*na göre, 16-74 yaş arası 2017 yılı toplam İnternet kullanımı oranı %66,8'dir. Hanelerde internet erişimi oranı ise %80,7'dir. Son 5 yıllık (2013-2017) sürece göre, 2013 yılında, toplam İnternet kullanımı oranı %48,9 ve internet erişimi oranı %49,1'dir. Bu sonuçlara göre bireysel İnternet kullanımı oranı son 5 yılda %17,9 ve toplam internet kullanımı oranı ise %31,6 artmıştır (Yıldırım, 2018: 2). Bireysel olarak İnternete erişim ve İnternet kullanımının giderek artması, doğal olarak siber tehditleri de beraberinde

getirmektedir. Gün geçtikçe İnternet kullanım oranı artmaktadır. Bu da dijital sigortacılık açısından bakıldığında, müşteri potansiyelinin de artabileceği anlamına gelmektedir.

Ne var ki siber saldırılar genellikle şirketlerin veri tabanlarına yöneliktir. Herhangi bir siber saldırı sonucunda veri tabanının kullanılamaz hâle gelmesi gibi sebeplerden dolayı verilen idari cezalardan doğan zararlar, siber risk sigortası kapsamında tazmin edilmektedir. Sigorta sektörü açısından değerlendirildiğinde bu bir teminat veya güvence demektir. Ancak siber güvenlik sigortası şahısların uğradığı bedensel zararlardan ve mallara gelen hasarlardan sorumlu değildir. Örneğin Ukrayna kaynaklı çevrimiçi devlet sitelerinin yanı sıra, finans ve enerji şirketlerine ait sitelere 2017'de "NotPetya" fidye yazılımı ile yapılan saldırılar yaklaşık olarak 300 milyon dolarlık zarara neden olmuş, CIA bu saldırının Rus askeri siber savaş birimlerince yapıldığını öne sürmüştür. Bu gibi olumsuz sonuçların diğer ülkelere yansıması ve olası tehditlerin küresel sorun hâline gelmesi, bu saldırıyı daha önceki saldırılardan farklı kılmıştır. Dolayısıyla siber alanda meydana gelebilecek her türlü riske karşı eylem planı hazırlanmalı, bu alanda "siber risk sigortası" sistemini geliştirerek meydana gelebilecek kayıplara yönelik eskiye dönüş imkânı sağlanmalıdır (Yenal ve Akdemir, 2020: 430- 436). Diğer bir ifadeyle, "WannaCry" ve "NotPetya" gibi çok büyük siber saldırılar nedeniyle yapılan fidye ödemelerinin sigorta teminatı kapsamında tazmin edilmesi için sigorta poliçesinde risklerin teminat kapsamında olduğu belirtilmelidir. Çünkü her şeyden önce siber güvenlik, veri, işlem, süreç, politika, deneyim, kapasite, insan ve sistemlerin siber ortamda sağlanmasıdır (Özkaya vd., 2019: 25). Bu sayede siber alandaki riskler *"kaçırılma-fidye sigortası"* teminatı kapsamına alınabilecektir (Light, 2019: 1136-1137). Siber güvenlik alanında şirketlerin yapmış olduğu çalışmalar olumlu olmakla birlikte, kayıp ve zararların karşılanması ve eskiye dönüş imkânının ortaya konulabilmesi için kayıpları önleyecek daha güçlü sistemlerin geliştirilmesi gerekir.

3. SONUÇ

Sigorta bir tür güvence, ya da bir nevi teminattır. Sigortacılık ise hizmet sektörü olduğu için müşterilerin tamamını somut bir ürüne dayalı satışa ve pazarlamaya değil, soyut bir hizmete yöneltir. Bu yüzden sigortacılığın temeli güven esasına dayanır ki, bu da en başta sosyal güvenliğin varlığını gerektirir. Ne var ki teknoloji ve dijitalleşmeyle birlikte siber güvenliğin olduğu her ortamda siber saldırılar da olabilmektedir. Bundan dolayı sigortacılık sektöründe dijitalleşme, şirketlerin siber sigorta konusuna verdikleri önem kadar, siber güvenlik konusuna da aynı hassasiyetle yaklaşmalarını öne çıkarır. Büyük, orta ve küçük boy şirketlere siber saldırının olduğu her sistemde siber güvenlik söz konusudur. Fidyeleme, nesnelerin İnterneti, sosyal mühendislik, oltalama, kırma, ortadaki adam saldırısı şeklinde gerçekleşebilen saldırılar karşısında güvenliğin tesis edilmesi kaçınılmaz bir gerçektir. Çeşitli tür ve biçimlerde gerçekleşen siber saldırılar gibi, siber güvenliğe yönelik tehditlerin de sürekli değiştiği, giderek karmaşık hâle geldiği ve diğer yandan yeni sistemlere uyum sağlamanın da bir zorunluluk olduğu düşünüldüğünde, güvenlik açığını bulup önlem almaya çalışmak neredeyse imkânsız hâle gelebilmektedir. Özellikle siber saldırı ve siber güvelik arasında kurulabilecek bir sürece geniş bütçe, işgücü ve kaynak ayırabilme olanağından yoksun olan küçük şirketler için bu durum bazen işin içinden çıkılamaz hâle gelmektedir. *2013 Dünya Sigorta Raporu* verilerine göre, Avrupa sigorta endüstrisi küresel sigorta pazarının en büyük pazar payına sahipti. Ancak *2019 Dünya Sigorta Raporu* verilere göre dünyada en büyük pazar payına sahip ülkenin Birleşik Devletler olduğu görülmektedir. Buna göre Türk sigorta sektörü, toplam prim üretiminde gelişmiş birçok Avrupa ülkesine kıyasla geridedir. Diğer taraftan, Türkiye'de sigortacılık bölüm ve programlarından mezun olanların sigorta şirketleri personeli içindeki payı ise sadece %1-3 düzeyinde seyretmektedir. Bu durum sigortacılık bölüm/programlarından mezun olan öğrencilerden sektörün yararlanamadığını göstermektedir. Diğer bir ifadeyle, verilen sigorta eğitimi, sigorta sektörü istihdamına yansımamaktadır (Çelikkol ve Dalkılıç, 2010: 77). Bütün bu gelişmeler ve sorunlar dikkate alındığında, Türkiye'nin dijital sigortacılıkta gelişmeye açık bir pazar olmasına rağmen, teknoloji ve bilişim alanında yapılanmaya, ivmelenmeye ve özellikle sigorta sektörünün pazar koşullarını dikkate alacak bir potansiyeli harekete geçirmeye ihtiyacı vardır.

KAYNAKÇA

Altuntaş, Eda, Kara, E., Soylu A.B., Kırkbeşoğlu, E., "Siber sigortalar: son gelişmeler, uygulamalar ve sorunlar", *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, 12: 8-22, 2018.

Başkır, M. Bahar, "Sigorta piyasasında finansal performansın klasik ve bulanık öbekleme yöntemleri ile incelenmesi", *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, 2(7-8): 19-33, 2015.

Cebeci, İpek, "Türkiye'de siber risk sigortalarına ilişkin bir değerlendirme", *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 56(1): 163-188, 2021.

Çelikkol, Hakan; Dalkılıç, Nilüfer, "Türkiye'de sigorta sektöründe istihdam, eğitim ve geleceğe ilişkin öneriler", *Ekonomi Bilimleri Dergisi*, 2(2): 73-80, 2010.

Çetintaş, Hakan; Biçen, Ömer Faruk, "Türkiye'de sigortacılık sektörünün etkinlik analizi", *TİSK Akademi*, II: 124-154, 2012.

Çotak, Alperen, "Sigortacılık sektöründe siber güvenliği, dünyada ve Türkiye'deki gelişmelerin incelenmesi", Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2019.

Engin, Cem; Karakuş, Burak, "Dünya, Avrupa Birliği ve Türkiye'de sigorta sektörü", *Kahramanmaraş Sütçü İmam Üniversitesi Dergisi*, 2020, 173-189.

Erendor, Mehmet Emin, "Risk toplumu ve refleksif modernleşme çerçevesinde siber terörizm: tanımlama ve tipoloji sorunu", *Cyberpolitik Journal*, 1(1): 114-133, 2016.

Gönen, Serkan; Yılmaz, Ercan Nurcan; Sanoğlu, Seda; Karacayılmaz, Gökçe; Özbiirinci, Özge, "Endüstri 4.0'ın gelişim sürecinde unutulan bileşen: Siber güvenlik", *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 9: 1142-1158, 2021.

Güler, Alptuğ; Arkın, Ali Kasım, "Siber hijyenin sağlanmasında iç denetimin rolü", *Denetişim*, 9(19): 17-40, 2019.

Karaman, Davut, "Sigortacılık sektörünün güncel sorunlarının belirlenmesi: Alanya'da bir araştırma", *Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi*, 5(10): 28-37, 2018.

Kurt, Ganite; Uysal, Tuğba Uçma, "Siber riskler ve COSO iç kontrol bütünleşik çerçevesi", *Muhasebe ve Denetime Bakış*, 15(46): 1-10, 2014.

Light, Didem Algantürk, "Siber tehlikelerin denizcilik sektörüne etkisi", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 2(2): 1131-1137, 2019.

Özkaya, Erdal; Sarıca, Raif; Durmaz, Şükrü, *Siber Güvenlik*, Buzdağı Yayınevi, İstanbul, 2019.

Özyalçın, Zehra Cemre, "Türk sigorta sektörünün gelecek perspektifi: Sorunsuz çözüm önerileri üzerine bir araştırma", İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü, *Yüksek Lisans Tezi*, İstanbul, 2017.

Selimoğlu, Seval; Altunel, Mehtap, "Siber güvenlik risklerinden korunmada köprü ve katalizör olarak iç denetim", *Denetişim*, 9(19): 5-16, 2019.

Şekeroğlu, Sinan; Özüdoğru, Haşim, "Dijital dönemin koruyucuları: Siber risk sigortaları", *4. International Research Congress on Social Sciences*, 11-13 September, 55-64, 2019.

Şentürk, Hakan; Çil, Celal Zaim; Sağıroğlu, Şeref, "Siber güvenlik yatırım kararları üzerine literatür incelemesi", *Politeknik Dergisi*, 19(1): 39-51, 2016.

Taş, Merve Kayaköy, "Dünya sigorta pazarında Türkiye'nin yeri", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 14(27): 133-148, 2015.

Terzi, Mahir, "E-Government and cyber terrorism: Conceptual framework, theoretical discussions and possible solutions", *Turkish Journal of TESAM Academy*, 6(1): 213-247, 2019.

Ünlenen, Fatma Burcu, "Ankara ilinde konut poliçesi hasarı oluşan sigortalıların sigorta farkındalığı", Başkent Üniversitesi Sosyal Bilimler Enstitüsü, *Yüksek Lisans Tezi*, Ankara, 2018.

Yayar, Rüştü; Daşçı, Ayşenur, "Kasko sigortası tercihini etkileyen faktörler: Kars ili örneği", *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, 13: 8-21, 2019.

Yayla, Şerafettin Okan, "Sigortacılık ve Türkiye'de sigorta sektörünün durumu", *Liberal Düşünce Dergisi*, 24(94): 107-125.

Yazıcı, Selim; Yanık, Serhat, "Sigorta sektöründe kurumsal yönetim ve kurumsal yönetim komitesinin rolü", *İstanbul Üniversitesi İktisat Fakültesi Mecmuası*, 60(2): 1-22, 2010.

Yenal, Serkan; Akdemir, Naci, "Uluslararası ilişkilerde yeni bir kuvvet çarpanı: Siber savaşlar üzerine bir vaka analizi", *ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi*, 11(1): 414-450, 2020.

Yıldırım, Ebru Yeniman, "Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması", *Mesleki Bilimler Dergisi*, 7(2): 1-11, 2018.

Yurdakul, Müberra, Dalkılıç, N., "Sigortacılık sektöründe dijital çağ", Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 50: 49-67, 2016.

http://webrazzi.com/2020/12/08/dijital-sigortacilik-girisimi-getsafe-30

http://webrazzi.com/2021/03/09/vodafone-dijital-sigorta

http://sigortastrateji.com/global-trendler/dijital-sigortacilik/2021.

http://haberall.com/ siber-guvenlik-ne-kadar-maas-alır/2021.