BSAD

ISSN: 1309-1859

Bankacılık ve Sigortacılık Araştırmaları Dergisi

Journal of Banking and Insurance Review

Sayı 12 (Aralık 2018)

Ankara Üniversitesi Beypazarı Meslek Yüksekokulu

BSAD

ISSN: 1309-1859

Bankacılık ve Sigortacılık Araştırmaları Dergisi hakemli bir dergidir.

Journal of Banking and Insurance Review

Sayı 12, Aralık 2018

Yayın aralığı (periyod): 6 ayda bir

Yayın tarihi: 28 Aralık 2018

Ankara Üniversitesi Beypazarı Meslek Yüksekokulu

ISSN: 1309-1859

http://dergipark.gov.tr/bsad

E-posta : editor.bsad@gmail.com

basaran@ankara.edu.tr

BSAD
Bankacılık ve Sigortacılık Araştırmaları Dergisi
Journal of Banking and Insurance Review
Sayı 12, Aralık 2018

Yayın Sahibinin Adı: Ankara Üniversitesi Beypazarı Meslek Yüksekokulu adına Prof. Dr. Timur GÜLTEKİN
Baş Editör: Asuman TURANBOY, Prof. Dr. (Ankara Üniversitesi)
Editör Yardımcıları: Ali BAŞARAN, Dr. Öğr. Üyesi (Karabük Üniversitesi), İlker ÖZDEMİR, Doç. Dr. (Çukurova Üniversitesi), Murat ÖZBOLAT, Okt. (Ankara Üniversitesi), Mustafa Cumhur AKBULUT, Öğr. Gör. Dr. (Ankara Üniversitesi)
Sorumlu Yazı işleri Müdürü: Sabri Serkan KIZILSU, Öğr. Gör. (Ankara Üniversitesi)
Yayın İdare Merkezi Adresi: Ankara Üniversitesi Beypazarı Meslek Yüksekokulu Milli Egemenlik Cad. No:206 06730 Beypazarı/Ankara e-posta: editor.bsad@gmail.com
Yayın İdare Merkezi Telefonu: 0 312 763 30 22 Belgeç: 0 312 763 30 20
Yayın Türü: Süreli dergi
Elektronik Yayın Türü: http (Kısıtsız tam açık erişim)
Yayın Sıklığı: 6 ayda bir
Yayın Dilleri: Türkçe, İngilizce

Ankara Üniversitesi Beypazarı MYO

ISSN: 1309-1859

http://dergipark.gov.tr/bsad
E-posta: editor.bsad@gmail.com
basaran@ankara.edu.tr

Odak ve Kapsam

BSAD yılda iki kez, elektronik ortamda yayınlanmaktadır. Türkçe ve İngilizce dillerinde makale kabul edilmektedir. Yayınlanacak makaleler Türkiye'de ve Dünya'da bankacılık ve sigortacılık sahasını konu edinir. Anılan sahada kuram ve uygulamalar ile kitap tanıtımları yayınlanır. Ayrıca ikincil olarak ilgili kişiler, yayın ve editörler kurulunca, mutabakatla 10 Mayıs 2017 tarihinde bankacılık ve sigortacılık sahası ile dolaylı alakalı konuların da (altın, altın hesapları, altın piyasası, döviz, döviz hesapları, döviz piyasası, kur hareketleri, faiz oranları, bankaların iştirakleri, sermaye piyasası, bankaların ve sigorta şirketlerinin aktif ve pasifini oluşturan kalemler, merkez bankalarının bilanço kalemleri ile ödemeler bilançosu kalemleri) gerek ve uygun görülürse değerlendirmeye alınması kararlaştırılmıştır. Anılan öncelikli saha ve dolaylı alakalı konularda kuram ve uygulamalar ile kitap tanıtımları yayımlanır. Dergi özel sayı da çıkartabilir.

Taranan indeksler ya da veri tabanları ya da keşif araçları: Ankara Üniversitesi Dergiler Veritabanı, Google Akademik, SOBİAD Sosyal Bilimler Atıf Dizini, EBSCO Keşif Aracı

Erişilen atıf bağlantı hizmeti: Crossref

Başvuru süreci devam eden indeksler ya da veri tabanlar ya da açık erişim platformları: TÜBİTAK ULAKBİM CABİM-Cahit Arf Bilgi Merkezi TR Dizin, Arastirmax, Proquest Open Academic Journal Index Directory of Open Access Journals (DOAJ)

Yazım Kuralları

BSAD'nin hedeflediği dizinlerin istediği güncel ölçütlere göre yazılar kabul ya da ret edilmektedir.

Öncelikle yazı önerinizi iletmeden önce güncel "TÜBİTAK ULAKBİM TÜRKİYE DERGİLERİ DİZİNİ (TR Dizin) DERGİ DEĞERLENDİRME KRİTERLERİ TR"de (2017 yılı için http://cabim.ulakbim.gov.tr/tr-dizin/tr-dizin-dergi-degerlendirme-kriterleri/) belirtilen ölçütleri karşıladığından emin olunuz.

Makalenizi aşağıdaki bağlantıdan bilgisayarınıza indireceğiniz şablona göre düzenleyiniz.

https://www.dropbox.com/s/uoiqm4litihoxtz/sablon_ornek_04122017.docx?dl=0

Kurgu

Makale yazımında aşağıdaki aşamaları, kurguyu mümkün olduğunca tercih ediniz.

Öz
Abstract
GİRİŞ
1. İLGİLİ ÇALIŞMALAR
2. YÖNTEM
2.1. Çalışmanın Amacı
2.2. Veri Toplama
2.3. Geçerlik ve Güvenirlik
3. BULGULAR
3.1.
3.2.
SONUÇ VE TARTIŞMA
Kaynaklar
Ek/Ekler
Yazar adlarının silinmesi

Başvuruların bağımsız değerlendirilmesi, yazar ve hakem kimliklerinin birbirlerine bildirilmemesi için gayret gösterilmektedir. Bu amaçla açık dergi sistemine (ADS/OJS) dosya gönderen yazarın metin ve dosyalar ile ilgili aşağıdaki noktalara dikkat etmeleri gerekir.

Yazarlar metinde adları ve kurumları geçen yerleri silmelidirler. Sayfa altı notları vb. yan metinler dâhil olmak üzere.

Microsoft Word belgeleri saklanır iken dosya bilgileri içine kişisel bilgiler de yazılır. Bu nedenle ya bu kişisel bilgiler belge özelliklerinden bulunup silinmeli ya da aşağıdaki sıra ile belge kişisel bilgi içermeyecek biçimde yeniden kaydedilmelidir. (File > Save As > Tools (or Options with a Mac) > Security > Remove personal information from file properties on save > Save) (Dosya > Farklı Kaydet > Araçlar > Güvenlik > Kişisel bilgileri silerek kaydet > Kaydet)

PDF dosyalarda da Adobe Acrobat ana menüsünden belge özellikleri seçilerek, yazar adı silinmelidir.

Atıflar

İlke olarak APA 6th edisyon ile düzenlenmelidir.

Kaynaklar

İlke olarak APA 6th edisyon ile düzenlenmelidir.

Diğer kurullar

Yazı önerinizi geri çekme hakkınızı kullanırken etik ilkelere aykırı hareket etmeyiniz. Örneğin yazınızın hakem değerlendirme süreçleri tamamlandıktan sonra geri çekilmesi BSAD hakem ve editörlerinin BSAD açısından emeklerinin zayi olmasına yol açacağını unutmayınız.

Diğer kurallar için bir önceki sayıda yayınlanan eserlere bakılabilir. Ayrıca öncelikle http://editor.ankara.edu.tr/index.php/bankavesigorta/information/authors gerekli açıklamayı bulamaz iseniz http://www.apastyle.org/index.aspx yine bulamaz iseniz http://mtad.humanity.ankara.edu.tr/yilkeleri.php adresini ziyaret ediniz. Bir tereddüt durumunda editor.bsad@gmail.com adresine e-posta yazabilirsiniz.

Dizgi, sayfa düzeni, sayfa numaraları verme aşamasında (mizanpaj) oluşacak hatalar için yazar/yazarlardan ancak bir sonraki sayının yayınına kadar yazılı değişiklik talebi gelmesi halinde bir sonraki sayıda düzeltme gerekli görülürse düzeltme yayınlanır.

Önerilen yazılar 6.000 kelimeyi geçmesi durumunda yazardan 6.000 kelimeye indirmesi istenebilir.

Dergide yayınlanan tüm yazıların ilmi ve fikri, etik sorumluluğu yazarına/yazarlarına aittir.

Makale sonuna yazar, yazı ve hakem bilgileri eklenir.

Değerlendirme İlkeleri

Makaleler https://www.dropbox.com/s/uoiqm4litihoxtz/sablon_ornek_04122017.docx?dl=0 bağlantıdan bilgisayarınıza indireceğiniz şablona göre düzenlenmemişse hakemlik süreci girmeden yazar/yazarlarına iade edilir. Yazılar, editörler tarafından uygun bulunduğu takdirde, değerlendirme için iki ya da üç hakeme gönderilir. Kitap tanıtmaları buna tabi değildir. Hakemlerin ismi gizli tutulur. Yazıları editörler ve yayın kurulu da gözden geçirebilir ve öneride bulunabilir. Editör ve yardımcı editörler yazıların ve hakemlerin takibini yapar. Bankacılık ve Sigortacılık Araştırmaları Dergisi daha önce baskı olarak veya elektronik ortamda yayınlanmış

çalışmaları dikkate almaz. Yazılar değerlendirme süreci tamamlandığında yazarına gerekli yönlendirmeler için geri gönderilir.

Makaleler en az iki hakemin aşağıda önerilen raporlamasına göre değerlendirileceğinden yazarların eserlerini göndermeden önce kendilerinin değerlendirmesi tavsiye edilir.

Bu değerlendirme formu tüm makale önerileri için kullanılacaktır / This review form is to be used for all submissions to the articles section.

Anlatım açıklığı / Clearness *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)
- ( ) Other

Kurgu / Research design *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)
- ( ) Other

Yazım kurallarına uygunluk / Convenience to writing rules *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)
- ( ) Other

Gerekliliği / Necessity *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)
- ( ) Other

Atıf alma ihtimali / Probability of citing *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)

Uygulamaya (iş yaşamına) katkısı / Contribution to business life *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor
- ( ) Other

Bulgular ile varsayımlar arası ilgileşim / Findings *

- (•) Mükemmel (Very Good)
- ( ) İyi (Good)
- ( ) Yetersiz (Poor)

Serbest alan/Free area

Sonuç / Result *

- ( ) Kabul / Accept
- ( ) Değişiklik / Revision
- (•) Ret / Rejection
- ( ) Önerdiğim değişiklikleri yazar/yazarlar yaptıktan sonra son kararımı vereceğim

Sonuç için önemli neden ya da nedenler lütfen yazınız / The most important cause or causes for result please write *

Eğer red kararı verdiyseniz ve başka bir dergiye önermek isterseniz lütfen yönlendirilecek dergi adını yazınız / If you have decided to reject and if you want to suggest another jounal please write the name of the jounal.

Diğer eklemek istedikleriniz varsa (Hakem makale sonuna isminin eklenmesini istemiyorlarsa aşağıdaki alana bu durumu bildirmelidir):

Ankara Üniversitesi Beypazarı Meslek Yüksekokulu

ISSN: 1309-1859

http://dergipark.gov.tr/bsad
E-posta: editor.bsad@gmail.com

basaran@ankara.edu.tr

BSAD
Bankacılık ve Sigortacılık Araştırmaları Dergisi
Sayı 12, (Aralık 2018)*

İçindekiler/Contents

Makaleler/Articles

*Sayı 12, (Aralık 2018) sayısı görevli editörü: Ali Başaran, Dr. Öğr. Üyesi.

BSAD

Bankacılık ve Sigortacılık Araştırmaları Dergisi
Sayı 12, ss.8-22

Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar

Eda ALTUNTAŞ

Başkent Üniversitesi

Emine KARA

Başkent Üniversitesi

Abdullah Buğra SOYLU

Başkent Üniversitesi

Erdem KIRKBEŞOĞLU

Başkent Üniversitesi

Öz

Bu çalışmanın amacı Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Bu kapsamda, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir paralel olarak Türkiye'de de araştırma ekibimizce uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif olarak çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak ve Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacıların söylem analizi yapılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. Görüşmeler neticesinde elde edilen bulgular, Türkiye ve AB sigortacılarının risk algıları ve riski değerlendirme bakış açıları arasında çok büyük farklılıklar olmamasına rağmen Türkiye'deki siber risklerin yaratacağı olası sorunlara ilişkin işletmelerin farkındalığının AB'den farklılık gösterdiğini göstermektedir.

Anahtar Sözcükler

Siber risk, siber sigorta.
JEL Sınıflaması: Z00.

Cyber Insurance: Recent Developments, Applications, and Problems

Abstract

The aim of this study is to examine the effectiveness of the Turkish insurance system following the harmonization process of the European Union and managing this process successfully from 2007 on the issue of securing the cyber risks. This is based on the project titled "Cyber Insurance: Recent Developments, Implementations and Challenges" conducted by the European Union Network and Information Security Agency in 2016. This project used the same methodology and questionnaire was administered by our research team in Turkey. In this context, Turkey cyber risks are actively working company managers with a semi-structured interview technique using and Risk Management about the Forum 2015: Cyber Question Risks Management Analyzing the discourse of speakers

at the forum called to test the effectiveness of cyber risk struggles were directed. At the end of the study, a significant level of risk perception and assessment styles of Turkey and the EU insurers have not shown differences. However, it was observed that low levels of awareness about the negative consequences of cyber risks in Turkey.

Keywords

Cyber risk, cyber insurance.
JEL Classification: Z00.

GİRİŞ

Günümüzde teknoloji, hemen her kesim tarafından yaşantımızın vazgeçilmezi olarak kabul edilmektedir. Teknolojinin önemi sadece insanlar için değil kurum ve kuruluşların tüm faaliyetlerinin ayrılmaz bir parçası olarak görülmektedir. Fayda sağlayan birçok durumun olumlu yanlarının olabileceği gibi kötüye kullanım sonucu birçok zararı da beraberinde getireceği bilinmektedir. Bilgi ve teknoloji hayatımızın en büyük kurtarıcısı gibi görünse de kötü niyetli kişi ve kuruluşların kendi menfaatleri uğruna yaptıkları birçok işin sonucu beklenmeyen zararlar oluşabilir. Dolayısıyla teknolojik sistemlerin kullanımı, gerek kamu kurumları ve işletmeleri gerekse de bireyleri siber risklerle karşı karşıya bırakmaktadır.

Günümüzde dünya çapında yaklaşık 6 milyar akıllı cihaz bulut üzerinden birbirine bağlanmış durumdadır. 2020 yılında ise bu rakamın 20 milyar olması beklenmektedir. Bu kapsamda siber tehditlerin önemi özellikle son yıllarda gündeme gelmiştir.

Bilgi teknolojisi alanında güvenlik ihlalleri giderek artmaya devam etmekte, işletmeler ise artık siber güvenlik riskini, doğal afet riskinden çok daha ciddiye aldıkları bir dönemdedirler. Son zamanlarda sıkça duymaya başladığımız siber risk aslında insanların geleneksel güvenlik anlayışında büyük bir değişimi ortaya çıkarmıştır. Bu değişim insanların güvenle kullandıkları telefondan, kişisel bilgisayarlarına kadar birçok teknolojinin parçası olarak görülen elektronik aletlerin daha dikkatli kullanılması gerektiğine de dikkat çekmiştir. Ancak ne kadar dikkat edilse de birçok kurumun siber risk yüzünden piyasada çok sayıda büyük risklerle karşı karşıya kaldıkları göz ardı edilmemelidir.

Günümüzde güvence kavramının en güzel karşılığı sigortadır. Sigortanın temeli güven esasına dayalıdır. Her geçen gün daha fazla şirket, verilerini ve markalarını tehdit eden riskleri minimuma indirmek için sigorta güvencesi arama yoluna gitmektedirler. Gelişmiş ülkelerde siber güvenlik ihlallerine karşı, sigortası olanların oranı %31'i geçmemektedir (Ekonomist Dergisi, 10.10.2016). Bu oran gelişmiş ülkeler için bir başarı göstergesi olarak tanımlanmasa da son yıllardaki artış göz önüne alındığında küçümsenemeyecek bir pazar payını temsil ettiği de söylenebilir. Ancak gelişmekte olan piyasalar için benzer bir seyrin olmadığı görülmektedir. Sigortacılığın büyük sayılar kanunu çerçevesinde etkin bir şekilde yürütülebildiği göz önüne alındığında özellikle siber risk sigortaları gibi uygulama sayısının az olduğu ülkelerde sigorta şirketlerinin etkin bir güvence sağlamasını beklemek imkânsızdır. Zira sigorta edilebilir bir riskten bahsedebilmek için sigorta şirketinin geçmiş yıllarda o risk grubunda yeterli veriye sahip olması gerekmektedir. Gerek prim gerekse de beklenen hasar tazminatlarının gerçekçi bir şekilde tahmin edilmesinin temelinde bu yatmaktadır.

Bu noktada temel sorun Türkiye gibi gelişen sigorta piyasaları için siber risklere karşı güvence sağlamadaki tecrübe eksikliğidir. Dolayısıyla bu çalışmanın amacı Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Daha açık bir ifadeyle, Avrupa Birliğine uyum politikasıyla hareket eden devlet politikası, siber riskler gibi spesifik tehditlere karşı ne derece teminat sağlamada etkin çalıştığı sorgulanacaktır. Bu soruya cevap bulabilmek adına Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir Türkiye'de araştırma ekibimizce

uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif olarak çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak ve Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacıların söylem analizi yapılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. Görüşmeler neticesinde elde edilen bulgular, AB raporundakilerle karşılaştırılarak, Türk sigortacılık sisteminin etkinliği ve farklılığı çalışma sonunda ortaya konulmuştur.

1. SİBER RİSKLER VE SİGORTA GEREKSİNİMİ

Gerek bilginin hızlı bir şekilde yayılımı gerekse teknolojinin gelişimi risklerin çeşitliliğini artırmaktadır. Yıllara göre risklerin çeşitlendiğini gözlemlediğimizde farklı risk gruplarıyla karşılaşmak mümkündür. 2017 yılının ön planda olan risklerini sıralayacak olursak terör, siber saldırılar, doğal afetler, göç, bölgesel çatışmalar ve iklim değişikliği gibi risk unsurlarının yer aldığı görülmektedir. Bu risklerden bir tanesi olan siber saldırılar göz ardı edilemeyecek kadar çok tehlikenin başlangıcını oluşturmaktadır. Siber saldırı sonucu olası riskler bu tehditlerin en önemlileri olarak kabul edilmektedir. Devlet kamu kurum ve kuruluşlarının yanı sıra KOBİ'lerden çok uluslu şirketlere kadar tüm ticari kuruluşlar finansal kayıplarla sonuçlanabilecek siber risklerin tehdidi altında bulunmaktadır. Türkiye en çok siber saldırıya uğrayan ülkeler arasında 9'uncu ırada yer alırken, dünyada yılda 556 milyon siber saldırı gerçekleşmektedir (Milliyet gazetesi, 2016). Siber saldırıların her yıl %50 oranında arttığı ifade edilmektedir. Ayrıca siber suçların global ekonomiye maliyeti yıllık 445 milyar USD'dir (Habertürk, 2016). Türkiye'de yılda 10 milyondan fazla kişinin mağdur olduğu ve bunun toplam net maliyetinin 556 milyon USD olduğu tahmin edilmektedir (Sigorta gündem, 2016).

Siber saldırılar bugün o noktaya gelmiştir ki gerek kamu kuruluşlarının gerekse özel şirketlerin en büyük kâbusu olmuştur. Yapılan araştırmalara göre, ülkemizde 2017'nin ilk üç ayında gerçekleşen siber saldırı sayısı, geçen yılın ilk üç ayına göre %50 artmış durumdadır (Sigorta.com.tr, 01.09.2017). Ülkemizde günde ortalama 75 bin siber saldırı gerçekleşmektedir ve bu sayı artan oranda yükselmektedir. Siber atak sayısında Türkiye, dünyada 5'inci, Avrupa'da 4'üncü sıradadır (Hürriyet Gazetesi, 21.05.2017). Yapılan siber saldırıların çeşitlerine bakıldığında ise, veri sızdırma teşebbüsleri %40, Truva atı saldırıları ise %30 civarındadır. En fazla siber saldırıların nereye yapıldığına bakıldığında da üniversiteler ve Millî Eğitim Bakanlığı başı çekmektedir (Sigorta.com.tr, 01.09.2017). Bu ciddi rakamlar aslında siber risklerin önemini daha da dikkate değer hale getirmektedir.

Bu tür riskin gerçekleşmesi durumunda kişiler ve kuruluşlar farklı yöntemlerle zarar görebilmektedirler. Kişisel olarak yapılan saldırılarda kişisel bilgilerin ele geçirilmesi birçok sorunu beraberinde getirmektedir. Kurumlar açısından baktığımızda bir bankaya yapılan siber saldırıda birçok müşteri hesabının etkilenmesi muhtemeldir. Kurumlara yapılan siber saldırı sonucu yaşanılan maddi kaybın yanında kurum itibarının zedelenmesi ve güvensizlik durumunun oluşması gerçekleşen riskin etkilerini arttırmaktadır. Zira işletmelerin temel amacı yalnızca mal veya hizmet sunmak değil, aynı zamanda güven ortamı içinde müşteri portföyü oluşturmaktır. Bu güvenin sarsılması, uzun vadede işletmenin hayatta kalmasını etkileyecek bir durum yaratabilir.

Siber risk için birçok saldırı türü bulunmaktadır. Türkiye'de en çok karşılaşılan beş siber saldırı çeşidi şunlardır: Fidye yazılımları, Olta saldırıları, Kredi kartı dolandırıcılıkları, DOS/DDOS saldırıları, Mobil tehditler (Trend Micro, 2014).

Fidye yazılımları iki tür olarak karşımıza çıkar: şifreleyiciler ve kilitleyicilerdir. Şifreleyiciler bilgisayarlara ulaştıkları zaman bilgisayarda bulunan her türlü veriyi şifre ile korumaya alırlar. Bu koruma ile kişiler kendi bilgisayarlarındaki dosyaları açamaz ve dosya içinde bulunan verilere ulaşamazlar. Kilitleyiciler ise cihazı kilit altına alırlar. Bu kilit sadece verilere ulaşmayı değil tüm erişimi engeller. Böylelikle sisteme giriş erişilmez olur ve son olarak fidye talebinde bulunurlar.

Olta saldırıları ise zaman zaman bankalardan ve birçok finansal kuruluşlardan gelmiş gibi görünen sahte e-postalar olarak örneklendirilebilir. Bireyler gelen bu e-postaları acil ve çok önemli hissi yaratan başlıklar halinde görünmesinden dolayı dikkate almaktadır. Böylelikle SMS yoluyla gizli olması gereken bilgiler, kişilerin kart numaraları ve şifrelerinin ele geçirilmesi mümkün olabilmektedir.

Kredi kartı dolandırıcılıklarında ise siber suçluların kullanıcılara, özellikle herkesin ilgi gösterdiği ürünler için çeşitli kampanya, fırsat ve indirimler içeren sahte sipariş sayfalarını kapsayan e-postalar yolladıkları görülmektedir. Bu e-postalar özellikle sevgililer günü, anneler günü, babalar günü ve yıl başı gibi birçok kişinin birbirine özellikle online alışveriş yaparak hediye aldığı dönemlerde yoğunlaşmaktadır. Bu e-postalardaki bağlantılara tıklayıp sahte sipariş sayfalarından alışverişini yapan kişilerin kredi kartı bilgileri bilgisayar korsanları tarafından çalınabilmektedir (Trend Micro, 2016).

DOS/DDOS saldırıları adı verilen saldırı türü sistemin çalışmasını engellemek ve bu sistemin hizmet verememesi için yapılan saldırı türüdür. Bu saldırı türü 2016 yılının siber saldırı olaylarında en çok gündemde yerini almıştır.

Son olarak mobil tehditler adından anlaşılacağı üzere mobil cihazlara gelecek siber saldırı türüdür. Sayıları ve teknolojileri her gün gelişim gösteren mobil cihazların ürettikleri veri miktarı küçümsenemeyecek düzeydedir. En temel mobil tehditler; SMS gönderme, bilgi çalma ve reklam gösterimidir. Mobil cihazlar bilgisayar kullanımına göre daha korunmasız durumdadır. Bunun nedeni ise mobil cihazlarda anti virüs korumalarının bilgisayara oranla çok daha az olmasıdır.

Elbette her tehdit gibi siber riskler için de alınabilecek önlemler vardır. Özellikle kurumlar açısından baktığımız zaman siber güvenlik açısından üç temel yetkinlik bulunmaktadır. Birinci yetkinlik; bir kurumun güvenli bir siber altyapıya sahip olmasıdır. NART Sigorta ve Reasürans Brokerliği A.Ş. tarafından düzenlenen "2015 Risk Management Forum" konuşmacılarından Deloitte Türkiye Siber Güvenlik Hizmetleri Lideri Ali Yılmaz Kumcu'ya göre, siber güvenlik sistemleri günümüzde kurumların kaleleri gibidir. Orta Çağ döneminde insanoğlunun kendini korumak için kaleler inşa etmesi, hendek kazması gibi güvenlik amacıyla alınan önlemler, günümüzde yerini güvenli bir siber altyapıya bırakmaktadır. Bu kapsamda ilk olarak bilgi güvenliğinin bilgi işlemden ayrı olması gerekmektedir. Yine Kumcu'ya göre siber güvenlikte bir sonraki adım, özellikle son yıllarda daha çok gündeme gelen farkındalık olarak ön plana çıkmaktadır. Kurumların gelişen ve değişen siber tehditlere hazırlıklı olmaları için tehditlerin farkında olmaları gerekmektedir. Bu kapsamda kendi siber güvenlik sistemlerini güncelleyebilmeleri ve bu konuda dinamik davranış sergileyebilmeleri gerekmektedir. Ayrıca bilgi güvenliğinin sorumluluğu şirketlerde sadece bilgi güvenlik çalışanlarının değil her çalışanın sorumluluğu olacak şekilde farkındalık kazanılması gerekmektedir. Ancak bu iki yetkinlik her zaman yeterli olmamaktadır. Kurumların, siber saldırıya maruz kaldıklarında müdahale edebilecek hem operasyonel teknik hem de yönetimsel kabiliyete ihtiyaçları vardır. Kriz esnasında ve kriz sonrasında gerçekleşebilecek riskler açısından kurumların risk yönetimi anlamında destek almaları da onların yararına olacaktır (NART, 2015: 34-38).

Siber saldırı sonucunda meydana gelebilecek olaylar data kayıpları, veri silinmesi manipülasyonu, iş durması, üretimin durması, şantaj, çalınmış bilgilerin ifşasıyla ilgili tehditler ve itibar kaybı olarak sıralanabilir. İtibar kaybı burada rizikoların en büyüğü olarak değerlendirilmektedir. Ancak siber saldırıya uğramış şirketlerin, saldırının etkilerini azaltmak amacıyla karşılaştıkları masraflara bakıldığında; kriz yönetimi maliyeti toplam masrafların %48'ini, avukatlık masrafları %15'ini, kredi kartlarıyla ilgili maliyetler %11'ini, kanuni maliyetler %10'unu, uzlaşma masrafları %10'unu, ceza maliyetleri ise %6'sını oluşturmaktadır (NART, 2015: 43-46).

Kurumların ve şahısların siber tehditlerin sonuçlarından korunma yöntemlerinden biri sigortadır. Yukarıda bahsedildiği gibi pek çok kurum günümüzde siber saldırıya uğrayabilmekte

veya hali hazırda siber saldırıya uğramış durumdadır. Bu kapsamda siber sigorta, diğer adı ile veri güvenliği sigortasının önemi ön plana çıkmaktadır.

2. SİBER RİSK SİGORTASI

İnsanlar doğumlarından ölümlerine kadar çok sayıda ve değişik türlerde risk ile karşı karşıyadır. Bu riskler yalnız gerçek kişiler için değil tüzel kişiler ve organizasyonlar için de söz konusudur. Risklerin sonuçlarından korunmak için sigorta güvencesinden yararlanılır. Sigorta şirketlerinin gündeminde yer alan siber risk sigortası, kurumları ve sigortalıyı siber saldırılardan oluşan kayıplara karşı korumayı hedeflemiştir. Bu koruma yönteminin geliştirilmesi ve piyasanın daha iyi anlaşılması siber risk sigortasındaki bazı soru işaretlerinin ortadan kalkmasını sağlayacaktır. Bu ürünü sunan birçok sigorta şirketi, ürünün piyasada yaygınlaştırılmasında sorunlar yaşamaktadır. Bunun en önemli nedeni, poliçenin hangi amaca yönelik olduğuna dair yeterli farkındalığın ve bilgi birikiminin henüz sağlanamamış olmasıdır. Siber risk sigortası için Mesleki Sorumluluk Genel Şartları geçerlidir.

Şirketler bu verilerin ne derecede değerli olduğu ve nasıl korunması gerektiği hakkında; dahası bu verilerin kaybolması ya da çalınması gibi durumlarda oluşabilecek tazminat talepleri hakkında yeterli bilgi ve tecrübeye sahip olmadıkları gözlemlenmiştir. Şirketlerin bu konuda yetersiz bilgiye sahip olması ve sigorta yaptıracak kişiyi yönlendirememesi sebebiyle muhtemel sigorta müşterileri, ihtiyaçlarına yönelik bir sigorta ürününün varlığından haberdar değildir. Bu sorun aslında siber risk sigortanın gelişmemesindeki en büyük etkendir.

Siber risk sigortasının gelişim sıralamasına bakacak olursak siber risk sigortası ürünü ilk olarak 1990'lı yılların sonunda Amerika Birleşik Devletleri'nde ortaya çıkmış ve 2000'li yılların başında da Avrupa'da siber risk sigorta teminatları sağlanmaya başlanmıştır. Türkiye'de ise ilk kez 2010 yılında siber risk sigortalarının bir ihtiyaç olduğu kanaati ortaya çıkmıştır. Türkiye bu sigorta talebi karşısında ilk zamanlarda teminatı yurtdışı piyasalardan sağlarken, 2012 yılı sonrası bazı küresel firmaların Türkiye ofisleri bu teminatı sunmaya başlamıştır. Böylelikle Türkiye'deki sigorta şirketleri 2012 yılından itibaren, yurt içinde teminat sunmaya başlamıştır. Türkiye'de siber risk kavramı, yalnızca "veri kaybı" olayları ile sınırlı olduğunu düşünülürken, zamanla gerçekleşen zararlar neticesinde siber risklerin ve sigorta teminatlarının çok daha kapsamlı olması gerektiği anlaşılmıştır. Saldırıların artması ve farkındalığın yükselmesi ile birçok şirket bu konu doğrultusunda çalışmalarını hızlandırmıştır. Bu çalışmaların ilk adımı olarak şartname ve teminatlarda genişletmeler yapmışlardır.

2013 yılında Kıta Avrupası'nda teminat sağlayan 8 pazar varken, bu rakam 2017 yılında 25 pazara yükselmiştir. Küresel ölçekte 50 civarı pazarın siber sigorta teminatı sağladığını söylemek mümkündür. Son 4 yılda Kıta Avrupası'ndaki seyre bakılırsa, önümüzdeki yıllarda bu sayının artacağını söylenebilir (Kayganacı, 2017).

Siber risk sigortasını diğer sigortardan ayıran en önemli özellik verinin silinmesi kaybolması ya da çalınması değildir. Çünkü siber risk sigortasında zarar görecek veri sigortalanmaz. Siber risk sigortasında verinin maddi bir değeri yoktur. Sigortalanan verinin kaybolmasından kaynaklı 3'üncü şahısların talebi sigortalanır. Siber risk sigortasını diğer sigortalardan farklı kılan bir diğer özellik ise, gerçekleşen riskin etki olarak kestirilebilmesinin güçlüğüdür. Çünkü zarar oluştuğunda bu zararı ölçmek çok zordur. Bütün bu karmaşık ve zor belirlemelerden dolayı sigortacıların bu alandaki ürünlerini kolay bir şekilde yaygınlaştırmaları ve uygun fiyatlı poliçelerini müşterilerine sunmaları hiç de kolay değildir. Siber risk sigortasında belirlenmiş paket bir poliçe yoktur. Bu yüzden her sigortalının talep ve ihtiyaçlarına göre ek teminat içeren poliçeler düzenlenmektedir. Siber risk sorumluluk poliçeleri, elektronik veri ve internet kullanımıyla ilişkili birçok riski kapsamaktadır.

2.1. Birinci Şahıs Riskleri

Birinci şahıs riskleri, sigortalıyı doğrudan etkileyen faktörlerdir. Yani firmanın kendini koruduğu kayıplar için geçerlidir. Birinci taraf kapsamı poliçe sahibinin kendi verilerine, gelir kaybına, bir veri ihlali veya siber saldırı sonucu poliçe sahibinin işine zarar verilmesi riskini güvence altına alır. Bir örnek verecek olursak, bir işletmenin elektronik veri dosyalarına bir bilgisayar korsanının neden olduğu hasardır. Birinci tarafa ilişkin risk türleri şu şekilde sıralanabilir (ENISA, 2016).

- Hırsızlık ve dolandırıcılık; işletmeye ait bilgi ve verilerin çalınması sonucunda işletmenin uğrayacağı maddi ve itibari kayıplardır. Bu gibi durumların yaşanması şirketin marka ve piyasa değeri üzerinde olumsuz bir etki yaratmaktadır.
- Adli soruşturma; riskin gerçekleşmesi neticesinde saldırının etkisini analiz etmek ve saldırıyı durdurmak için gerekli yasal, teknik ve adli hizmetlere ilişkin maddi kayıplardır.
- İş kesintisi; bir poliçe sahibinin siber risk olayıyla veya veri kaybı sebebiyle iş yapamaması durumunda ortaya çıkan gelir kaybını ve ilgili maliyetlerini içerir.
- Bilgisayar veri kaybı ve restorasyonu; veri, donanım, yazılım veya bir siber saldırının neden olduğu tahrip sonucunda varlıkların fiziksel olarak zarar görmesini ve kullanılamamasını kapsar. Hasar gören diğer bilgileri kurtarma masrafları da dâhil olmak üzere, bilgisayarla ilgili varlıkların olumsuz sonuçlarını da içerir.

2.2. Üçüncü Şahıs Riskleri

Üçüncü şahıs riskleri kapsamı, poliçe sahibinin bir veri ihlalinden veya siber saldırıdan kaynaklı üçüncü şahıslara (müşteriler ve devlet kurumları da dâhil olmak üzere) karşı yükümlülüğünü güvence altına alır. Yani üçüncü şahıs teminatları, sigortalı firmaya karşı üçüncü şahısların bir takım zarar taleplerini ifade etmektedir. Örneğin, bir müşteri çalıştığı şirketin bilgisayar sisteminden, kişisel bilgilerinin çalınıp çevrimiçi yayınlandıktan sonra kişisel verilerini koruyamamaktan dolayı bu şirketi dava edebilir. Kapsam, genel olarak elektronik verilerin oluşturulması, gönderilmesi, alınması veya depolanmasında işlediği iddia edilen hatalar ya da ihmallerin bir sonucu olarak firmaya karşı talep edilen zararlardan oluşmaktadır. Poliçeler, genellikle firmayı tazminat taleplerine karşı savunmanın maliyetini karşılar. Bu maliyetler sigorta limitini azaltabilir. Üçüncü taraf risk kapsam türleri şu şekilde sıralanabilir (ENISA, 2016; Mcguirewoods, 2013).

- Dava tazminatları; siber bir saldırıdan kaynaklanan sivil dava, yargı veya ceza ile ilgili maliyetlerini kapsar.
- Bildirim maliyetleri; bir siber risk olayından etkilenen mağdurların, kanunların gerektirdiği bir bildirimle alakalı masraflarını karşılar.
- Kriz yönetimi; siber riske maruz kalmış bir sigortalının, piyasadaki itibarını korumak adına müşterilerine ne tür bir çağrıda bulunması ve bu süreçte ne tür bir kriz yönetimi politikası sergilemesi için katlandığı kriz yönetimi ve halkla ilişkiler masraflarını kapsar.
- Kredi izleme; bir siber risk olayından etkilenen şirketin müşteri veya çalışanlarına, bir daha bu tip bir dolandırıcılıkla karşılaşmaması için neler yapması gerektiğini eğitme konusundaki masraflardır.
- Medya sorumluluğu; telif hakkı, ticari marka veya hizmet markası ihlalinin sigortalı tarafından çevrimiçi yayınlanmasından kaynaklanan medya sorumluluğunu kapsar.

- Gizlilik yükümlülüğü; gizli tutulması gereken bilgilerin çalışan veya müşterilerin gizlilik ihlali nedeniyle sorumluluk kapsamını içerir.

2.3. Teminat Dışı Haller

- Rekabet; rekabet ve ticaretin engellenmesi, haksız rekabete ilişkin yasaların ihlali teminat dışı haller kapsamındadır.
- Bedensel yaralanma ve maddi varlıkların hasarı; fiziksel yaralanma, hastalık, ölüm ve/veya veriler dışındaki maddi varlıkların kaybı gibi durumlar teminat dışı hal olarak nitelendirilmiştir.
- Sözleşme sorumluluğu; sigortalının bir sözleşme sonucunda sorumlu olduğu herhangi bir garanti, teminat veya sorumluluk istisnadır.
- Siber terörizm; bilgisayarlar aracılığıyla işlenmiş, kamunun kullanmakta olduğu iletişim, ulaşım, enerji tedariki, güvenlik sistemlerinin şiddete, ölüme, imhaya yol açacak şekilde bozulması gibi durumlarda hükümet politikalarını değiştirmeye zorlayan karışıklık ve terör gibi durumlar istisnai hallere dahil edilmiştir.
- İşverenin yükümlülükleri; çalışan emeklilik planları, çalışan istihdam planları, çalışan kâr paylaşım, sosyal güvenlik hakları, işyerinde sağlığı ve güvenliği koruyan sorumluluklar vb. gibi işverenin sorumlu olduğu durumlar istisnai haller dahilindedir.
- İcra bildirimi; icra bildiriminde tanınan süreye riayet edilmemesi gibi durumlar istisnai durumlar dahilinde değerlendirilmiştir.
- Altyapı veya güvenlik arızası; mekanizma arızası, voltaj dalgalanmaları, elektrik kesintileri, uydu sistem arızaları, bilgisayar sistemi güvenliğinin sağlanamaması teminat dışıdır.
- Fikri mülkiyet; patentler ve ticari sırlar gibi fikri mülkiyet dahilinde bulunan hakların ihlalinden ileri gelen hususlar teminat dışı hallerdir.
- Kasıtlı eylem; sigortalı aleyhine talepte bulunulmasına yol açacak kasıtlı, planlı eylemler istisna edilmiştir.
- Suç teşkil eden eylemler; mahkeme kararına ya da sigortalı itirafına dayanılarak suç ve dolandırıcılık teşkil eden eylemlerden kaynaklanan durumlar istisna edilmiştir.
- Önceki talepler ve olaylar; poliçe başlangıç tarihinden önce yapılmış talepler veya poliçe başlangıç tarihinden itibaren bir talebe neden olabileceği bilinen durumlar istisna edilmiştir.
- Menkul kıymet talebi; menkul kıymetlerin mülkiyeti, alımı, satımı ile bağlantılı bir yasanın ihlalinden kaynaklı haller istisna edilmiştir.
- Terörizm/savaş; herhangi bir savaş, kargaşalık ve terörizmden kaynaklı haller istisna edilmiştir.
- Ticari zarar; elektronik fon transferi veya işlemin parasal değerinin hesaplanmasında, hesaplar arasındaki transfer sırasında vb. gibi durumlarda sigortalının uğrayacağı ticari kayıplar istisna edilmiştir.
- Veri güvenliği sorumluğu; yöneticilerin veya sorumlu kişilerin şirket verilerinin sızdırılmasında kötü niyetli ve kasıtlı hareketlerinin bulunması durumlarında ortaya çıkan zararlar teminat dışı hal kapsamındadır.

3. UYGULAMA VE YÖNTEM

Çalışmanın amacı, Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Bu soruya cevap bulabilmek adına Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir Türkiye'de araştırma ekibimizce uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. 2015 yılında İstanbul'da düzenlenen Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacılara söylem analizi yapılarak aynı sorulara cevaplar aranmıştır.

3.1. Türkiye Uygulaması

Çalışmanın Türkiye ayağında niteliksel araştırma yöntemlerinden iki farklı veri toplama tekniği seçilmiştir. İlk yöntem olan yarı yapılandırılmış görüşme tekniği ile önceden hazırlanmış sorulara sadık kalarak görüşmecilerle derinlemesine mülakatlar gerçekleştirilmiştir.

Çalışmanın amacına ulaşmak adına üç şirket seçilmiş ve çalışmanın analiz ve bulgular kısmında raporlanmış konu başlılarına uygun sorular sorulmuştur. Bu şirketlerin her birinin sermaye yapısı birbirlerine göre farklıdır. Sermaye yapılarına göre görüşmeler; sigorta şirketi, brokerlik ve acente olarak sınıflandırılmıştır. Öncelikle siber risk sigortasının Türkiye'deki yeri ve öneminin tespiti hedeflenmiştir. Bu nedenle yalnızca siber risk sigortası teminatı sunmuş veya buna aracılık etmiş kişiler seçilmiştir. Dolayısıyla görüşmenin gerçekleştirildiği kişiler Türkiye'de siber risk sigortası konusunda gelişkin bilgiye sahip sınırlı sayıdaki kişilerdir.

Görüşmeciler:

- Elementer Sigorta Şirketi: İsminin beyanını istemeyen bu sigorta şirketi, siber saldırı sonucu oluşabilecek kayıpları 2012 yılından itibaren Veri Koruma Sigortası ile Türkiye'de teminat altına almaya başlamıştır. Bu veri koruma sigortası işletmelerin siber risk sonucunda yaşanılan kaybı teminat altına alarak işletmelerin herhangi bir sarsıntı etkisinde kalmadan rutin işlerine kaldıkları yerden devam edebilmelerini sağlıyor. Bu anlamda şirket, siber risk sigortası alanında atılım yapan ilk şirketler arasında bulunuyor. Bu şirket alanına göre özel şartlar sunması ve siber risk konusunda uzman hasar süreci yönetimi ile bu konuda farkındalığını ortaya koymaktadır.
- Marsh Brokerlik: Türkiye'de siber risk sigortası konusunda atılım yapan ilk şirketler arasında yer alıyor. Aynı zamanda dünyanın lider sigorta brokerliği ve risk yönetim şirketidir. Marsh sigorta brokerliğinin, siber risk sigortası alanında pazar payının oldukça büyük olduğu bilinmektedir. Aynı zamanda Marsh, sigortalıların siber ataklar ile karşı karşıya kalması durumunda ne yapmaları gerektiği hakkında eğitim ve danışmanlık hizmeti de vermektedir.
- ERN Sigorta Aracılık Hizmetleri: İlgili sigorta acentesi uzun yıllardır Ankara'da faaliyet gösteriyor, ürün portföyü anlamında yangın, mühendislik ve sorumluluk sigortalarının çeşitli türleri konusunda tecrübeye sahiptir. Şirket aynı zamanda siber risklere yönelik birkaç sigorta poliçesinin hazırlanmasına aracılık etmiş ve risk danışmanlığı desteği sunmuştur.
- Çalışmanın veri toplama ayağının ikinci kısmında söylem analizi tekniği kullanılmıştır. 2015 yılında İstanbul'da gerçekleştirilen "Siber Risklerin Yönetimi" temalı Nart Risk Yönetimi forumuna katılan araştırma ekibi, dünyada ve Türkiye'de siber riskler konusunda yüksek bilgi ve tecrübeye sahip panelistlerin söylemlerini analiz etmiştir. Panelistler:

- Levent Nart: Nart Sigorta ve Reasürans Brokerliği A.Ş. yönetim kurulu başkanı ve genel müdürü olarak görevine devam etmektedir. Risk Management Forum 2015'te siber risklerle ilgili açılış konuşmasında verilerin güvenliğinden bahsetmiştir. Birinci oturumda ise dijital ve global bir risk olan "siber risk"in işletmeler tarafından nasıl algılandığından, yapılması gerekenlerden ve siber sigortalardan bahsetmiştir.
- Steven Young: Alman-Türk Ticaret ve Sanayi Odası başkan yardımcısı olarak görevine devam etmektedir. Forum'un açılış konuşmasında, siber risklerin gelecek yıllarda öneminin artacağından ve güvenlik önlemleri alınması gerektiğinden bahsetmiştir.
- Faruk Eczacıbaşı: Türkiye Bilişim Vakfı yürütme kurulu başkanı olarak Risk Management Forum 2015'te oturum başkanlığı yapmıştır. Konuşmasında, dünya ve Türkiye'deki siber tehditlerin etkilerini incelemiştir.
- Halil Öztürkci: Adeo Bilişim Danışmanlık A.Ş.'nde white hat hacker olarak çalışmaktadır. Forum'daki konuşmasında, devletleri, şirketleri ve bireyleri bekleyen siber saldırıları örneklerle açıklamıştır. Uygulamada bu risklerin yönetimiyle ilgili yapılan çalışmaları aktarmıştır.
- Murat Lostar: Lostar Bilgi Güvenliği A.Ş.'nde genel müdür olarak çalışmaya devam etmektedir. Forum'da yaptığı konuşmada, en kötü güvenlik krizlerinin aslında insan hatası ve bilinçsizlik olduğunu vurgulamıştır. Farkındalığı yükseltmek ve eğitim düzeyini arttırmak için yapılması gerekenlerden bahsetmiştir.
- İlhami Koç: Türkiye Sermaye Piyasaları Birliği başkanı olarak Forum'da yaptığı konuşmasında siber risklerin finans sektöründeki yerini, önemini ve siber güvenlik uygulamalarını aktarmıştır.
- Av. Gönenç Gürkaynak: ELİG Ortak Avukat Bürosunda yönetici olarak çalışmaya devam etmektedir. Forum'da siber suçlara karşı internet hukukunun nasıl şekillendiğinden bahsetmiştir. Siber suçla karşılaşıldığı esnada kişi ve kurumların yükümlülüklerini açıklamıştır.
- Burak Sadıç: PwC Türkiye'de bilgi güvenliği ve siber güvenlik hizmetleri lideri olarak çalışmaktadır. Yönetim kurulları, şirket yöneticileri ve üst düzey yöneticilerin bakış açısından siber riski anlatarak, oluşturulması gereken farkındalığın önemini bir kez daha vurgulamıştır. Bununla birlikte, kendi müşterilerine yapılan saldırıların yıllar bazından arttığını rakamlarla açıklamıştır.
- Daniel Shepherd: S21sec Cybersecurity şirketinde yönetici olarak çalışmaktadır. İspanyol bir şirket olan S21sec şirketi, siber güvenlik alanında uzmanlaşmış ve şirketlere bu konuda risk yönetimi hizmeti sunan bir firmadır. Daniel Sepherd, Forum'da yaptığı konuşmada, tecrübelerini aktararak şirketlerin siber saldırı sonucunda mali açıdan büyük zarar gördüklerini belirtmiştir. Siber sigortanın öneminin ve kurumlar için gerekliliğinin altını çizmiştir.
- Karolina Vogelpohl: Allianz Global Corporate&Specialty şirketinde Kuzey, Orta ve Doğu Avrupa finansal riskler bölge başkanı olarak görev yapmaktadır. Forum'daki konuşmasında hangi risklerin hangi yollarla teminat altına alınabileceğini aktarmıştır.

3.2. Avrupa Birliği Uygulaması

Çalışmada referans alınan kaynak, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından hazırlanan ve 2016 yılında tamamlanan "Siber Sigortalar: Güncel Gelişmeler, İyi Uygulamalar ve Sorunlar" isimli projedir. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), AB, üye ülkeleri, özel sektör ve Avrupa vatandaşları için bir ağ ve bilgi güvenliği uzmanlığı merkezidir. ENISA, bilgi güvenliği konusunda başarılı uygulamalar için tavsiyelerde bulunmak

için çok sayıda paydaş gruplarla birlikte çalışmaktadır. AB üyesi ülkelere, ilgili Avrupa Birliği mevzuatının uygulanmasında yardımcı olmakta ve Avrupa'nın kritik bilgi altyapısının ve ağlarının dayanıklılığını geliştirmeye çalışmaktadır. ENISA, AB çapında ağ ve bilgi güvenliğini geliştirmeyi taahhüt eden sınır ötesi toplulukların geliştirilmesine destek vererek AB üye ülkelerindeki mevcut uzmanlığı geliştirmeye çalışmaktadır.

ENISA'nın raporu iki kısımdan oluşmaktadır. İlk kısımda siber risklerin sigortacılar tarafından yönetilmesi sürecinde başarılı uygulamalar tespit edilmeye çalışılırken ikinci kısımda yine aynı süreçteki zorluklar tespit edilmeye çalışılmıştır. Bu amaçla ajans, siber sigortalar konusunda faaliyet gösteren sigorta şirketlerinin yetkin temsilcileriyle yarı yapılandırılmış görüşme tekniği kullanarak görüşmeler gerçekleştirmiştir.

Avrupa Birliği uygulamasındaki toplam görüşmeci sayısı 37'dir. 28 sigortacı Birleşik Krallık'tan, 2 sigortacı Almanya'dan, 2 sigortacı Yunanistan'dan ve birer sigortacı da Finlandiya, Fransa, İtalya, İspanya ve Hollanda'dan seçilmiştir.

4. ANALİZ VE BULGULAR

4.1. İyi Uygulamalar

Yöneticilerin yalnızca bugünü değil geleceğe ilişkin örgütleriyle ilgili plan ve politikalar üretmeyi, hedefler belirlemeyi ve bu hedeflere ulaşmada stratejiler geliştirmeyi zorunlu kılmaktadır. Zira belirlenen hedeflere ulaşmak için birçok riskle baş edilmesi gerekecektir. Bu nedenle yöneticiler, mevcut faaliyet alanlarındaki risk seviyesini çok iyi çözümlemek zorundadır. Önemli risklerin, belirlenerek önceliklendirilmesi ve en zayıf kritik kontrollerin tanımlanması kurumlar için önemlidir. Dolayısıyla hedeflere ulaşma yolunda risklerin yönetilmesi gerekliliği, son yıllarda yöneticilerin temel görevleri arasında gösterilmektedir (Kırkbeşoğlu ve McNeill, 2015: 210).

Sigorta sözleşmesinin hazırlanmasından önceki süreç sigorta şirketi için çok önemlidir. Bu süreçte sigorta şirketi, teklifi yapan müşterisinin riskini analiz edip değerlendirmesi gerekir. Bu aşamada ilk olarak müşterisinin teklif formu veya beyan formu adı verilen formu doldurmasını ister. Bu formun amacı, olası risklerin müşteri tarafından iyi niyetli bir şekilde beyan edilmesidir. Sigortacı, sigorta konusuna ilişkin çeşitli sorular sorduğu bu formdan bir risk primi hesaplayacaktır. Zira sigortacılıkta risk ne kadar yüksekse müşteriden istenecek prim o kadar ağırlaşacaktır. Sigortacı sadece teklif formuyla yetinmek zorunda değildir. İsterse sigorta konusunu yerinde ziyaret edebilir. Sigortacının hatalı bir risk seçimi yapmaması için bu süreç oldukça önemli olsa da yine de hatalı risk seçimi ortaya çıkabilir. Hatalı risk seçimi, sigortacının ortalama hasar olasılığından yüksek olasılıktaki bir riski, dikkatsiz bir risk değerlendirme (underwriting) sürecinden sonra ortalama bir fiyatla sigorta kapsamına alması anlamına gelir (Rejda, 2005). Siber risk sigortası hizmeti sunan sigorta şirketleri için bu süreç çok daha hassastır. Her bir müşteriye ait risklerin farklı olarak değerlendirilmesi nedeniyle bu süreçte riskler sürekli değişim göstermektedir. Son zamanlarda Avrupa'da, çeşitli sigorta şirketleri, ortak uygulamaları geliştirmek ve pazarda daha yüksek bir tutarlılık kurmak için çaba sarf etmektedirler.

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın siber risk araştırması (2016) sonuçlarına göre AB sigorta şirketleri müşterilerin riskini değerlendirirken genel olarak aşağıdaki ana kategorilere odaklanması gerektiği sonucuna ulaşmıştır. Aşağıda tanımlanan bu unsurlar gerek sigortacıların riski ölçmede gerekse siber sigorta satın almak isteyen işletmelerin riski yönetmede sahip olması gereken özellikleri göstermektedir.

Gözetim mekanizması; şirket bünyelerinde yer alan bilgi güvenliği sorumluları (Chief Information Security Officer), diğer çalışanların rutin iş tempolarında bilgi güvenliğine ayırmak zorunda oldukları zamanı telafi etmektedir. Bu kişilerin varlığı aynı zamanda şirket içinde bilgi güvenliği risklerinin düzenli ve sistematik takibini zorunlu kılacağından uzun vadede siber

risklerin ortaya çıkma ihtimalini azaltır. Bu nedenle Avrupa ülkelerindeki sigorta şirketleri, bir şirkette bilgi güvenliği sorumlularının varlığına daha fazla önem vermekte ve siber risk sigortası satın almak isteyen işletmelerde bu yönde çaba sarf etmektedir.

Bilgi güvenliği politikaları ve prosedürleri; sigortacılar önceleri şirketlerin bilgi güvenliği ile ilgili yazılı politika ve prosedürleri genel hatlarıyla dikkate alırken, günümüzde bu politikaların ne şekilde olduğu detaylarıyla sorgulanmaktadır. Dolayısıyla Avrupa ülkelerindeki sigorta şirketleri kapsamlı ve resmi bir bilgi güvenliği programının varlığını sorgulamak, buna ek olarak siber güvenlik konusundaki olgunluğunu dikkate alacak noktadadır. Benzer şekilde Türkiye'deki sigorta şirketleri tüm dizüstü, cep bilgisayarları, akıllı telefonlar ve ofis içi/dışı kullanılmakta olan masaüstü bilgisayarlardaki yetkisiz erişimi engelleyen sürücü şifrelemeleri için kontrol prosedürleri olup olmadığını sorgulamaktadır. Ayrıca şirket bünyesinde doküman koruma, saklama ve imha etme prosedürlerinin varlığı sorgulanmaktadır.

Çalışan farkındalığı; insan faktörü, bir örgüt içerisinde önemli bir risk oluşturabilirken, doğru eğitimle değerli bir savunma mekanizması ve risk yönetimi aracı haline gelebilmektedir. Örneğin, şifre çalma amaçlı e-postaları tanıyamayan eğitimsiz bir çalışan uygulanabilecek her güvenlik önleminin en zayıf halkasıdır. Buna ek olarak farkındalığı yüksek olan bir çalışan sadece politikaları ve prosedürleri uygulamakla kalmaz aynı zamanda bunları yorumlayarak uygulamaya çalışır. Avrupa ülkelerindeki sigorta şirketlerinin bir şirkette insan faktörünü güvence altına almanın önemli bir unsuru olan resmi bir güvenlik farkındalığı programının mevcudiyetini artık sorgulamaktalar. Özellikle sigortacılar; çalışanların, sık karşılaşılan siber risklere karşı eğitilmesine yönelik bir şirket prosedürünün varlığını sorguladıkları dikkati çekmektedir. Benzer şekilde Türkiye'de veri güvenliği ve gizliliği, yasal yükümlülükler, sorunlar, toplum mühendisliği (örneğin şifre çalma, phishing vb.) konularında farkındalık eğitimlerinin şirketler tarafından yürütülüp yürütülmediği sorgulanmaktadır.

Olay tepkisi; olay tepkisi, bir güvenlik ihlalinin veya siber saldırının sonrasını ele almak ve yönetmek için önceden geliştirilmiş risk yönetimi programıdır. Amaç, ortaya çıkan zararı sınırlayacak bir şekilde ele almak ve iyileşme süresini ve masraflarını azaltmaktır. Olay tepki planında, olayı neyin oluşturduğunu belirli koşullarla tanımlayan ve olay oluştuğunda izlenmesi gereken adımlar ve politikalar yer alır ve tüm departmanların buna uyması beklenir. Avrupa ülkelerindeki sigorta şirketleri, risk yönetimi sürecinde, işletmelerin bu tür bir programa sahip olup olmadıklarını sorgulamaktadır. Benzer şekilde Türkiye'de de sigortacıların risk analizi sürecinde işletmelerin iş devamlılık planı (BCP), yıkım onarım (DR) ve kriz yönetimi planlarının varlığı sorguladıkları tespit edilmiştir. Ayrıca herhangi bir bilgisayar saldırısı veya diğer veri kaybı/ihlali sonrasında operasyonların düzeltilmesi ve yeniden işler hale gelmesi için ne kadarlık süre harcandığı da sigortacıların risk analizi sürecinde dikkat ettikleri bir husustur. Yine bunun bir parçası olarak personelin iç bilgisayar ağına ve sistemlerine erişim yetersizliği/engellenmesi durumunun ne kadarlık bir sürede işletme için kriz yaratacağının sigortacılar tarafından sorgulandığı gözlemlenmiştir.

Güvenlik ölçümleri; şirketlerin düzenli olarak sahip oldukları bilişim risklerine yönelik güvenlik açıklarını izlemeleri önemlidir. Periyodik süreçler dahilinde ağ saldırılarının sıklıkları ve güvenlik açıklarının tespiti gibi testlerin yapılıp yapılmadığı ve mevcut şifreleme sisteminin içeriği Avrupa ülkelerindeki sigorta şirketleri için değerli konuma gelmiştir. Benzer şekilde Türk sigorta şirketleri de tüm bilgisayar aygıtlarında, sunucularında ve ağlarında yazılım sağlayıcının önerileri ve gereklilikleri doğrultusunda güncellemeleri yapılan anti-virüs yazılımı olup olmadığını, kullanılan güvenlik duvarı ve işgal/sızıntı görüntüleme tespit sisteminin olup olmadığını sorguladıkları gözlemlenmiştir. Buna ek olarak bilgisayar ağlarında hassas veriye erişimin sadece yetkili kişilerce erişimine sınırlı olup olmadığının da sorgulandığı tespit edilmiştir.

Tedarikçi (dış kaynak) kontrolü; çok sayıda firmanın üçüncü şahıslardan aldıkları tedarik hizmeti (mal veya hizmet şeklinde olabilir) neticesinde siber risklerle karşı karşıya kalma

ihtimalleri bulunmaktadır. Bu durum çoğu zaman şirketlerin kontrolünün dışında gelişse de Avrupa ülkelerindeki sigorta şirketleri için son yıllarda büyük önem arz etmektedir. Bu nedenle şirketlerin mal veya hizmet tedarik ettiği firmalarla kurduğu ilişkilerden kaynaklı siber tehlikelere karşı sigortacıların dikkat etmesi gerekliliği doğmaktadır. Türkiye uygulaması ise benzer şekilde sigortacıların, network, bilgisayar sistemi veya bilgi güvenliği fonksiyonlarının herhangi birinden dış kaynak kullanımı sağlayıp sağlamadıklarını sorguladıklarını göstermektedir. Bunun yanı sıra Türkiye'de sigortacıların, veri işleme veya depolama işlemlerini outsource ettikleri tüm iş ortaklarının IT sistemlerinin yeterliliklerini de sorguladıkları gözlemlenmiştir.

Üst yönetim farkındalığı; önemli bilgi güvenliği konularıyla ilgili yönetim kurulunun farkındalığı riski ele almak için atılan ilk adımdır. Bir kurul kararsız veya gecikmiş bir şekilde bu gibi konulardan haberdar olursa düzeltme eyleminin yetkisiz, kötü zamanlanmış veya orantısız olma riski bulunmaktadır. Daha açık bir ifadeyle siber tehlikelerle karşı karşıya olacak işletmelerde yönetim kurulunun periyodik olarak bilgilendirileceği bir yapıya sahip olması önemlidir. Yönetim kurulları rutin toplantılarında sıklıkla bu tür konuları tartışmaya almazlar. Ancak Avrupa ülkelerindeki sigorta şirketleri son yıllarda, yönetim kurullarının siber risklere karşı bilgilendirilme sıklığını ve toplantılarda siber risklere ilişkin alınan kararları sorgulamaktadır.

Sorunlar

Sigortacılar için en büyük zorluk, risk değerlendirmesini destekleyen siber güvenlik olayı verilerinin henüz büyük sayılar kanunu destekleyecek boyutta olmamasıdır. Sigortacıların henüz az sayıda gözleme ve veriye sahip olması geleceğe yönelik risk hesaplama sonuçlarındaki başarıyı etkilemektedir. Bu durum aynı zamanda Türkiye'deki sigorta şirketleri için benzer şeklindedir.

Avrupa ülkelerindeki sigorta şirketlerinin özellikle dikkat çektikleri bir diğer sorun, günümüz işletmeler dünyasında birleşme ve satın almaların sayısının artması neticesinde ortaya çıkan siber risklerdir. Şirketlerin satın alma veya birleşme yoluyla kimi zaman aynı çatı altında kimi zamanda yeni bir işletme olarak ortaya çıktığı bu durumlarda birleşen şirketlerin teknolojileri arasında da bir uyumsuzluğun veya güvenlik açıklarının yaşanması mümkün hale gelmektedir. Bir şirket siber riskle mücadelede kusursuz bir sisteme sahip olsa bile birleştiği veya satın aldığı diğer şirketin sahip olduğu bilişim alt yapısının güvensiz olması, ortaya çıkacak riskin boyutunu birleşme sonrası artıracaktır.

Siber risklere yönelik bir diğer sorun bulut bilişim ile ilgilidir. Bilindiği üzere tüm uygulama, program ve verilerinizin sanal bir sunucuda depolanması sistemine bulut bilişim denmektedir. Yani internetin olduğu her yerde elektronik cihazların aracılığı ile çeşitli bilgi ve verilere bulut bilişim veya teknolojisi sayesinde ulaşılabilmektedir. Bu noktadaki sorun müşteri konumundaki işletmelerin hangi veriyi ne kadar sıklıkta veya yoğunlukta bulut teknolojisiyle koruduklarının tam olarak kestirilemiyor olmasıdır. Bulut teknolojisiyle verilerin geri dönüşünü garanti altına almak kolaylaşsa da bu teknolojinin işletmeler tarafından düzenli olarak kullanılıp kullanılmadığı tam kestirilememektedir. Bu durum aynı zamanda Türkiye'deki sigorta şirketleri için benzer şekilde yorumlanmaktadır.

Gerek Avrupa'da gerekse de Türkiye'deki sigorta şirketlerinin daha az sıklıkta müşteri farkındalığının olmamasını, siber risklere ilişkin işletme içindeki plan ve politikaların tüm çalışanlarca aynı şekilde anlaşılamamış olmasını ve yeterli sayıda teknik beceri gerektiren personelin istihdam edilmiyor olmasını siber riskle mücadelede sorun olarak ortak değerlendirdikleri tespit edilmiştir.

Özetle çalışmada her iki bağlamda gerçekleştirilen paralel uygulamalar neticesinde birbirine benzer veya farklı seyreden iyi uygulamalar ve sorunlar yarı yapılandırılmış mülakat tekniğiyle karşılaştırma yapılabilir boyuta indirgenmiştir. Yukarıda anlatılanları bir tablo altında özetlemek bulguların anlaşılırlığına katkı sağlayacaktır. Buna göre siber risklerin sigortacılar tarafından yönetilmesi noktasında, iyi uygulamalar ve sorunları şu şekilde özetlenebilir;

Tablo 1. Siber risklere ilişkin risk analizi sürecinde karşılaşılan başarılı uygulamalar ve sorunlar

	Avrupa Birliği	Türkiye
Başarılı Uygulamalar		
Gözetim mekanizması	✓	X
Bilgi güvenliği politikaları ve prosedürleri	✓	✓
Çalışan farkındalığı	✓	✓
Olay tepkisi	✓	✓
Güvenlik ölçümleri	✓	✓
Tedarikçi (dış kaynak) kontrolü	✓	✓
Üst yönetim farkındalığı	✓	X
Sorunlar		
Yetersiz veri	✓	✓
Birleşme ve satın almalar	✓	X
Bulut bilişim kullanımı	✓	✓
Zayıf müşteri farkındalığı	✓	✓
İşletme içinde farkındalığı genele yayamama	✓	✓
Teknik beceriye sahip personel eksikliği	✓	✓

SONUÇ VE DEĞERLENDİRME

Her iki bağlamda gerçekleştirilen yarı yapılandırılmış mülakatlar neticesinde Türkiye ve AB sigorta şirketlerinin risk algıları ve riski değerlendirme bakış açıları arasında çok büyük farklılıklar olmadığı gözlemlenmiştir. Ancak Türkiye'deki siber risklerin yaratacağı olası sorunlara ilişkin işletmelerin farkındalığı AB'den farklılık göstermektedir. Ülkemizde siber uygulamaların gelişimi her ne kadar gelişmiş ülkelerle paralel seyretse de bu siber uygulamalar neticesinde ortaya çıkacak risklere ilişkin farkındalık ve risk algısı henüz düşük düzeyde seyrettiği gözlemlenmiştir. Ülkemizdeki bireysel risk algısının görece düşük olmasından siber risklerin de payını aldığı söylenebilir. Risk algısının düşük olması, sigortacıların bu tür risklere teminat sunmasında birtakım kısıtlar yaratacağı açıktır. Riskin yönetimi veya olası zararlardan korunmak ve tedbir almak öncelikle sigortalı bilincinin ve risk farkındalığının gelişkin olmasına bağlıdır. Bu nedenle toplumsal olarak risk farkındalığı yaratılamadığı sürece sigortacılar için siber sigortaların sürdürülebilir olması zorlaşacaktır. Zira ülkemizde siber sigorta ürününe sahip sigorta şirketi sayısı 2 iken, bu sayı 2017 yılı içerisinde bu şirketlerden birinin başka bir sigorta şirketi tarafından satın alınması neticesinde 1'e düşmüştür. Daha açık bir ifadeyle siber sigorta satışı ülkemizde yaygın bir uygulama olmaktan uzaktır. Gerçekleştirilen mülakat gösteriyor ki sigortacılar gerek işletmeler içerisinde yeterli teknik beceriye sahip personel eksikliğinden gerekse üst yönetim ve diğer çalışanların farkındalığının yetersiz olmasından bu sigorta ürününü satmaktan çekinmektedirler. Oysa Avrupa Birliği ülkelerinin büyük bir kısmında bu sigorta ürününün satışı artmaktadır. Dolayısıyla ülkemizdeki çabaların henüz karşılığını bulduğu söylenemez.

Türkiye uygulamasından elde edilen sonuçlar özellikle risk analizinin sigortacının soru formuyla başladığını ve işletme sahiplerine yöneltilen sorularla risklerin ortaya çıkarılmaya çalışıldığı bir durumu ortaya koymaktadır. Bu konuda yakalanacak açıkların sabit kıymetlerinde, sorumluluklarında özellikle kâr kaybında yaratacağı hasarların sigortacılar tarafından işletme sahiplerine raporlanarak risk farkındalığı yaratılmaktadır. Bunun en zayıf tarafı, farkındalık analizinin müşterinin izin verdiği ölçüde gerçekleşebiliyor olmasıdır. Ancak tersine AB sigortacılık sistemi özellikle siber riske maruz kalacak işletmelerin hali hazırda bir risk yönetimi sistemine, politika ve prosedürlerine sahip olunmasını zorunlu kılmaktadır. Daha açık bir ifadeyle sigorta satılacak bir işletmenin öncelikle risk yönetimi ve politikasına sahip olması zorunludur.

Sigorta şirketlerinin kendi siber güvenliklerini sağlamadaki çabaları ve farkındalıkları açısından Türkiye ile AB karşılaştırıldığında, AB sigortacılarının bu konuda ciddi yatırımlar yaptıkları görülmektedir. AB sigorta şirketlerinin pek çoğu, bilişim teknolojileri yatırımlarının %8-12'sini güvenlik yatırımlarına yönlendirmektedir (O'Connor, 2017). Richard Clarke'a göre güvenlik yatırımı için ayrılan bütçenin %8-12'den düşük olması sonucu oluşacak hataları gidermek şirketler için hem zor hem daha pahalı olacaktır. Yine Clarke'a göre, siber güvenliğin sağlanmasında en önemli unsur çalışanların beceri ve farkındalıkları olmaktadır. Sigorta şirketlerinin siber güvenlik yazılımları ve güvenlik duvarları ne kadar iyi olursa olsun, bilgi işlem çalışanlarının yetersiz bilgi, beceri ve farkındalığa sahip olması durumunda güvenlik tam anlamıyla sağlanamayacaktır (O'Connor, 2017). Sigorta şirketlerinin siber güvenlikleri, kişisel verilerin korunması bakımından büyük önem arz etmektedir. Dolayısıyla, şirketlerin gelebilecek olası siber saldırılara karşı bugünden önlem alması aynı derecede önemlidir. Ülkemizde sigorta şirketlerinin bu boyutlarda ciddi altyapı, güvenlik ve eğitim yatırımları olmasa da gelecekte bu yatırımların doğru yönlendirilmesine yönelik farkındalığın gelişmekte olduğu görülmektedir.

Her ne kadar risk analizi sürecinde başarılı uygulamalar farklılaşsa da sorunlar AB ile Türkiye arasında benzerdir. Ancak bu ortak sorunların ne düzeyde gerçekleştiği ileriki çalışmalarda nicel yöntemler yardımıyla daha da netleştirilebilir ve düzeyleri ve etkileri daha somut ortaya konabilir.

KAYNAKÇA

http://blog.trendmicro.com.tr/turkiyede-en-cok-karsilasilan-bes-siber-saldiri-cesidi/

http://riskandinsurance.com/analyzing-cyber-risk-coverage/

http://www.burakavci.com.tr/2016/01/dos-ddos-cyber-attack.html

http://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html

http://www.millire.com/dergi/SAYI_91.pdf

http://www.nart.com/siber-riskler-nart-guvencesinde/

http://www.paraanaliz.com/2017/ekonomi/sigorta-sektorunde-yeni-akim-siber-sigortalar-11654/

http://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik-yayinlari/siber-riskler-sigortalanirken-nelere-dikkat-edilmeli-pwc.pdf

http://www.sigortacigazetesi.com.tr/siber-riskler-dogru-analiz-edilmeli/

http://www.sigortagundem.com/haber/siber-saldirilara-karsi-sigorta-teminati-geldi/1125704

https://blog.kaspersky.com.tr/ransomware-for-dummies/2713/

https://www.abi.org.uk/products-and-issues/products/business-insurance/cyber-risk-insurance/

https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf

https://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx

https://www.slideshare.net/CezeriSGACezeriSiber/abd-siber-gvenlik-stratejisi

https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Ekim-%20Aral%C4%B1k%202016.pdf

https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/tr-web-kuresel-siber-guvenlik-yonetici-bilgilendirme-raporu.pdf

Amy O'Connor (2017), 5 Ways the Insurance Industry Can Improve Cybersecurity: Former U.S. Security Chief Clarke, Insurance Journal, https://www.insurancejournal.com/news/national/2017/11/15/471130.htm Erişim: 24.04.2018.

Kırkbeşoğlu E. ve McNeill, J. (2015). Risk Yönetimine Giriş. *Risk Yönetimi ve Sigortacılık* (der. Kırkbeşoğlu E.) Gazi Kitabevi. Ankara., 21-42.

NART Sigorta ve Reasürans Brokerliği (2015). Siber Risklerin Yönetimi, Risk Management Forum 2015, İstanbul.

Rejda, G.E. 2005. Principles of Risk Management and Insurance, 9th edition. Pearson.

Eda ALTUNTAŞ
Başkent Üniversitesi, Sigortacılık ve Risk Yönetimi Yüksek Lisans Öğrencisi
E-posta: edaaltuntas.00@hotmail.com
ORCID: http://orcid.org/0000-0003-2874-5728

Emine KARA
Başkent Üniversitesi, Sigortacılık ve Risk Yönetimi Yüksek Lisans Öğrencisi
E-posta: e.kara20@outlook.com
ORCID: http://orcid.org/0000-0003-1824-6538

Abdullah Buğra SOYLU
Başkent Üniversitesi, Ticari Bilimler Fakültesi, Sigortacılık ve Risk Yönetimi Bölümü
E-posta: absoylu@baskent.edu.tr
ORCID: http://orcid.org/0000-0001-8119-369X

Erdem KIRKBEŞOĞLU
Başkent Üniversitesi, Ticari Bilimler Fakültesi,
E-posta: erdemk@baskent.edu.tr
ORCID: https://orcid.org/0000-0002-6781-9753

Yazı Bilgisi:

Alındığı tarih: 11 Şubat 2018.
Yayına kabul edildiği tarih: 30 Nisan 2018.
E-yayın tarihi: 28 Aralık 2018.
Yazıcı çıktı sayfa sayısı: 15.
Kaynak sayısı: 21.

Hakemler:
Prof. Dr. Ali Köse (Marmara Üniversitesi – İstanbul)
Öğr. Gör. Mehmet İsel (Bandırma Onyedi Eylül Üniversitesi - Manyas/Balıkesir)

BSAD
Bankacılık ve Sigortacılık Araştırmaları Dergisi
Sayı 12, ss.23-32

Türkiye'de Defansif Tıp Uygulamalarının Sigortacılık Boyutu

Zeynep REVA

İstanbul Medeniyet Üniversitesi

Oğuz POLAT

Acıbadem Mehmet Ali Aydınlar Üniversitesi

Öz

Sigorta sektörünün en temel branşlarından olan "sağlık sigortası" ile sorumluluk sigortaları branşı altında yer alan "tıbbi kötü uygulamaya ilişkin zorunlu mali sorumluluk sigortası"nın kesişim noktalarından birisi de "tıbbi uygulama hataları"dır. Tıbbi uygulama hatası iddialarına ve bu konudaki davalara muhatap olmak istemeyen hekimler, bu sorumluluktan kaçınmak için gerekli olmayan teşhis ve tedaviye yönelerek veya riskli olduğunu düşündükleri hastalardan ve tedavilerden kaçınarak defansif tıp uygulaması gerçekleştirebilmektedirler. Defansif tıp uygulamalarının tıbbi ve etik boyutunun yanı sıra sigortacılık boyutunun da tartışılması önemli olup, defansif tıp uygulamaları sigorta şirketlerinin yapacağı tazminat ödemelerini ve prim hesaplamalarını etkilemektedir. Defansif tıp uygulamasına konu teşhis ve tedavi masraflarının özel sağlık sigortası kapsamında ödenip ödenmeyeceğini ve ayrıca defansif tıp uygulaması gerçekleştiren hekimin bu uygulama bakımından tıbbi kötü uygulama zorunlu mali sorumluluk sigortası güvencesine sahip olup olmayacağını tartışmak ve değerlendirmek gerekmektedir. Bu çalışmada literatür taraması yapılmış olup, sigortacılık ve sağlık mevzuatının konuyla ilgili düzenlemeleri mevcut uygulamalar çerçevesinde analiz edilerek değerlendirilmiştir. Sağlık sigortacılığında etkin tazminat yönetimi yapabilmek adına defansif tıp uygulamalarına dikkat edilmesi gerektiği düşünülmektedir.

Anahtar Sözcükler

Tıbbi uygulama hatası, defansif tıp, sağlık sigortası, hekim sorumluluk sigortası.

JEL Sınıflaması: G22, I13, K32, P46.

The Insurance Dimension of Defensive Medicine Practices

Abstract

One of the intersection points of "health insurance" which is one of the most basic branches of the insurance sector and "compulsory financial liability insurance for medical malpractice" which is under the branch of liability insurance is "medical malpractice". Physicians who do not want to be faced to the claims of medical malpractice can make defensive medicine by avoiding the responsibility by practicing a diagnostic test or medical treatment that is not necessarily the best option for the patient or by avoiding the patients and treatments that they think are risky. Since defensive medicine practices affect insurance claims and account of premiums, it is important to discuss the insurance dimension of defensive medicine as well as the medical and ethic dimension of it. It is required to discuss and evaluate whether the diagnostic and treatment costs of defensive medicine practices will be covered under private health insurance by the insurance company and whether the physician performing the defensive medical practice can have the assurance under the of compulsory medical malpractice liability insurance. For this study, the relevant literature in Turkish insurance legislation and Turkish health legislation has been considered and evaluated. It is considered that defensive medicine practices should be paid attention in order to manage insurance claims process more effectively.

Keywords
Medical malpractice, defensive medicine, medical malpractice liability insurance.

JEL Classification: G22, I13, K32, P46.

GİRİŞ

Sorumluluk sigortaları branşı altında yer alan "tıbbi kötü uygulamaya ilişkin zorunlu mali sorumluluk sigortası" ya da yaygın olarak bilinen adıyla "hekim sorumluluk sigortası" ile "sağlık sigortası"nın yollarının kesiştiği noktalarından birisi de "tıbbi uygulama hataları"dır. Tıbbi uygulama hatası iddiasına ve bu konudaki davalara muhatap olmak istemeyen hekimler, gerekli olmayan teşhis ve tedaviye yönelerek veya riskli olduğunu düşündükleri hastalardan ve tedavilerden kaçınarak defansif tıp uygulaması gerçekleştirebilmektedirler. Defansif tıp uygulamaları; sağlık hizmetlerinin kalitesinin düşmesine, yüksek maliyetlere ve hastanın yıpranmasına neden olabilmektedir. Bazı durumlarda bu uygulamalar hastanın sağlığını tehlikeye atmakta ve hatta hastanın hayati tehlike yaşamasına dahi neden olabilmektedir. Defansif tıp uygulamalarının tıbbi ve etik boyunun yanı sıra sigortacılık boyutunun da tartışılması önemlidir. Sağlık hizmetlerinin finansmanında önemli aktörlerden olan özel sigorta şirketleri bakımından da konunun irdelenmesi, defansif tıp uygulamasına konu teşhis ve tedavi masraflarının özel sağlık sigortası kapsamında ödenip ödenmeyeceğini ve ayrıca defansif tıp uygulaması gerçekleştiren hekimin "hekim sorumluluk sigortası" güvencesine sahip olup olamayacağını tartışmak da gerekmektedir.

1. DEFANSİF TIBBIN TANIMI VE TÜRLERİ

1.1. Defansif Tıbbın Tanımı

Dünya Tabipler Birliği'nin 1992 yılındaki 44'ncü Genel Kurulu'nda "Tıpta Yanlış Uygulama" konulu bir tebliğ yayınlanmış olup, bu tebliğde tıbbi uygulama hataları "*hekimin tedavi sırasında standart uygulamayı yapmaması, beceri eksikliği veya hastaya tedavi vermemesi ile oluşan zarar*" olarak tanımlamıştır. Dünya Tabipler Birliği bu açıklamayı bu konuya ilişkin davaların sayısının çok artması nedeniyle yapmak zorunda kalmıştır (Powers, Harris ve Lockard, 2000). Son yıllarda konuşulmaya başlayan bir konu olan defansif tıp ilk olarak 1970'li yıllarda ABD'de yapılan çalışmalarda hekimlerin tıbbi uygulamalardan kaynaklanabilecek sorumluluklardan kaçınmak amacıyla o an için birinci öncelikli olmayan tıbbi uygulamaları daha sık gerçekleştirdiklerinin veya riskli olduğunu düşündükleri hastalardan ve tedavilerden kaçındıklarının tespit edilmesi ile dikkat çekmeye başlamıştır. (Stoll, 1982; Studdert ve diğerleri, 2005). Defansif tıp, pozitif defansif tıp ve negatif defansif tıp olmak üzere iki türe ayrılmaktadır.

Tıbbi uygulama hatası sorumluluğundan kaçınmak amacıyla gereğinden fazla test ve tetkikler uygulanması pozitif defansif tıp ve yüksek riskli hasta ve uygulamalardan kaçınılması ise negatif defansif tıp olarak tanımlanmaktadır (US Congress Office of Technology Assessment, 1994). Defansif tıp hekimler tarafından hukuki ve cezai sorumluluktan kurtulmak ve kendilerini bir nevi koruma kalkanı altına almak amacıyla gerçekleştirilen ve çoğunluğu standart dışı sayılabilecek tıbbi uygulamalardır.

Defansif tıp uygulamaları; özellikle son yıllarda tıbbi uygulama hatası konulu dava sayısının artması, buna bağlı olarak hekimlerin bu davalarında ağır tazminatlar ödemesi ve cezaya maruz kalması üzerine artış göstermiştir (Polat, 2014).

Defansif tıp uygulamaları şu problemlere yol açabilmektedir. 1. Sağlık hizmetlerinin kalitesinin düşmesi, 2. Yüksek maliyetler, 3. Hastanın yıpranması. Bu uygulamalar hastanın sağlığını tehlikeye atmakta ve zor vaka diye tedaviden kaçınılıp başka hastaneye sevk edilmek istenen hastanın tedaviye zamanında ulaşamaması ve hatta sevk esnasında hayati tehlike yaşaması gibi olasılıklar dahi gündeme gelebilmektedir.

Her ne kadar hekimlerin niyeti kendilerinin olası ceza ve tazminat sorumluluğuna karşı koruma kalkanı geliştirmek olsa da defansif tıp başlı başına tıbbi uygulama hatası olabilecek bir konudur. Çünkü gelen hastaya standart prosedürler çerçevesinde bir tedavi protokolü uygulanmamış ve bilimsel gereklerin ve standart prosedürlerin dışına çıkılarak başlı başına tıbbi uygulama hatası yapılmıştır. Yani, tıbbi uygulama hatasının sorumluluğundan kaçınmak isteyen hekim aslında bir başka tıbbi uygulama hatası yapmaktadır.

Tıp etiğinin temel prensipleri olan "önce zarar verme" ve "yararlılık" ilkeleri ile defansif tıp çelişmektedir. Bu bakımdan etik açıdan yanlış olması ve hatta kimi zaman hastada yaşamsal tehlike yaratması defansif tıbbın en önemli yönleri olmakla birlikte konunun bir başka açıdan değerlendirilmesinde fayda bulunmaktadır. Sağlık hizmetlerinin finansmanında önemli aktörlerden olan özel sigorta şirketleri bakımından da konunun irdelenmesi önem taşımaktadır.

1.2. Defansif Tıp Türleri

1.2.1. Pozitif Defansif Tıp

Pozitif defansif tıp uygulamalarında hekim bunu yaparken standart tıbbi prosedürleri genişletmektedir. Bu uygulamalar, çoğu zaman herhangi bir tıbbi değeri olmayan uygulamalardır. Bu türden uygulamaları standart tıbbi prosedürlerden ayıran temel özellik hekimin hasta yararından çok kendi hukuki güvenliğini düşünmesi ve birçoğunun tıbbi herhangi bir faydasının olmamasıdır.

Pozitif defansif tıbbın uygulanma şekli; hastanın durumu, hastalığın durumu, hekimin uzmanlık alanı, hekim ve sağlık kurumunun hizmet algısı, tıbbi ve teknolojik imkânlar gibi pek çok unsura göre değişkenlik gösterebilmektedir.

Fazladan ilaç yazma, fazladan konsültasyon isteme, fazladan tıbbi tahlil isteme, fazladan görüntüleme tekniklerine başvurma, tıbbi endikasyonu olmayan girişimsel ve cerrahi yöntemlerin uygulanması, sıkı ve detaylı kayıt tutma, hasta takiplerini sıklaştırma en sık görülen davranışlardır (Edwards, 1985; Studdert ve diğerleri, 2005; Hershey, 2011; Summerton, 1995). Önemli olan hastanın ve hastalığın durumu gerektirmediği halde fazladan tıbbi prosedürlerin uygulanmasıdır. En sık başvurulan pozitif uygulama olan görüntüleme tekniklerinin gereksiz uygulanmasının, hastanın görüntüleme cihazlarının yaydığı zararlı radyoaktif ışınlara gereksiz bir şekilde maruz kalmasına sebep olduğu görülmektedir. Biyopsi gibi girişimsel uygulamalar ve sezaryen gibi cerrahi müdahalelerin de tıbben gerekli olmadığı halde uygulanmasının hastalar üzerinde ekonomik külfetler yarattığı da göz ardı edilmemelidir.

Pozitif defansif tıbbın yarattığı en önemli problem mali kaynakların kötü kullanılması ve hasta ile hekimin bu tür davranışlar yüzünden çok fazla zaman kaybı yaşamalarıdır. Hasta fazladan istenen tahlil ve görüntüleme tekniği uygulamalarına zaman harcamak zorunda bırakılmakta, yıpranmakta ve bu işlemleri yapan görevliler de gereksiz yere mesai harcamaktadırlar.

1.2.2. Negatif Defansif Tıp

Negatif defansif tıp uygulamalarında hekim dava edilme ve tıbbi uygulama hatası sebebiyle sorumlu tutulma endişesiyle riskli vakalarda teşhis ve tedaviden kaçınma davranışlarına yönelmektedirler. Hekim tıbbi görgü ve bilgisine göre yüksek risk içeren hastalardan ve yüksek risk içeren tedavi yöntemlerinden bazı davranış ve uygulamalarla kaçınarak sorumluluğu üzerinden atmak istemektedirler. Negatif defansif tıp uygulamaları pozitif uygulamalar kadar sık uygulanan davranışlar değildir. Ancak korkutucu olan bu uygulamanın her geçen gün yaygınlaşmasıdır.

Negatif defansif tıp uygulamaları hastaya zarar verme ihtimali olan ve yasal açıdan da pek çok riskleri barındıran uygulamalardır. Yaşamsal riske sahip hastalardan kaçınma, komplikasyon ihtimali yüksek tedavi yöntemlerinden kaçınma, agresif ve dava etme ihtimali

bulunan ya da yakınları aynı ihtimali taşıyan hastalardan kaçınma, doğum gibi tıbbi uygulamaları gerçekleştirmeyi bırakma, hastayı bir başka sağlık kurumuna sevk etme en sık görülen davranışlardır.

Negatif defansif tıp uygulamalarının en can alıcı noktası, elinde olanakları olmasına rağmen hekimin riskli hastaya bakmaması ve hastayı bir başka sağlık kurumuna sevk etmesidir. Dolayısıyla hekim bu davranışıyla tıp etiğine aykırı davranmaktadır. Elinde olanakları olmayan ve uzmanlık alanı da hastalıkla ilişkili olmayan bir hekimin, hasta için ilk etapta yapılması gerekenleri uygulayıp, hastayı daha donanımlı bir kuruma sevk etmesi tıbbi bir gereklilik olup bu davranış doğal olarak negatif defansif tıbbi uygulama değildir.

Hekimler aleyhine açılan davalardaki artış (Powers, Harris ve Lockard, 2000) hekimlere yönelik mesleki sorumluluk sigortası primlerini de doğal olarak etkilemektedir. Sigorta şirketleri tıbbi uygulama hataları davalarının yoğunlaşması nedeni ile oluşan yüksek maliyetlerden kurtulmak ve riski sigortalı olan hekimle paylaşma için ek tedbirler almaya başlamışlardır.

2. DEFANSİF TIBBIN SİGORTACILIK BOYUTUNUN DEĞERLENDİRİLMESİ

Defansif tıp uygulamalarının özel sigorta perspektifinden incelenirken iki temel boyutu değerlendirmek gerekmektedir: 1. Özel sağlık sigortaları, 2. Hekim sorumluluk sigortaları.

2.1. Defansif Tıbbın Özel Sağlık Sigortaları Yönünden Değerlendirilmesi

Sağlık sisteminde gerek genel sağlık sigortasının kapsamının genişliği, gerekse değişen demografik ve ekonomik göstergelere bağlı olarak artan maliyetler göz önüne alındığında, kaliteli bir kamu sağlık sistemine erişimin sürdürülebilirliği oldukça zorlaşmaktadır (Deloitte, 2012). Artan kronik hastalıklar ve nüfusun yaşlanması sonucunda mevcut kapsamı daraltmaksızın ve kaliteden ödün vermeksizin sağlık sistemini sürdürebilmek gelecekte daha da zorlaşacaktır. Sürdürülebilirliği sağlamak adına, teminat kapsamının özel sağlık sigortaları tarafından karşılanmasının gerekliliği ortaya çıkmaktadır (Deloitte, 2012). Özel sağlık sigortaları kaliteli sağlık hizmetlerinin sürdürülebilirliği noktasında önemli bir role sahiptir.

Özel sağlık sigortaları, sigortalıların sigorta süresi içinde hastalanmaları ve/veya herhangi bir kaza sonucu yaralanmaları halinde tıbbi tanı ve tedavileri masraflarının sigorta genel ve özel şartları çerçevesinde sigortalılara ödenmesini güvence altına alan sigortalardır.

Sigorta şirketleri aktüeryal hesaplama yaparak ve büyük sayılar kanunu çerçevesinde istatistiklerden yararlanarak fiyatlama yapmakta yani sigorta primi tutarını belirlemektedirler. Yapılan tazminat ödemeleri sigortalıların ödediği primlerden finanse edilmektedir. Ödenen tazminatlar bir sonraki yılın primini belirlemede en önemli etkenlerdendir. Yani doğru ve adil bir fiyatlama yapılmaması halinde bundan etkilenen sadece sigorta şirketi değil aynı zamanda fazladan prim ödeyen sigortalılar olacaktır. Çünkü ödenen tazminatlar sigortalıların bir sonraki yıl için ödeyeceği prim miktarını belirlemektedir. Sigortacılıkta Tazminat (Hasar)/Prim oranı (Loss Ratio) olarak isimlendirilen bu oran sigorta şirketlerinin, sigorta acentelerinin ve brokerler için, işletmelerinin kârlılığını ve performansını değerlendirmede önemli bir göstergedir (Bishop, 2009). Tazminat (Hasar)/Prim Oranı ne kadar düşükse, performans o kadar iyidir. Sigortalı açısından bakıldığında da Tazminat (Hasar)/Prim oranı ne kadar büyük olursa sigortalılar o kadar fazla prim ödeyecek demektir. İşte bu yüzden sigorta suiistimallerinin finanse edilmemesi, doğru ve adil bir fiyatlama yapılması önem taşımaktadır.

Pozitif defansif tıbbın yarattığı en önemli problemlerden birisi de mali kaynakların kötü kullanılmasıdır. Sağlık hizmetleri günümüzde oldukça pahalı uygulama ve teknolojiler üzerine kuruludur. Makro anlamda düşündüğümüz zaman toplumdaki hemen hemen her birey bir şekilde sağlık kurumlarına başvurmaktadır. Bu bağlamda defansif kaygılarla çekilecek bir röntgen filmi dahi büyük maliyetlere sebep olabilmektedir. Pozitif defansif tıp uygulamaları içinde en maliyetli

uygulamaların başında gelen ise defansif kaygılarla yapılan hastaneye yatışlar olarak göze çarpmaktadır.

Hekimlerin tıbbi endikasyon olmaksızın, standart uygulama prosedürlerinin dışına çıkarak fazladan talep ettiği tedavi ve tetkik harcamaları özel sağlık sigortaları bakımından sigorta suiistimali olarak tanımlanmaktadır (Reva, 2018). Fazladan yaptırılan bu test ve tetkiklerin ticari amaçla değil de hekimin kendisini koruma amacıyla istiyor olması sigortacılık bakımından farklılık oluşturmayacak ve tıbbi endikasyonu olmayan test ve tedavi masrafları özel sağlık sigortası teminatı kapsamı dışında kalacağından ödeme yapılmayacaktır.

Pozitif defansif uygulaması niteliğindeki test ve tetkik masrafları sigorta tazminatı ödemesine konu olmayacağı gibi defansif tıp uygulamaları aslında bir tür suiistimal niteliğinde olduğundan "yanlış sigorta uygulaması" yapan hekimin SİSBİS'e bildirilmesine neden olacaktır. Sigorta Suistimalleri Bilgi Paylaşım Sistemi'nin kısaltılmış hali olan SİSBİS, üçüncü şahıslardan ve sigorta şirketlerinden sağlanan "yanlış sigorta uygulamaları" ve sigorta suiistimaline konu olabilecek verilerin tutulduğu ve suiistimal bildirimlerinin elektronik ortamda yapıldığı merkezi bir veri tabanıdır. Sigortacılık uygulamalarının gereklerine aykırı davranan kişiler buraya kayıt edilmektedirler (Yanlış Sigorta Uygulamalarının Tespiti, Bildirimi, Kaydı ve Bu Uygulamalarla Mücadele Usul ve Esasları Hakkında Yönetmelik madde 11). SİSBİS sayesinde dürüst sigortalıların haklı menfaatlerinin korunması, prim maliyetlerinin düşürülmesi amaçlanmaktadır (https://www.sbm.org.tr/tr/Sayfalar/Yanlis-Sigorta-Uygulamalari.aspx). Pozitif defansif tıp uygulaması yapan hekimler, bu davranış aynı zamanda sigorta suiistimali niteliği taşıdığı için, SİSBİS'e kayıt edilecek ve bu çerçevede suiistimal yapmış hekim olarak kayıtlara geçmiş olacaktır.

Negatif defansif tıbbi uygulamalarda pozitif uygulamaların aksine tıbbi endikasyon olmaksızın fazladan uygulanan tetkik ve tedavi masrafları olmadığıü tam tersine tetkik ve tedaviden kaçınıldığı için özel sağlık sigortaları bakımından etkisi bulunmamaktadır. Negatif defansif tıp uygulamalarının sigortacılık bakımından etkisi olmasa da hukuki açıdan etkisinin olduğu ve derecesine göre cezai ve hukuki sorumluluk gerektirebileceği de unutulmamalıdır.

2.2. Defansif Tıbbın Hekim Sorumluluk Sigortaları Yönünden Değerlendirilmesi

2.2.1. Hekim Sorumluluk Sigortalarının Niteliği

Gerçek veya tüzel kişilerin üçüncü kişilere verebileceği zararları teminat altına alan sorumluluk sigortalarının bir türü de mesleki sorumluluk sigortalarıdır. Mesleki sorumluluk sigortası, sigortalının kusurlu davranışlarından kaynaklanan üçüncü kişilere verdiği zarar nedeniyle hem sigortalının hem de üçüncü kişilerin zararının giderilmesine yönelik olarak oluşturulan bir sigorta türüdür. Mesleki sorumluluk sigortası, "*Meslek erbaplarının mesleki uygulamalar sırasında oluşacak hatalar nedeniyle, tazminat ödemeleri gerektiğinde kullanılmak üzere sigorta şirketleri tarafından sigortalanmalarıdır.*" şeklinde de tanımlanabilmektedir (Sayek, 2000).

Tıbbi kötü uygulamaya ilişkin zorunlu mali sorumluluk sigortası, serbest ya da kamu veya özel sağlık kurum ve kuruluşlarında çalışan hekimler, diş hekimleri ve tıpta uzmanlık mevzuatına göre uzman olanların (sigortalının) poliçe kapsamındaki mesleki faaliyeti ifa ederken, sözleşme tarihinden önceki on yıllık dönemdeki veya sözleşme süresi içinde mesleki faaliyeti nedeniyle verdiği zararlara bağlı olarak sözleşme süresi içinde kendisine yapılan tazminat taleplerine ve bu taleple bağlantılı yargılama giderleri ile hükmolunacak faize ve sigortalı aleyhine ileri sürülen tazminat talebine ilişkin makul giderlere karşı poliçede belirlenen limitler dahilinde yaptırmakla yükümlü olduğu sigortalardır (Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Genel Şartları, madde A.1.).

2.2.2. Hekim Sorumluluk Sigortası Prim ve Hasar Paylaşım Esasları

Risk gruplarına göre hazırlanmış olan "Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı (https://www.tsb.org.tr/default.aspx?pageID=654&yid=120) ile "Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası"nın uygulanmasına ilişkin esaslar belirlenmiştir. Hekim sorumluluk sigortası kapsamında her bir olay için ödenecek azami teminat tutarları aşağıdaki tabloda yer almaktadır.

Tablo 1: Her bir olay için azami teminat tutarları

Risk Grubu	Azami Teminat Tutarı (TL)
I. Grup	200.000
II. Grup	400.000
III. Grup	600.000
IV. Grup	800.000

Kaynak: Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı (https://www.tsb.org.tr/default.aspx?pageID=654&yid=120).

Teminat tutarı maddi, manevi tazminat ve yargılama giderleri için geçerlidir. Risk gerçekleşmiş olsa dahi, olay başı azami teminat miktarı sözleşme süresi boyunca aynı kalmakla birlikte her durumda sözleşme kapsamında ödenecek tazminat miktarı 1.800.000₺'yi aşamamaktadır.

Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı, aynı zamanda risk gruplarına göre azami primi tutarlarını da belirlemiş bulunmaktadır. Her bir tıbbi branş için risk grubu ataması yapılmış olup, her branş girdiği risk grubu için belirlenen primi ödeyerek sigorta yaptırmakla yükümlüdür. İlk kez yapılacak sigortalarda aşağıdaki tabloda belirtilen prim tutarları uygulanmaktadır:

Tablo 2: Prim tutarları tablosu

Risk Grubu	Prim Miktarı (TL)
I. Grup	150
II. Grup	300
III. Grup	500
IV. Grup	750

Kaynak: Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı (https://www.tsb.org.tr/default.aspx?pageID=654&yid=120).

Risk grupları tablosu, Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı ekleri arasında yer almaktadır. Buna göre; Acil Tıp (İlk ve acil yardım), Ağız, Yüz ve Çene Cerrahisi, Anesteziyoloji ve Reanimasyon, Beyin ve Sinir Cerrahisi, Cerrahi Onkoloji, Çocuk Acil, Çocuk Kalp ve Damar Cerrahisi, Çocuk Yoğun Bakımı, El Cerrahisi, Gastroenteroloji Cerrahisi, Genel Cerrahi (Genel şirürji), Göğüs Cerrahisi (Göğüs kalp ve damar şirürjisi), Jinekolojik Onkoloji Cerrahisi, Kadın Hastalıkları ve Doğum, Kalp ve Damar Cerrahisi, Neonatoloji, Ortopedi ve Travmatoloji, Periferik Damar Cerrahisi, Perinatoloji, Plastik, Rekonstrüktif ve Estetik Cerrahi ve Yoğun Bakım dalları en yüksek riskli (IV. Grup) olarak belirlenirken; Adli Tıp, Anatomi, Askeri Sağlık Hizmetleri, Çevre Sağlığı, Epidemiyoloji, Fizyoloji, Halk Sağlığı, Histoloji ve Embriyoloji, Temel İmmünoloji (İmmünoloji), Tıbbi Biyokimya (Biyokimya ve klinik biyokimya), Tıbbi Ekoloji ve Hidroklimatoloji, Tıbbi Farmakoloji, Tıbbi Mikoloji (Mikoloji), Tıbbi Mikrobiyoloji, Tıbbi Patoloji (Patoloji) ve Tıbbi Viroloji (Viroloji) dalları en düşük riskli en düşük riskli (I. Grup) olarak belirlenmiştir.

Uygulamada sigorta şirketlerinin III. ve IV. (yüksek) risk gruplarındaki hekimlerin sigortalanmadığı iddiasının üzerine Hazine Müsteşarlığı, hekim sorumluluk sigortasında poliçe düzenlenmesine yönelik sıkıntıların aşılması amacıyla "havuz sistemi" getirmiştir. Buna göre sigorta priminin ve hasarın paylaşımına yönelik bazı esaslar belirlenmiştir. Prim ve ödenen hasarın %50'si şirketler arasına eşit olarak, kalan %50'si ise şirketlerin Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası primlerinden son 3 yıllık dönemde aldıkları paya göre paylaştırılmaktadır. (2017/4 sayılı Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Hakkında Sektör Duyurusu).

2.2.3. Hekim Sorumluluk Sigortası Kapsamında Bulunmayan Haller

Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Genel Şartları'nın A.3. maddesine göre aşağıdaki haller sigorta teminatı kapsamı dışındadır;

a. Sigortalının, poliçe kapsamında yer alan ve sınırları hukuk kuralları veya etik kurallar ile tespit edilen mesleki faaliyeti dışındaki faaliyetlerinden kaynaklanan tazminat talepleri,

b. İnsani görevin yerine getirilmesi hariç, sigortalının, poliçe kapsamındaki kuruluşların sorumluluk alanı dışındaki faaliyetlerinden kaynaklanan tazminat talepleri,

c. İdari ve adli para cezaları dâhil her tür ceza ve cezai şartlar,

d. İlgili mevzuatla belirlenen çerçevede tıbbi mesleki faaliyet gereği yapılanlar hariç her türlü deneyden kaynaklanan tazminat talepleri.

"*Sigortalının, poliçe kapsamında yer alan ve sınırları hukuk kuralları veya etik kurallar ile tespit edilen mesleki faaliyeti dışındaki faaliyetlerinden kaynaklanan tazminat talepleri*" maddesi uyarınca defansif tıp uygulamaları sigorta teminatı kapsamında bulunmamaktadır. Çünkü, defansif tıp uygulamaları hekimin hukuk kuralları veya etik kurallar ile tespit edilen mesleki faaliyetleri dışında sayılmaktadır. Yani, defansif tıp uygulaması yapan bir hekim, zorunlu sigortasını yaptırmış olsa ve teminat limitleri uygun dahi olsa sigorta genel şartlarının hükmü gereğince sigorta teminat dışında kalacak ve bu uygulamanın hastada neden olduğu zarar sigorta şirketi tarafından tazmin edilmeyecektir.

Pozitif veya negatif her türlü defansif tıp uygulaması tıbbi uygulama hatası anılan madde hükmü kapsamında sigorta teminatı kapsamında kalacaktır. Yani, tıbbi endikasyonu olmayan fazladan yaptırılan gereksiz bir tetkik esnasında hasta bir şekilde zarar gördüğü takdirde hekimin tıbbi kötü uygulamaya ilişkini zorunlu mali sorumluluk sigortası devreye girmeyecek ve hekimi hastanın zararın bizzat kendisi karşılamak durumunda kalacaktır ya da riskli gördüğü hastayı aslında her türlü imkâna sahip olmasına rağmen sırf kendisini korumak maksadıyla başka bir kuruma sevk eden hekim, sevk esnasında fenalaşarak durumu ağırlaşan hasta için bizzat kendisi tazminat ödemek zorunda kalacak ve hekim sorumluluk sigortası yine devreye girmeyecektir.

SONUÇ VE ÖNERİLER

Defansif tıp uygulamalarının özellikle son 20 yılda hem dünyada hem ülkemizde artış gösterdiği görülmektedir (Aynacı, 2008; Yılmaz, 2012). Buradaki temel amaç, tıbbi endikasyon olmaksızın standart uygulama prosedürlerinin dışına çıkıp fazladan tetkik ve tedavi uygulamak (pozitif defansif tıp) veya riskli hasta veya tedavilerden kaçınmak (negatif defansif tıp) suretiyle hekimlerin kendilerini olası bir tıbbi uygulama hatası suçlamasından korumak istemeleridir.

Defansif tıp uygulamaları hastada yıpranmaya ve finansal zarara yol açarken aynı zamanda sağlık sistemine bir yük bindirmekte ve hem ekipman hem de personelde yıpranmaya neden olabilmektedir. Bu açıdan konu özel sigorta perspektifinden incelenirken özel sağlık sigortaları ve hekim sorumluluk sigortaları olmak üzere iki boyutuyla değerlendirilmelidir.

Özel sağlık sigortalarında temel kriter tıbbi endikasyonu olan girişimlerin kabul edilmesi olduğundan hekimlerin tıbbi endikasyon olmaksızın, standart uygulama prosedürlerinin dışına çıkarak fazladan talep ettiği tedavi ve tetkik harcamaları, özel sağlık sigortaları bakımından sigorta suiistimali olarak değerlendirilmektedir. Bu işlemler de sigorta teminatı kapsamı dışında kabul edilmekte yani fazladan uygulanan bu tetkik ve tedavilerin masrafları sigorta şirketi tarafından ödenmemektedir. Bu durum aynı zamanda yanlış sigorta uygulaması niteliğinde olduğu için hekimler yanlış sigorta uygulaması yapanların işlendiği merkezi veri tabanı olan SİSBİS'e kayıt edilebilmektedir.

Defansif tıp uygulamaları, hekim sorumluluk sigortaları açısından değerlendirildiğinde sigorta teminatı kapsamı dışında kalmaktadır. Çünkü pozitif defansif tıp uygulamalarında, tıbbi endikasyonu olmayan fazladan yaptırılan gereksiz bir tetkik esnasında hasta bir şekilde zarar gördüğü takdirde hekim sorumluluk sigortası devreye girmeyecek ve hekim hastanın zararını bizzat tazmin etmek durumunda kalacaktır. Negatif defansif tıp uygulamalarında ise riskli gördüğü hastayı aslında her türlü imkana sahip olmasına rağmen sırf kendisini korumak maksadıyla başka bir kuruma sevk eden hekim için hekim sorumluluk sigortası yine devreye girmeyecek ve sevk esnasında fenalaşarak durumu ağırlaşan hasta için bizzat hekimin kendisi tazminat ödemek zorunda kalacaktır.

Tıp etiğinin temel ilkeleri ile de bağdaşmayan ve iyi hekimlik tanımı dışında kalan defansif tıp uygulamaları sigortacılık bakımından da hekimin menfaatini zedeleyerek hastanın zararının hekim tarafından kişisel olarak tazmin edilmesini gerekli kılmaktadır. Hastanın sağlığını tehlikeye atan, tıp etiği ile bağdaşmayan, hastaya gereksiz maliyet yaratan ve sigortacılık bakımından değerlendirildiğinde de hekim nezdinde de maliyet kalemi yaratan defansif tıp uygulamalarının hem hasta hem de hekim için yararlı olmadığı ve bu davranışların saptanması halinde problemlerin oluşacağı görülmektedir.

Sağlık sigortacılığında etkin ver adil tazminat yönetimi yapabilmek adına defansif tıp uygulamalarına dikkat edilmesi ve bu kapsamda analizler yapılması önerilmektedir.

KAYNAKÇA

2017/4 sayılı Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Hakkında Sektör Duyurusu. https://www.tsb.org.tr/images/Documents/2017-4%20Sekt%C3%B6r%20Duyurusu.pdf (Erişim tarihi: 06.05.2018).

2. US Congress Office of Technology Assessment. (1994). Defensive medicine and medical malpractice. *Publication OTA-H-602. Washington, DC: US Government Printing Office*

21.07.2010 tarihli ve 27648 sayılı Resmi Gazete.

Aynacı Y. (2008). *Hekimlerde Defansif (Çekinik) Tıp Uygulamalarının Araştırılması,* Selçuk Üniversitesi Meram Tıp Fakültesi Adli Tıp ABD., Tıpta Uzmanlık Tezi, Konya.

Bishop A. (2009). How-Tos, How to calculate Claims Loss Ratio example, *Actuarial Science, Best Posts, Insurance Glossary, Loss Ratio*, June 2009. http://riskheads.org/calculate-claim-loss-ratio-example/#what Erişim tarihi: 04.06.2018)

Deloitte, Yased. (2012) *Türkiye Sağlık Sektörü Raporu*, 84, 90.

Edwards KS. (1985). Defensive Medicine: Health Care With A Pricetag. Ohio State Med J 81:38-42.

Hershey N. (2011). The Defensive Practice Of Medicine: Myth Or Reality., Catino M. Why Do Doctors Practice Defensive Medicine? The Side-Effects Of Medical Litigation. *Safety Science Monitor,* 15,1: 1-12.

https://www.sbm.org.tr/tr/Sayfalar/Yanlis-Sigorta-Uygulamalari.aspx (Erişim tarihi: 04.06.2018)

https://www.tsb.org.tr/mesleki-sorumluluk-sigortasi.aspx?pageID=761 (Erişim tarihi: 04.06.2018).

Polat O. (2014). *Tıbbi Uygulama Hataları*, Seçkin Yayınevi, 2. Baskı, 245-267.

Powers M., Harris N. & Lockard Mirams A. (2000). Clinical Negligence. *3rd ed, London: Butterworths law* London.

Reva Z. (2018) *Adli Sigortacılık*. Acıbadem Mehmet Ali Aydınlar Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Bitirme Projesi, İstanbul.

Sayek F. (2007). Soru ve Yanıtlarla Mesleki Sorumluluk Sigortası Yasa Taslağı. *Medikal Bakış Dergisi*, 10.03.2000. http://www.medikalbakis.net/2/sayfa8.htm, (Aktaran: Turgaz G. Sağlık Sektöründe Mesleki Sorumluluk Sigortası Uygulaması, Yüksek Lisans Tezi, 2007, İstanbul, s. 16.)

Stoll P. (1982), Defensive Medicine. *Beitr Gerichtl Med*., 40:35-40.

Studdert D.M., Mello M.M., Sage W.M., Desroches C.M., Peugh J., Zapert K. & Brennan T.A. (2005). Defensive Medicine Among High-Risk Specialist Physicians İn A Volatile Malpractice Environment. *JAMA* 293(21):2609-2617.

Summerton N. (1995). Positive And Negative Factors In Defensive Medicine: A Questionnaire Study Of General Practitioners, *BMJ*. Jan 7;310 (6971):27-9.

Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Genel Şartları, madde A.1. 21.07.2010 t. ve 27648 s. RG https://www.tsb.org.tr/tibbi-kotu-uygulamaya-iliskin-zorunlu-mali-sorumluluk-sigortasi.aspx ? pageID=521 (Son Erişim tarihi: 04.06.2018).

Tıbbi Kötü Uygulamaya İlişkin Zorunlu Mali Sorumluluk Sigortası Tarife ve Talimatı. https://www.tsb.org.tr/default.aspx?pageID=654&yid=120 (Erişim tarihi: 04.06.2018).

https://www.tsb.org.tr/default.aspx?pageID=654&yid=120 (Erişim tarihi: 05.06.2018).

Yanlış Sigorta Uygulamalarının Tespiti, Bildirimi, Kaydı Ve Bu Uygulamalarla Mücadele Usul ve Esasları Hakkında Yönetmelik madde 11. Yönetmelik metni için bakınız: 300.4.2011 tarih ve 27920 sayılı Resmi Gazete.

Yılmaz K. (2012). *Defansif Tıbbi Uygulamaların Hukuki Açıdan Yorumlanması*, İstanbul Üniversitesi Adli Tıp Enstitüsü Sosyal Bilimler ABD., Yüksek Lisans Tezi, İstanbul.

Zeynep REVA
Avukat, LL.M. – İstanbul Medeniyet Üniversitesi Tıp Hukuku doktora programı Öğrencisi

E-posta: z_reva@yahoo.com
ORCID: https://orcid.org/0000-0003-0719-2175

Oğuz POLAT
Prof. Dr. Acıbadem Mehmet Ali Aydınlar Üniversitesi Tıp Fakültesi Adli Tıp Anabilim Dalı
E-posta: ouzpol@yahoo.com
ORCID: http:// orcid.org/0000-0001-8454-6817

Yazı Bilgisi:

Alındığı tarih: 24 Temmuz 2018.
Yayına kabul edildiği tarih: 05 Aralık 2018.
E-yayın tarihi: 28 Aralık 2018.
Yazıcı çıktı sayfa sayısı: 10.
Kaynak sayısı: 22.

Hakemler:
Dr. Öğr. Üyesi Habil Gökmen (Dokuz Eylül Üniversitesi – İzmir)
Dr. Öğr. Üyesi Özgür Akpınar (Marmara Üniversitesi – İstanbul)

BSAD
Bankacılık ve Sigortacılık Araştırmaları Dergisi
Sayı 12, ss.33- 42

Spekülatif İşlemlerin Toplumsal Etkileri: İran Döviz Piyasası Örneği

Hüseyin KARAMELİKLİ

Karabük Üniversitesi

Öz

Bu çalışmanın temel amacı spekülasyon yapanların ödüllendirilmesi veya cezalandırılmasının uygunluğunu tartışmaktır. Bu makalede spekülasyon analiz edilmektedir. Bir ekonomide spekülatörlerin varlığı ekonomiye zararlı mıdır yoksa onların aktiviteleri ekonomik düzene, piyasa dengesine katkı sağlar mı sorusuna yanıt aranmaktadır. Bu soruyu cevaplandırmak için önce stokçuluğun iktisadi etkisi modellenmiştir. İkinci aşamada spekülatörlerin İran döviz piyasasındaki etkisi tespit edilmiştir. İran döviz piyasasında polisiye önlemlerin uygulandığı ve kur artışının yargı ve polisiye yöntemlerinin riski artırdığı görülmüştür. Ancak spekülatörlerin piyasada olumlu etkisi göze çarpmıştır.

Anahtar Sözcükler

Spekülasyon, piyasa dengesi, İran, döviz

JEL Sınıflaması: F31, O24

Social Effects of Speculative Operations: The Case of Iranian Foreign Exchange Market

Abstract

The main purpose of this study is to discuss the appropriateness of rewarding or punishment of speculators. In this paper speculation is analyzed. Is the presence of speculators in an economy harmful to the economy or their activities contribute to the economic order and market equilibrium? In order to answer this question, the economic impact of stocking was modeled. In the second stage, the influence of speculators on the Iranian foreign exchange market was determined. It has been observed that police measures have been implemented in the Iranian foreign exchange market and that the exchange rate increase and judicial methods increase the risks. However, the positive effect of speculators has been observed in the market.

Keywords

Speculation, Market equilibrium, Iran, Exchange rate

JEL Classification: F31, O24

GİRİŞ

İran ekonomisi kendine özgü kurum ve işleyişe sahiptir. Devlet ekonomik alanda müdahalesi diğer ülkelere göre fazladır. Ürünlerin fiyatlandırılması, dağıtımı ve üretimi üzerinde kontrol sağlamaya çalışmaktadır. Para piyasası, temel gıda maddeleri, yakıt, eğitim ve ulaşım gibi birçok işkolunda denetim ve yönlendirme yapmaktadır. Bazen sadece ekonomik faktörlerle müdahile edilirken bazen de polisiye yöntemlerle ve yargı yoluyla müdahale edilir. Döviz

piyasasına devletin müdahalesi zaman zaman polisiye yöntemlerle olurken bazen de kur serbest bırakmaktadır. Döviz piyasası sadece İran dış ticaretini etkilemez devletin bütçesini de derinden etkilemektedir. Petrol gelirlerinin bütçeye dahil edilmesi devletin belirlediği kurda olurken karaborsada farklı kur geçerli olabilir. Bazı ekonomik veya siyasi olayların kur artışına yol açtığı durumda kur artışının spekülatörlerin kötü amaçlarından kaynaklandığını ileri süren devlet yetkilileri onlarla fiziki ve polisiye yöntemlerle mücadele etmeye çalışmıştır. Bu durum da piyasada mevcut belirsizliğin artışı ve ekonomik sorunların artmasına yol açmaktadır.

İran İslam Cumhuriyeti ekonomisinin kendine özgü karakterleri ve dinamikleri vardır. İran ekonomisini anlamak için İran toplum ve tarihini göz önünde bulundurmak gerekir. Günümüzde ekonominin tümü, döviz piyasası dahil, devletin sıkı denetimi altındadır (Karamelikli ve Alizadeh 2017:32). İran ekonomisi petrol gelirlerine bağlıdır, petrol piyasalarındaki değişmeler iç ekonomiye yansımaktadır (Karamelikli, Akalin, ve Arslan 2017). Bu açıdan hem petrol gelirleri hem döviz kurundaki değişmeler İran ekonomisine derinden etki yapmaktadır. Batılı ülkelerle yaşanan siyasi krizler sonrası uygulanan siyasi, iktisadi, kültürel müeyyidelerin etkisi döviz piyasasına yansımıştır.

İran-Irak savaşı dahil birçok faktör İran devletinin ekonomiye müdahale gerekçelerini hazırlamıştır. Özellikle savaş döneminde halkın temel ihtiyaçlarına destek çıkılmış (sübvansiyonlar) piyasada pahalıya sattığı farz edilenlerle ciddi mücadele edilmiştir. Bu yolda çok geniş çaplı bir yargı sistemi kurulmuş suç atfedilen ekonomik aktivitelere gerek nakdî gerek fiziki cezalar verilmiştir. Devletin belirlediği fiyatın üzerinde satış yapanlara ekonomik terörist lakabı verilmiş ve çeşitli hapis, kırbaç ve idam cezaları uygulanmıştır. Döviz kurunun enflasyona etkisi ve ithal malların maliyetinin belirlemesi ile bağından dolayı döviz piyasası her zaman devletin gözetimi altında olmuştur. Polis ve istihbaratın döviz ve altın piyasasında müdahil olmaları ekonomik olgudan çıkıp güvenlik olayına dönüştürmüştür.

STOKÇULUĞUN EKONOMİK ETKİLERİ

Stokçuluk özellikle savaş dönemlerinde ve büyük felaketlerde ortaya çıkmaktadır ve benzer mekanizma birçok ülkede farklı şekillerde ortaya çıkmıştır. Örneğin Japonya II. Dünya Savaşı öncesinden savaş bitimine kadar bu olayla karşılaşmıştır (Griffiths 2002). Stokçuluk Adam Smith'ten beri incelene gelmektedir. Smith (1776) stokçuluğun topluma faydalı olduğunu iddia etmiştir.

> "Ama, bir tacirin filanca pazardan (az sonra yine aynı pazarda satmak üzere) zahire topladığı olursa, bunun nedeni pazara o sıradaki kadar bol malın bütün mevsim boyunca gelemeyeceğine ve dolayısıyla, fiyatın yakında yükselmesi icap ettiğine tüccarın aklının kesmesi olmalıdır. Bu yargısında yanılır da fiyat yükselmezse, tacir, böylece başka zahirenin ambara konulup saklanmasında ister istemez var olan masraf ve fire dolayısıyla, sermayesinin de bir kısmını yitirir. Bundan ötürü, pazar kurulan o belli günde gereksinmelerin karşılamalarına engel olduğu belli kimseleri bile zedeleyebildiğinden çok daha esaslı biçimde, kendi kendini örseler. Çünkü, onlar sonra, pazar kurulan herhangi bir başka gün, ihtiyaçlarını aynı derecede ucuza giderebilirler. Tacir, doğru yargıda bulunursa, büyük halk topluluğunu örseleyecek yerde, ona pek önemli bir hizmeti olur. Fiyat ucuzluğu, mevsimin gerçek darlığı ile bağdaşamayacak kadar çabuk tüketimde bulunmaya heveslendirdiği takdirde, halka bir kıtlık sıkıntısını normalde duyabileceğinden biraz önce duyurmakla tacir, bu sıkıntıyı onun sonradan kesenkes duyacağı şiddetle hissetmesini önler. Gerçekten darlık halinde, halk için yapılabilecek en iyi şey, bunun sıkıntısının elden geldiğince yılın ayrı ayrı bütün aylarına, haftalarına ve günlerine eşitlik üzere dağıtmaktır." (Smith, 1776:371).

1.1. Modern piyasalarda spekülatörlerin önemi

Spekülasyon piyasa mekanizmasının bir ürünüdür. Devletin spekülatörlerle mücadele etmesi bazı sorunlara yol açabilir. Smith'e göre devletin müdahalesi kıtlık zamanında bile uygun değildir.

> "Hükümet, bir kıtlığın doğurduğu sıkıntılara çare olsun diye, bütün tacirlere zahirelerini, kendince akla sığar saydığı fiyata satmalarını emredince, ya onların zahireyi piyasaya getirmelerine engel olur; bu ise, bazen mevsim başında bile açlık doğurabilir; yahut tacirler zahireyi piyasaya getirecek olurlarsa, halkın onu mevsim sona ermeden kesenkes bir açlık yaratacak hızla tüketmesini mümkün kılar bunu kışkırtır. Zahire ticaretinin engelsiz, kısıntısız serbestliği, açlık musibetinin biricik etkin önleyicisi olduğu gibi, kıtlık sıkıntısının da en iyi yatıştırıcısıdır. Çünkü, gerçek bir darlığın sıkıntısına çare bulunamaz; sıkıntı olsa olsa yatıştırılabilir. Kanunun tam desteğine ondan daha değer bir ticaret yoktur; hiçbir ticaret onun kadar korunmaya gerek göstermez. Çünkü âlem, hiçbir ticarete karşı, ona duyduğunca hınç beslemez.
>
> Darlık yıllarında halkın alt tabakaları, çektiklerini zahire tacirinin açgözlülüğünden bilir; tiksinti ve öfkelerine o hedef olur. Bundan dolayı, bu gibi hallerde zahire taciri kâr edeceğine, onların ortalığı kasıp kavurması yüzünden, çoğu zaman sıfırı tüketme ve ambarlarının talan edilip yok olması tehlikesiyle karşılaşır. Oysa, zahire taciri asıl kazancını, fiyatların yüksek olduğu darlık yıllarında bekler." (Smith, 1776:367).

Spekülasyon bir ekonominin hızlı ve doğru dengeye gelmesi için gereken bir eylemdir. Spekülatörler geleceği tahmin ederek yatırımcı ve tüketicilerin beklentilerinin fiyatlanmasına ve piyasanın öngörülebilirliğine katkıda bulunurlar. Risk alan bu yatırımcılar, doğru tahmin yaptıkları zaman piyasa tarafından kâr elde edilerek ödüllendirilirken, yanlış tahminlerinde zararla cezalandırılırlar. Profesyonel spekülatörlerin uzun süre piyasada kalabilmeleri için tahminlerini doğru yapmaları gerekir. Aksi halde piyasadan silinmeleri çok normal bir durum olur. Fiziki yatırım kararları alan bir girişimci veya ileri vadede iç veya dış ticaretle uğraşan biri, sadece kendi yatırım ve ticareti ile uzmanlaşıp piyasadaki belirsizlikten kaçınmak ister. Bu yükümlülüğü spekülatör alır. Riski üstlenerek gelir elde etmek isteyen spekülatörler, piyasanın dalgalanmasından kâr veya zarar ederken fiziki yatırım yapanlar, güvenli bir ekonomik alan elde etmiş olurlar. Ancak riski kabul eden spekülatör, sadece maddi zarar riskini taşımaz sağlık açısından da tehlike altındadır (Carlsson vd., 2014:8). Carlsson vd. finansal risklerin kalp damar hastalıkları üzerinde önemli etkisi olduğunu ve bu risklere maruz kalan kişilerde ölüm oranlarının yüksek olduğunu göstermişlerdir.

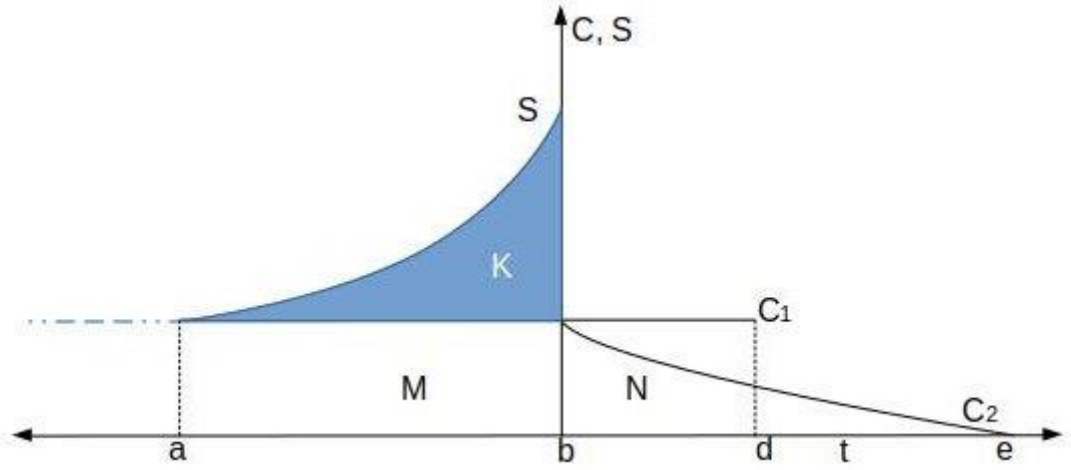
Spekülatörlerin dış ticarette de önemli katkısı bulunmaktadır. İhracatın ekonomi ve büyüme üzerine olan etkisi Michaely (1977) tarafından geniş biçimde açıklanmıştır. İthalatın azaltılması hem ülkenin ödemeler dengesine olumlu etki yaparken istihdam ve büyüme üzerinde de pozitif etki yapmaktadır. Spekülatörlerin yokluğunda dış ticaretçilerin iç ve dış piyasalardaki risklere ek olarak para ve siyasetten etkilenen kur riskini de yüklenmeleri gerekir. Spekülatörler özellikle döviz piyasasında vadeli işlemler risklerinin azalmasında önemli rol almaktadırlar. İhracatçıların ileri vadeli tahsilatları ve ithalatçıların ileri vadeli tediyelerini garantilemek amacıyla VİOP önem kazanmaktadır. Bu nedenle TCMB 31 Ağustos 2018 tarihinde 2018-35 sayılı duyurusunda sermaye piyasasına derinlik kazandırılması amacıyla VIOP işlemleri yapacağını duyurmuştur. Burada dikkat çeken nokta Merkez Bankasının Türkiye'de döviz kurlarının aşırı dalgalandığı bir sırada bu kararı almasıdır.

MODEL

Spekülasyonun etkisini araştırırken, stokçulukla ilgili modelin kurgulanması aydınlatıcı olabilir. Modelimizi kurarken bazı varsayımların yapılması gerekmektedir. Model varsayımları, üreticiler stok yapma imkanlarına sahipken tüketiciler stok yapamıyorlar. Piyasada tam rekabet koşulları geçerlidir. Stok maliyeti yoktur ve üreticilerin stok miktarı sınırlıdır. Bir ülke veya kale belirli bir tarihte yaptırıma maruz kalıyor. Bu tarihten sonra ürünün satışı oraya durdurulur. Örneğin kalenin düşman tarafından kuşatılacağı biliniyor.

2.1. Sabit fiyat durumu

Şekil 1: Fiyatların sabit olduğu model



Belirli bir zamanda ekonomiye ürünün girişi yasaklanıyor. Ancak tüketicilerin ileri kullanım için depolama imkânı olmadığı varsayımı altında tüketim zaman içinde sabittir ve değişmemektedir. Grafik 1'de gösterildiği gibi tüketim C düzeyinde ve sabittir. Ancak satıcılar normal kârlarını sürdürmek amacıyla ve b zamanında yaptırımın başlayacağı (piyasaya arzın daralacağı) öngörüsü sonucunda stokta artışlar a döneminden itibaren başlar. Stokçular üstlendikleri riske karşılık yaptırım sonrasında kâr etmeye devam ederler. Toplam stokları bitene kadar satışlar devam eder. Böylece K alanı N alanıyla eşit olmalıdır. Tüketiciler stokçunun risk alması sayesinde b döneminde stoktan tüketerek d noktasına kadar stoklardan istifade ederler.

$$\int_a^d C_t dt = M + N = \int_a^b S_t dt \qquad (1)$$

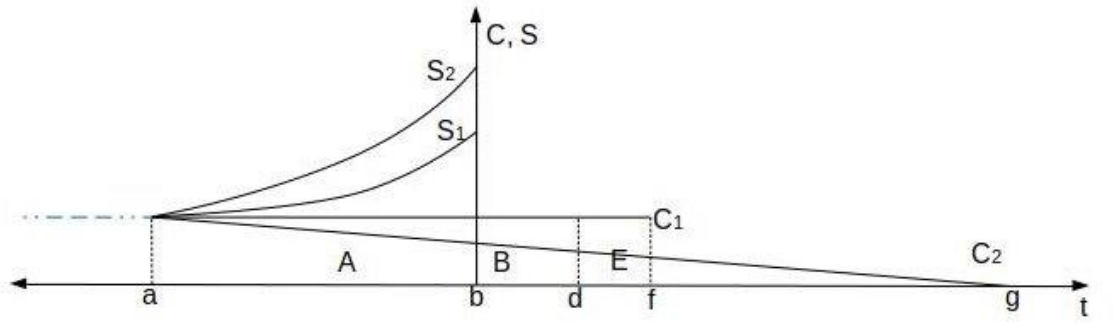
bu durumda stokçuların kâr güdüsüyle hareket etmesi, toplumun gıdasız kalmasını önlemiştir. Fiyatın en azından b döneminden sonra sabit kalması pek gerçekçi bir yaklaşım olmayabilir. Bu nedenle fiyatların değişmesi ile piyasa mekanizmasının işleyişi modele dahil edilebilir. Yaptırım uygulandıktan sonra devlet müdahalesi ile fiyatların önceki seviyede tutulması durumunda toplum d noktasına kadar tüketime devam edebilirken fiyat mekanizmasının çalışması durumunda ve fiyatların yaptırım sonrası artışı ile birlikte tüketim miktarı azalır. Böylece toplum e noktasına kadar tüketimini azaltarak devam ettirebilir. Fiyat mekanizmasına müdahale olmadığı durumda 1 no'lu denklem aşağıdaki gibi yazılabilir.

$$\int_a^b C_t^1 dt + \int_b^e C_t^2 dt = \int_a^b S_t dt \qquad (2)$$

2.2. Artan fiyat durumu

Yaptırımların başlanmasıyla birlikte fiyatların artacağı beklenilen bir durumdur. Ayrıca ileri zamanda yaptırımların beklenmesi ve satıcıların ürünlerin bir kısmını satış zincirinden çıkarıp stokladıkları durumda arz kıtlığı sonucunda fiyatlar artar. Piyasada fiyat artışları arz yönünde iki etkiye yol açar, birincisi mevcut üreticilerin daha fazla üretmesi ve ikinci etki ise mümkünse kârlı alanı gören yeni üreticilerin piyasaya girmesi ya da dışa açık ekonomi ise ithalatın artması.

Şekil 2: Fiyatların artışı durumu



Mevcut üreticilerin üretimi S1 ve yeni ve eski üreticilerin toplam üretimi S2 ile gösterilmektedir. Devlet tüketicilerin refahını koruma adına fiyatların sabit tuttuğu zaman fiyatlarda bir değişme olmaz ve C1 geçerli olur. Ancak a noktasında satıcıların depolamaya başlamasıyla veya fiyat artışı hakkında beklentilerin oluşmasıyla birlikte piyasada fiyatlar artar.

Senaryo 1. Devlet piyasa mekanizmasına müdahile ederek fiyatların sabit olduğunu ilan ediyor, alıcı ve satıcılar eski fiyattan işlem yapıyorlar. Fiyatlar devlet tarafından sabitlendiğinde kâr amacıyla yeni girişimcilerin piyasaya girmesi söz konusu olmaz. Ayrıca satıcılar satış fiyatlarının artmayacağını bildikleri için stoklamazlar. Çünkü tüketilen miktar üzerinde bir işlem fiyatları (maliyetleri) artıracağından yüksek fiyattan alıp düşük fiyattan satmaları zararlı olacakları anlamına gelir. Bu durumda yeni stok sıfırdır. b noktasında ülkede tüketim sona erer.

Senaryo 2. Devlet fiyat artışlarına izin verir, ancak yükselen fiyatlara karşı tüketicileri koruma adına sübvansiyon uygulanabilir. Bu durumda stoklama ekonomik olur ve toplum f noktasına kadar tüketime devam edebilir.

$$\int_a^f C_t^1 dt = \int_a^b S_t^2 dt = B + E \qquad (3)$$

Burada B eski üreticilerin stoklarından ve E yeni gelen stokçuların satışlarından faydalanılmaktadır.

Senaryo 3. Devlet piyasaya müdahale etmemekte ve piyasa mekanizması fiyat ve stok miktarını belirlemektedir. Bu durumda a noktasında stoklama amacıyla piyasadaki talep miktarı artar ve bu durum fiyat artışlarına yol açar. Bu durum iki etkiye sahiptir bir yandan fiyat artışından dolayı tüketim miktarı düşer ve diğer taraftan fiyat artışından dolayı arz artar. Doğal olarak ileride kıt olacak ürünün yaptırımların başlanmasından önce daha az kullanılması ve üretimin artması sonucunda toplam daha uzun süre tüketime devam eder.

$$\int_a^g C_t^2 dt = \int_a^b S_t^2 dt \qquad (4)$$

Bu üç durum karşılaştırıldığında en uzun süre devlet müdahalesinin olmaması ve en kısası ise fiyat kontrolünün tam olduğu senaryodur.

2.3. Piyasada risklerin etkisi

Döviz sadece para birimi olarak değil iç ekonomik dalgalanmalardan korunmak için kullanılan bir araçtır. Bu nedenle ekonomik ve siyasi riskler döviz kuru üzerinde etkiye sahiptir (Bailey ve Chung, 1995:558). Sadece siyasi riskler değil ekonomik politikaların belirsizliği de kur üzerinde etkilidir (Beckmann ve Czudaj, 2017:161). Döviz kurundaki belirsizlik dış ticareti derinden etkilemektedir. Söz konusu belirsizlik, uluslararası kaynak tahsisleri üzerinde olumsuz etki yapmaktadır (Perée ve Steinherr, 1989:1261). Döviz kurundaki belirsizlik ülkeye yapılan/yapılacak doğrudan yatırımlar üzerinde de negatif bir etkiye sahiptir (Darby vd. 1999:67).

Döviz piyasasında bir istikrarsızlık sadece kur artışı, azalışı üzerinde etkili olmaz, döviz alışı ve satışı arasındaki makasın açıklığını da artırır. Çünkü döviz piyasasındaki aracılar açık pozisyon vermenin riskini kapatamayacaklarını düşündükleri için kâr marjlarını yükseltirler. Bu durum istikrarsızlık beklentilerinde ortaya çıkar (Seyidoğlu 2001:392). İstikrarlı döviz piyasası durumunda döviz satış ve alış fiyatı arasındaki fark azdır. Ancak istikrarlı piyasa durumunda yıllık bazda çok sayıda alışveriş yapıldığından aracıların bu farktan elde ettikleri gelir yüksek olabilir. Ancak dikkat edilmesi gereken konu, ihracatçılar alış kuru, ithalatçılar ise satış kuru ile karşı karşıyadırlar.

$$P_S = (1 + \beta)\, P_B \qquad (5)$$

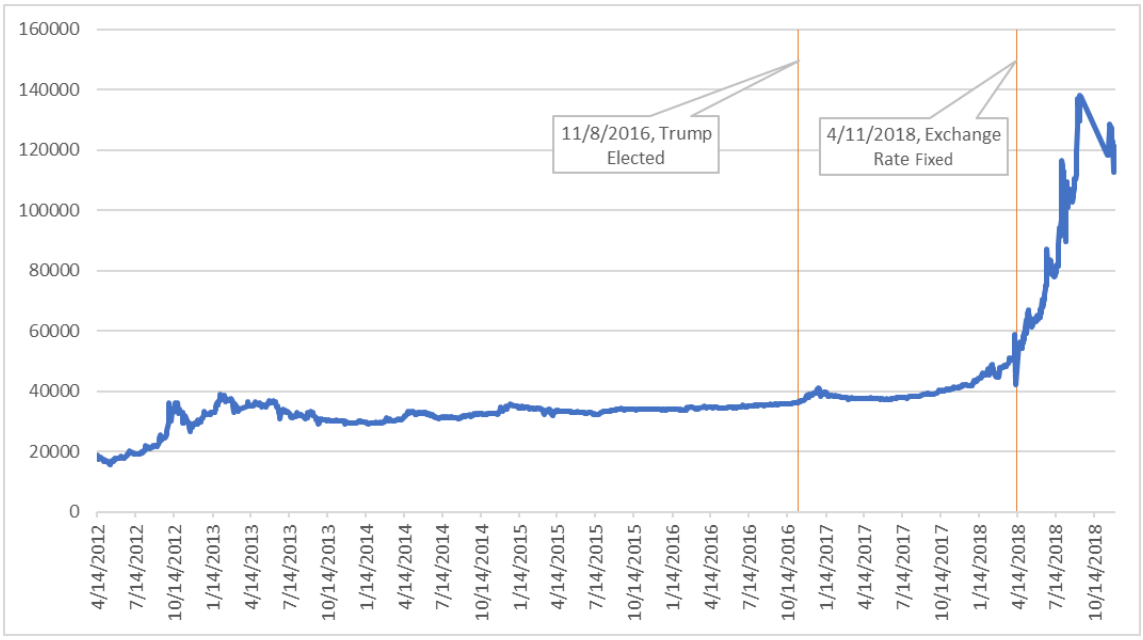
5 numaralı denklemde döviz alışı P_B, satışı P_S ve kâr marjı β ile gösterilmektedir. β aracı kurumun maliyeti, işlem hacmi ve piyasa riskine bağlıdır. Söz konusu katsayı arttığında alım satım arasındaki fiyat farkı artar. Normal ekonomide kur artışı ihracatçıların yararına ve ithalatçıların zararınadır. Ancak kur artışı ithalat maliyetinin artışından dolayı yurtiçi fiyatlarına yansımaktadır (Karamelikli ve Korkmaz 2016). Kur artışından dolayı ihracat için yaratılan fiyat avantajı enflasyon sonucu yok olabilir. Literatürde bu konu çok geniş çapta araştırılmıştır. Risk primi yüksek olduğunda kur artışı P_B ve P_S arasını açtığı için ithalatçı ihracatçıya göre çok daha yüksek kurla karşı karşıya kalır. Bu durumda da enflasyon etkisi hızla ihracat avantajını yok eder.

2. İRAN DÖVİZ PİYASASI DURUMU

Gelişmekte olan ülkelerin bazısında döviz piyasasında talep fazlası, piyasanın kontrol edilmesine yol açmaktadır. Piyasanın kontrolü talep fazlasını kontrol etme amacıyla uygulanmasına rağmen, kaçınılmaz olarak kara borsanın oluşmasına neden olur (Olgun 1984). İran ekonomisini incelerken özellikle para piyasasında, döviz kara borsasının dikkate alınması gerekliliği ortadadır (Bahmani-Oskooee 1996). Ayrıca resmi kura karşı, kara borsada geçerli olan kurun PPP geçerliliği görülmüştür (Bahmani-Oskooee ve Tankui 2008).

İran döviz piyasası özellikle 1979 yılındaki İslam devriminden sonra devletin ağır müdahalesine maruz kalmıştır ve kurun kontrol altına alınması için birçok değişik politika uygulanmıştır (Karamelikli 2018). Devlet bu yıllarda bazen ekonomik bazen de adli ve kaba kuvvet yardımıyla piyasaya baskı yapmıştır. İki tüccarın İran Merkez Bankası tarafından satılan altınlardan yüksek miktarda satın aldıkları için, ekonomik düzeni bozma suçlamasıyla idam edilmesi söz konusu müdahalenin boyutunu göstermektedir.

Grafik 1: İran Gayrı resmi ABD dolar kuru.



Kaynak: www.tgju.org

Döviz piyasasındaki hareketler sadece ekonomik çerçevede değerlendirilemez ve birçok siyasi olayın etkisi ekonomiye yansımaktadır. İran nükleer programı nedeniyle uygulanan yaptırımlar 14 Temmuz 2015 yılında sona erdirilmiştir. Beş Birleşmiş Milletler Güvenlik Konseyi daimi üyesi artı Almanya ile İran'ın yaptığı anlaşmaya göre nükleer denetimlerin arttırılması karşılığında bir çok yaptırım sonlandırılmıştır (Khodadadi 2016). Ancak ABD başkanı Trump 2016 yılında İran'la yapılan anlaşmayı gözden geçireceğini seçim kampanyasında ilan etmiştir (Kroenig 2018:94). 8 Kasım 2016 tarihindeki seçimler sonrası Trump 20 Ocak 2017 tarihinde göreve başlamıştır. İran'ın yılbaşı olarak resmî tatil olan Nevruz tatilleri süresinde döviz piyasasında hareketlenme başladı. Piyasadaki kur artışını önleme amacıyla 11 Nisan 2018 tarihinde Dolar Merkez Bankası tarafından 42000 Riyal seviyesinde sabitlendiğini ilan etti. Bu fiyat dışında yapılan işlemlerin kaçak niteleneceğini açıkladı. Sürekli İran'la yapılan anlaşmanın kabul edilemez olduğunu beyan eden Trump 24 Nisan 2018'de Fransa Cumhurbaşkanı Emmanuel Macron ile görüşmesinde İran'ın füze programlarını ele almış ve önceki anlaşmayı bırakmayarak ilave uygulamalar üzerinde anlaşmıştır. Ancak 9 Mayıs tarihinde Trump ABD devletinin anlaşmadan çekildiği ve İran'a bir dizi yaptırımların uygulanacağını ilan etmiştir. 21 Mayıs tarihinde Mike Pompeo ABD'nin çok katı finansal yaptırımlarını ilan etmiştir. 7 Ağustos 2018'de ilk yaptırım paketi uygulanmış ve 5 Kasım 2018'de ikinci yaptırım paketi uygulamaya konmuştur (Davenport 2018).

Grafik 2: İran Gayrı resmi piyasasında 2017-2018 arasında ABD dolar kuru.

Kaynak: www.tgju.org

Grafik 2'nin modelimizi teyit ettiği görülmektedir. ABD 9 Mayıs 2018 tarihinde anlaşmadan çekildi ancak bu riskin piyasada önceden satın alındığını görülmektedir. Spekülatörler durumu doğru tespit ve öngördükleri için fiyatta ani bir yükseliş görülmemektedir. İlk yaptırım paketinin uygulandığı tarihte de riskin piyasada önceden satın alındığı görülmektedir. Eylül 14-Kasım 14 arasında kurla ilgili sağlıklı bir veri bulunmadığı ve döviz piyasasında yapılan ticaretin sığ olmasıyla birlikte polisiye uygulamaların varlığı döneminde alış ve satış arasındaki fark yüksek seviyede idi. Ancak piyasadaki hâkim olan korku ve baskı göreceli olarak azaldıktan sonra döviz kuru yeniden azalmaya başlamıştır. Veriler spekülatörlerin İran döviz piyasasına olumlu etki yaptıklarını göstermektedir.

SONUÇ

Döviz kuru çoğu ürün gibi İran devletinin sıkı denetimi altındadır. Ancak kurdaki hareketlilik hem piyasadaki ürünler hem de devlet bütçesini etkilemesi nedeniyle İran ekonomi yönetiminin dikkat odağındadır. İran'da zaten yeterince serbest olmayan piyasanın işleyişine ekonomi yönetimi kendi program ve amaçlarına ters düştüğünü düşündüğünde tekrar müdahale etmektedir. Bu müdahale polisiye yöntemlerin uygulanmasına ve fiziki kontrollerin sıkılaştırmasına kadar varmaktadır. Ekonomiye mühendis gözüyle bakıldığı durumda müdahalelerin istenilen sonuçlara yol açacağına inanmaya yol açabilir. Serbest piyasa mekanizmasının çalıştırılmayıp ve denetimli piyasadaki spekülatörlerin düşmanın bir kolu, ajanı olarak görmesi sonucunda İran döviz resmi piyasasında ya da karaborsada belirsizliğin, dalgalanmanın artacağı kaçınılmazdır. Serbest piyasayı (Liberalizmi) şeytanlaştıran düşüncedeki, fikriyattaki İran ekonomi yöneticilerinden spekülatörlerin kâr güdüsüyle mal ya da döviz stoklamalarının ülke toplumunun yararına olacağını düşünmelerini bekleyemeyiz.

İran'daki gibi devletin nakdi ceza, yargılama korkusu, fiziki müdahalesi, idam korkusu nedeniyle spekülatörlerin piyasayı düzenleyici, tüketimi uzun vadeye yayma (darlığın geleceğini fark edip fiyatları ve stokları arttırarak tüketimin azalmasını teminle tüketimin daha uzun döneme yayılmasına neden olmaları) işlevlerinin yok edilmesi ya da örselenmesi durumunda ekonomide malların kıtlığı, darlığı, yokluğu ya da fiyatların daha geniş bir aralıkta dalgalanması sözkonusu olabilir. Kısaca spekülasyonun sinyalizasyon görevini yok edilerek topluma uzun dönemde zarar verilir.

İran'da spekülatörlere adeta savaş açılsa da spekülatörler İran toplumuna faydalı olmuştur. Kara borsayı düşman ilan eden İran ekonomi yönetimine bile kara borsa faydalı olmuştur. Şöyle ki Amerika'nın yaptırımlarını ön gören spekülatörler kurda artışa yol açmışlar ve bu artış kıt olan döviz gelirlerinin toplum ve devlet ekonomi yönetimince daha dikkatli harcamasına, döviz biriktirilmesine yol açmıştır. Spekülatörlerin kâr güdüsü olmasa idi ve döviz fiyatı eski seviyede devam etmiş olsaydı kısıtlı döviz gelirleri gerek özel gerek kamu sektörleri tarafından yurtdışı ithalatta kullanılarak hızlıca bitirilebilirdi. Kur artışı yaptırımlardan amaçlanan ekonomik kargaşayı önlemiş ve ülke ekonomisi yeni duruma daha iyi uyum sağlamıştır. İran ekonomi yöneticileri para arzını kontrol etme veya şeffaflığın artırılması gibi konularda ilerleme sağlamadıklarından kur artışı bir sonuç değil bir neden olarak sunulmuştur ve bu durum kur artışından dolayı olası avantajların yok olmasına neden olmuştur. İran ekonomi yöneticilerinin serbest piyasa kurallarına müdahale etmemesi, mal, döviz arz ve talebinin istikrarlı seyri için iktisadi, siyasi tedbirleri alması toplum yararına olacaktır. Mal ya da döviz stoklarının artması halinde ise bunu ekonomide bir tehlike işareti olarak görüp idari ya da adli uygulamalarla değil piyasa verilerini dikkate alarak serbest piyasa kuralları içinde arz ve talep dengesini kısa, orta ve uzun dönemde temine yönelmesi toplum yararına olacaktır. Merkez bankasından altın almak suç olmamalıdır. Merkez bankası satacağı altın miktar ve fiyatını ekonomik şartlara göre ayarlamasını bilmelidir. İki tüccarın idamı merkez bankası yöneticilerinin fiyat ve miktar ayarı yapamadığını gösterir.

KAYNAKÇA

Bahmani-Oskooee, Mohsen. 1996. "The black market exchange rate and demand for money in Iran". *Journal of Macroeconomics* 18(1):171-76.

Bahmani-Oskooee, Mohsen ve Altin Tankui. 2008. "The black market exchange rate vs. the official rate in testing PPP: Which rate fosters the adjustment process?" *Economics Letters* 99(1):40-43.

Bailey, Warren ve Y. Peter Chung. 1995. "Exchange Rate Fluctuations, Political Risk, and Stock Returns: Some Evidence from an Emerging Market". *The Journal of Financial and Quantitative Analysis* 30(4):541-561.

Beckmann, Joscha ve Robert Czudaj. 2017. "Exchange rate expectations and economic policy uncertainty". *European Journal of Political Economy* (47):148-62.

Carlsson, Axel C. vd. 2014. "Financial stress in late adulthood and diverse risks of incident cardiovascular disease and all-cause mortality in women and men". *BMC Public Health* 14(17):1-8.

Darby, Julia, Andrew Hughes Hallett, Jonathan Ireland, ve Laura Piscitelli. 1999. "The Impact of Exchange Rate Uncertainty on the Level of Investment". *The Economic Journal* 109(454):55-67.

Davenport, Kelsey. 2018. "Timeline of Nuclear Diplomacy With Iran". *Arms Control Association*.

Griffiths, O. 2002. "Need, greed, and protest in Japan's black market, 1938-1949". *Journal of Social History* 35(4):825-858.

Karamelikli, Hüseyin. 2018. "İran döviz kuru politikalarının ekonomik etkileri". Ss. 611-620 içinde *1st International Congress of Political, Economic and Financial Analysis*. C. 2.

Karamelikli, Huseyin, Guray Akalin, ve Unal Arslan. 2017. "Oil exports and non-oil exports: Dutch disease effects in the Organization of Petroleum Exporting Countries (OPEC)" editör M. Bahmani-Oskooee. *Journal of Economic Studies* 44(4):540-51.

Karamelikli, Hüseyin ve Naseraddin Alizadeh. 2017. "İran İslami Bankacılık Sistemi Üzerine Bir Değerlendirme". *Bankacılık ve Sigortacılık Araştırmaları Dergisi* 2(11):36-58.

Karamelikli, Huseyin ve Suna Korkmaz. 2016. "The dynamics of exchange rate pass-through to domestic prices in Turkey". *Journal of Business Economics & Finance* 5(1):39-48.

Khodadadi, Masood. 2016. "A new dawn? The Iran nuclear deal and the future of the Iranian tourism industry". *Tourism Management Perspectives* (18):6-9.

Kroenig, Matthew. 2018. "The return to the pressure track: The trump administration and the Iran nuclear deal". *Diplomacy and Statecraft* 29(1):94-104.

Michaely, Michael. 1977. "Exports and growth". *Journal of Development Economics* 4(1):49-53.

Olgun, Hasan. 1984. "An analysis of the black market exchange rate in a developing economy — The case of Turkey". *Review of World Economics* 120(2):329-47.

Perée, Eric ve Alfred Steinherr. 1989. "Exchange rate uncertainty and foreign trade". *European Economic Review* 33(6):1241-64.

Seyidoğlu, Halil. 2001. "Uluslararası İktisat Teori Politika ve Uygulama". Güzem yayınları, İstanbul.

Smith, Adam. 1776. *An Inquiry into the Nature and causes of the wealth of nations. Book IV, Chapter V*. Edinburgh.

Hüseyin Karamelikli
Doç. Dr., Karabük Üniversitesi, İİBF
https://orcid.org/0000-0001-7622-0972
E-posta: hakperest@gmail.com

Yazı Bilgisi:

Alındığı tarih: 04 Ocak 2018.
Yayına kabul edildiği tarih: 28 Aralık 2018.
E-yayın tarihi: 28 Aralık 2018.
Yazıcı çıktı sayfa sayısı: 10.
Kaynak sayısı: 19.

Hakemler: