AÇIK BANKACILIK:
KİŞİSEL VERİLERİN KORUNMASINA BİR TEHDİT Mİ?*

Furkan Güven TAŞTAN** **Utku SARUHAN*****

Özet

Finansal teknolojilerin önemli çıktılarından birini oluşturan açık bankacılık, müşteri verilerini istek veya onayları doğrultusunda üçüncü taraf sağlayıcıların kullanımına açarak müşteri yararına çeşitli ürün ve hizmetlerin sunulmasını sağlamaktadır. Bu kavramın temel yasal altyapısı; Avrupa Birliği'nde PSD2, Türkiye'de 7192 sayılı Kanun'la oluşturulmuştur. Çalışmamızda açık bankacılık kavramı, açık bankacılık ilişkilerindeki taraflar, açık bankacılığın Türk Hukukunda ve Avrupa Birliği Hukukundaki gelişimi ile 6698 sayılı Kişisel Verilerin Korunması Kanunu temel alınarak kişisel verilerin korunmasına dair belirlediğimiz yedi hukuki problem ele alınmıştır.

Anahtar Kelimeler: Açık Bankacılık, Ödeme Hizmeti, Hesap Bilgi Hizmeti, Ödeme Başlatma Hizmeti, Kişisel Verilerin Korunması

Abstract

The notion of open banking has emerged as one of the significant output of financial technologies. It provides customers with several products and services for their benefits by making their data available to third-party providers following the customers' request or consent. This concept's legal framework was created by the PSD2 in the EU and the Law No. 7192 in Turkey. This research addresses the concept of open banking, the parties of open banking, legal background of open banking in the Turkish Law and the European Union Law, and seven legal issues identified on the protection of personal data based on the Turkish Data Protection Law (No. 6698).

Keywords: Open Banking, Payment Service, Account Information Service, Payment Initiation Service, Data Protection

---

* Bu çalışmada öne sürülen fikirler tamamıyla yazarlara aittir. Değerlendirmeler yazarların bağlı bulundukları kurumların görüşlerini temsil etmemektedir.

Görüş ve eleştirileriyle çalışmamıza katkı sağlayan **Doç. Dr. Leyla Keser**'e, **Av. Yaşar K. Canpolat**'a ve **Av. Ezgi Damla Saruhan'a** teşekkür ederiz.

** Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi, Medeni Hukuk Anabilim Dalı Araştırma Görevlisi
0000-0002-4565-3895 LinkedIn

*** Türkiye Cumhuriyet Merkez Bankası, Uzman Yardımcısı,
0000-0003-3980-3647 LinkedIn

Önerilen Atıf Biçimi: Taştan, Furkan Güven/Saruhan, Utku; "Açık Bankacılık: Kişisel Verilerin Korunmasına Bir Tehdit Mi?", academia.edu (Yayın Tarihi: 4 Kasım 2020)

İÇİNDEKİLER

GİRİŞ

İzmir depreminin üzerinden 65 saat geçmişken,
kahraman itfaiyecinin parmağından hayata sımsıkı sarılarak
umutlarımızı tazeleyen Elif bebeğe…

Dijital çağla birlikte bilgiye kolay erişim, akıllı telefon kullanımının artması ve bunun getirdiği rekabetçi sonuçlar, bireylerin finansal hizmetlere ulaşımını kolaylaştırmıştır. 70'lerden itibaren teknolojinin bankacılık sektörüne olan etkisi artarak devam etmiş ve 2000'lerde toplum internet bankacılığıyla tanışmıştır. Bankacılık sektörü geçmişten günümüze teknoloji kullanımında ön plana çıkan bir sektör olarak zihinlerde yer edinmiştir[2].

Teknoloji, tüketici hakları, sermaye piyasaları ve rekabet gibi pek çok ilişkili alanda yenilikler gerçekleşmesine rağmen, geride bıraktığımız 2010'lu yıllara kadar bankacılıkta pek çok süreç eski usul ve sistemlerle sürdürülmeye devam etmiştir. Bu açıdan 2010'ların en büyük getirisi, finansal hizmetler alanındaki teknolojik gelişmelerin *FinTech* (financial technologies) adıyla yeni bir devinim başlatarak bankacılık ve finans alanında teknolojik dönüşümü hızlandırması olmuştur. FinTech faaliyetlerinin sonucunda geliştirilen ürün ve hizmetler, geleneksel banka müşteri ilişkileri başta olmak üzere ödeme hizmetlerini geri dönüşü olmayan bir değişime sürüklemiştir.

FinTech faaliyetlerinin önemli çıktılarından birisi de açık bankacılık hizmetleridir. Açık bankacılık bağlamında oluşturulacak yeni ürün ve hizmetlerin, inovasyonu hızlandırarak bankaların işlevinin platforma indirgenmesine (platformization of banking) yönelik büyük değişimi tetikleyeceği öngörülebilir bir gerçek olarak karşımızda durmaktadır[3]. Müşteriler tarafından elle yapılan ve tekrarlayan iş akışları, yeni ürün ve hizmetlerle otomatik bir sistem içerisine alınarak daha güvenli ve daha ekonomik bir şekilde yapılabilecektir[4].

İngiltere orijinli olarak başlayan açık bankacılık faaliyetleri, Avrupa Birliği kanadında Ödeme Hizmetleri Direktifi 2 (PSD2) ile düzenlenmiştir. Öte yandan ABD, Kanada, Singapur,

---

2 Remolina, 2019, s. 5.

3 Zachariadis ve Ozcan, 2017, s. 14; Basel Committee on Banking Supervision, 2019, s. 4.

4 Milne, 2016, s. 9; Mansfield-Devine, 2016, s. 9. Açık Bankacılığın getirdiği ekosistemde gelecekte kendisinden oldukça söz ettirecek bir araç olan akıllı sözleşmelerden (*smart contracts*) faydalanılmasının ilerleyen dönemde üçüncü bir hizmet türü olarak açık bankacılık hizmetleri arasında yer alacağını değerlendirmekteyiz.

Endonezya ve Japonya gibi büyük finansal merkezlerde de açık bankacılığın mevzuat altyapısına, denetimine ve kişisel verilerin korunmasına ilişkin çeşitli gelişmeler yaşanmaktadır[5]. Gelişmiş bir bankacılık sistemine sahip olan Türkiye de, 7192 sayılı Kanun'un kabul edilmesiyle birlikte bu konuda Dünya'daki öncü devletlerden biri olmayı başarmıştır[6].

Çalışmamızda bu kapsamda Avrupa Birliği hukukuyla karşılaştırmalı şekilde sırasıyla (i) açık bankacılık kavramına ve açık bankacılık ilişkisindeki taraflara; (ii) açık bankacılık hizmetlerinin gelişimine, (iii) daha geniş bir perspektifle açık bankacılık kavramlarının karşılaştırmalı incelemesine, (iv) açık bankacılık işlemlerinin kişisel verilerin korunması ekosistemindeki karşılıklarına, kişisel verilerle ilgili muhtemel hukuki problemlere ve değerlendirmelerimize yer verilecektir.

I. GENEL OLARAK AÇIK BANKACILIK

A. AÇIK BANKACILIK KAVRAMI

Yirmi birinci yüzyılda dünyadaki en değerli kaynaklardan birinin veri olduğu anlaşılmış, buna paralel olarak finans sektöründe de müşterilerin verilerini değerlendirme ve koruma hususları önem kazanmaya başlamıştır[7]. Bankalar ve diğer finans kuruluşları, müşterilerinin işlem bilgileri, düzenli fatura ödemeleri, harcama bilgileri, kullanılan kredi bilgileri, kimlik bilgileri, yatırım tercihleri, işletme performans bilgileri gibi birçok veriyi toplayarak kapsamlı bir veri havuzunun sahibi olmuştur. Toplanan verilerin hem banka içindeki birimler arasında hem de diğer banka ve piyasa oyuncularıyla sınırlı bir şekilde paylaşılmasının, sistemden istenen verimliliğine ulaşılmasını zorlaştırması nedeniyle, verilerin daha etkin kullanılarak bir transfer unsuru haline getirilmesi amacıyla açık bankacılık kavramı geliştirilmiştir[8].

Teknik bir anlam taşımaktan uzak şekilde genel olarak açık bankacılık, teknolojik gelişmeler ışığında müşteri verilerinin üçüncü taraflarla paylaşılması ve dolayısıyla geleneksel bankacılık anlayışındaki değişim sürecini ifade etmektedir[9]. Açık bankacılıkta bankalar ve diğer ödeme hizmeti sağlayıcıları, müşterilerinin verilerini izinleri doğrultusunda üçüncü taraf sağlayıcılarla (TPP[10]) paylaşmaya teşvik edilmektedir[11]. Açık bankacılık, bankacılık sistemini klasik müşteri - banka temelli kapalı bir sistemden, birden çok paydaşın farklı ilişki türleriyle zenginleştirebileceği açık bir boyuta taşımaktadır.

Dünyanın çeşitli ülkelerinde yapılan regülasyonlar ışığında somut ve teknik bir terim olarak açık bankacılık, banka ve diğer ödeme hizmeti sağlayıcılarından hizmet alan müşterilerin verilerinin, rızalarına dayalı olarak Uygulama Programlama Arayüzü (API[12]) ve

5 Basel Committee on Banking Supervision, 2019, s. 5.
6 Pymnts. Deep Dive: What Does Open Banking Mean For Turkish Banks?.
7 Remolina, 2019, s. 4.
8 Remolina, 2019, s. 6 – 7.
9 Remolina, 2019, s. 9.
10 Çalışmamızda ödeme hizmeti sağlayan üçüncü taraf hizmet sağlayıcılar yaygın kullanıma uygun şekilde *Third Party Provider* (*TPP*) olarak anılacaktır.
11 Tsang, 2019, s. 358.
12 API'ler (*Application Programming Interface*), basit tabirle en az iki sistemi birbiri ile iletişim haline getirmek amacıyla ortak bir dil yaratan mekanizmalardır (Basel Committee on Banking Supervision, 2019, s. 9; Gün,

benzeri güvenli iletişim kanalları üzerinden diğer ödeme hizmeti sağlayıcılarla paylaşılmak suretiyle, kendilerine sunulan inovatif ürün ve hizmetleri ifade eder[13].

Açık bankacılık hizmetleri, müşterilere yakın gelecek için farklı bankalardaki hesapları tek arayüzde yönetebilme, daha hızlı, ekonomik ve güvenli ödeme başlatma hizmetlerinden yararlanma[14], işlem maliyetlerini azaltma, entegre bir ödeme pazarından faydalanma, mevduatlar için daha yüksek faiz teklifi ve krediler için daha düşük faiz teklifi alabilme, hizmet aldıkları banka veya finans kuruluşlarını değiştirmeyi kolaylaştırma[15] gibi imkânlar vaad etmektedir. Bu hizmetler bankalar bakımından ise; müşteri istihbaratı ve finansal risklerin yönetimi, bankaların müşteri bazlı olarak daha iyi hedefleme yapabilmesi ve bu sayede müşterilerden daha fazla gelir sağlama imkânı[16], finansal durumu zayıflayan müşterilerin takibi gibi avantajlar sağlamaktadır.

Açık bankacılık sisteminin nihai hedefinin, ödeme hizmetlerinde daha ucuz, daha hızlı ve daha güvenli bir ekosistem yaratma amacına dayandığı göz önüne alındığında, geliştirilen sistemin bu alanlarda rekabetçi bir ortam yaratacağı öngörülebilir. Günümüz bankacılığında sermaye yeterlilikleri, bankacılık düzenlemelerinde öngörülen diğer şartlar ve işletme giderlerinin yüksekliği piyasada sınırlı sayıda oyuncunun yer almasına izin vermektedir. Özellikle Birleşik Krallık ve Avrupa Birliği'nde kabul edilen arayüzlerin standartlaştırılmasına yönelik düzenlemelerin amacı, yeni aktörlerin ödeme sistemleri evrenine daha kolay giriş yapmasını sağlamaktır. Açık bankacılık faaliyetlerinin yaratacağı bu ortam özellikle zincir alışveriş siteleri, FinTech kuruluşları, start-up'lar gibi bağımsız oluşumların finansal piyasalara girişini teşvik edecektir[17].

Açık bankacılık hizmetleri; rekabet hukuku, kişisel verilerin korunması hukuku, tüketici hukuku, bankacılık hukuku ve bunların düzenleyici otoritelerinin yetki sınırları içerisinde yer alan disiplinler arası bir alandır. Bu hizmetler, anılan faydalarının yanı sıra, madalyonun diğer tarafında geleneksel banka - müşteri arasındaki sadakat ilişkisini oldukça esnetmesi ve anılan alanlara nüfuz eden birçok tartışmayı beraberinde getirmiştir. Örneğin disiplinler arası niteliği nedeniyle açık bankacılık hizmetlerinde idari otorite fragmantasyonu gündeme gelebilecek; bu durum da uygulama ve denetim açısından sistemin gelişimini yavaşlatacak ve ek maliyetler doğurabilecektir[18]. Dolayısıyla önümüzdeki yıllarda bir momentum yakalaması beklenen açık bankacılık hizmetlerinin birçok riski de beraberinde getirdiğini ifade etmek mümkündür.

Taşıdığı riskler itibariyle kimi bankaların, müşterilerinin verilerini ve bir anlamda müşterilerini üçüncü taraflarla paylaşmak istememesi ve API standartlarına uyum konusundaki

---

2019, s. 4; Milne 2016, s. 10; Remolina, 2019, s. 12). API, Bankacılık Düzenleme ve Denetleme Kurumu'nca çıkarılan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te *"Bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilmesi için oluşturulmuş uygulama programlama arayüzü"* olarak tanımlanmıştır (m. 3/1-c).

13 Brodsky ve Oakes, s. 2; Zetzsche ve diğerleri, 2019, s. 24.

14 Açık bankacılık ödeme sistemlerinde maliyetler sebebiyle müşteriler tarafından tercih edilmeyen küçük tutarlı gönderilerin artmasına da olanak tanır. Örneğin, telif haklarına ilişkin olarak sanatçılara yapılan ödemeler, hayır kurumlarına yapılan küçük bağışlar (Mansfield-Devine, 2016, s. 13). Açık bankacılık sisteminin bir diğer faydası yüksek meblağlı ödemelerde müşteriye ekstra güvenlik sağlanması imkânıdır (Milne 2016, s. 10).

15 Meral, 2019, s. 28; ProCompliance. Açık Bankacılık II - Dünya Uygulamaları.

16 ProCompliance. Açık Bankacılık II - Dünya Uygulamaları.

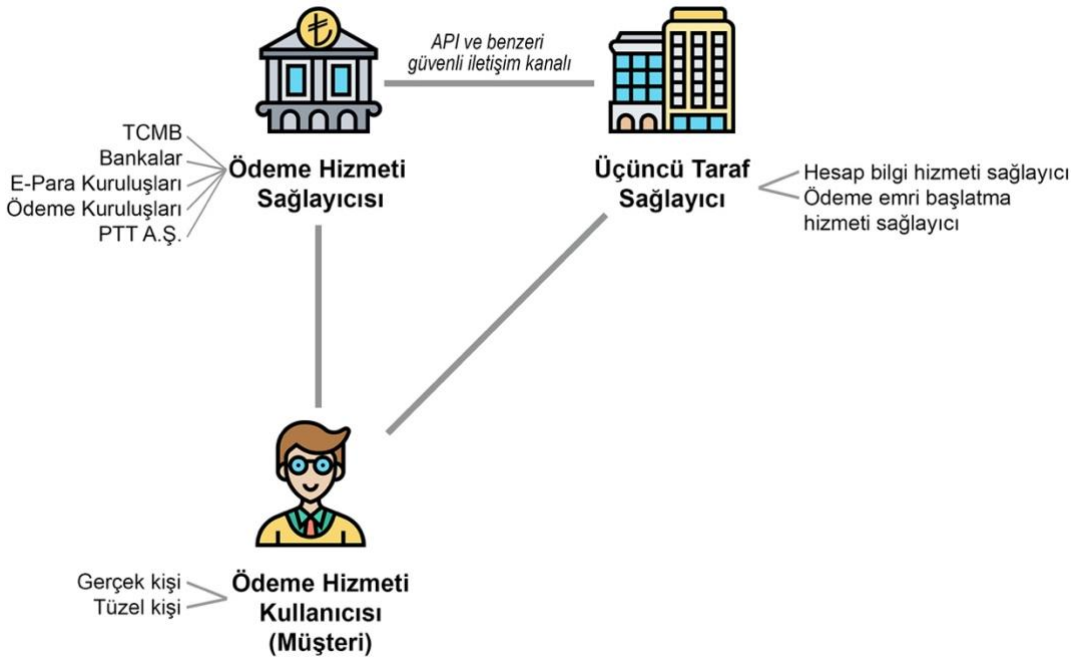
17 Zetzsche ve diğerleri, 2019, s. 24.

18 Basel Committee on Banking Supervision 2019, s. 5, 11; Remolina, 2019, s. 20; Tsang, 2019, s. 366 vd.

maliyetler nedeniyle, açık bankacılık uygulamalarına ilişkin muhafazakâr bir yaklaşım sergilediğini söylenebilir[19]. TPP'lere ödeme başlatma imkânı tanınması ile birlikte bireyler, API'ler kanalıyla kredi kartı olmadan ödemelerini doğrudan satıcıya gerçekleştirebileceklerdir. Bu durumun özellikle kredi kartı çıkaran kartlı sistem kuruluşları açısından oldukça büyük bir işlem kaybı getireceğini değerlendirmek mümkündür[20]. Nitekim açık bankacılık sistemini bankacılık sektöründe faaliyet göstermek isteyen *Google*, *Apple*, *Facebook* ve *Amazon* gibi şirketlerin sisteme getirdiği bir truva atı (trojan) olarak değerlendiren bir eğilim de bulunmaktadır[21]. Özellikle ödemeler sisteminde *Visa*, *American Express*, *Mastercard* gibi belli başlı firmaların pazar hâkimiyeti karşısında, büyük şirketlerin açık bankacılık kanalıyla bankaları ve bu şirketleri tasfiye ederek pazardan pay sağlayacakları düşüncesi bankacılık sistemindeki oyuncuları değişime ve daha güçlü bir sisteme sahip olmaya zorlamaktadır[22].

B. AÇIK BANKACILIK İLİŞKİLERİNDEKİ TARAFLAR

Açık bankacılık hizmetlerinde üç temel aktör bulunmaktadır. İlk olarak açık bankacılık hizmetinden faydalanan müşteri, ödeme sistemleri literatüründe *ödeme hizmeti kullanıcısı* olarak anılmaktadır. İkinci taraf müşterinin ödeme hesabının bulunduğu *ödeme hizmeti sağlayıcısıdır.* Son taraf ise müşterinin verilerinin paylaşıldığı *üçüncü taraf sağlayıcı*lardır.



Şekil 1: Açık Bankacılık İlişkilerindeki Taraflar

[19] Basel Committee on Banking Supervision 2019, s. 6; Brodsky ve Oakes, s. 6; Mansfield-Devine, 2016, s. 9; Milne 2016, s. 5. Özellikle küçük bankaların bu süreçte nasıl bir yol izleyeceği gelecek için bir soru işareti yaratmaktadır.

[20] Mansfield-Devine, 2016, s. 9.

[21] Remolina, 2019, s. 26.

[22] Remolina, 2019, s. 30.

1. Ödeme Hizmeti Kullanıcısı (Müşteri)

Ödeme hizmeti kullanıcısı, ödeme emrini başlatan veya ödeme hizmetinden faydalanan gerçek veya tüzel kişidir. Bir başka deyişle ödeme hizmeti kullanıcısı, finansal hizmetten yararlanan müşteriyi[23] ifade eder.

Açık bankacılık sistemi özelinde ödeme hizmeti kullanıcısı, hesap bilgi hizmeti ve ödeme başlatma hizmetinden yararlanan kişidir. Ödeme hizmeti kullanıcısı, kendi istek veya onayıyla ödeme hizmeti sağlayıcıları nezdindeki hesaplarına üçüncü taraf sağlayıcılar kanalıyla tek bir ekrandan erişilebilecek ya da başka bir ödeme hizmeti sağlayıcısında bulunan ödeme hesabından üçüncü bir kişiye ödeme gerçekleştirebilecektir.

2. Ödeme Hizmeti Sağlayıcısı

Ödeme hizmeti sağlayıcısı, müşterinin hesap ilişkisi içinde bulunduğu banka ve diğer finansal kuruluşları ifade eder[24]. Ödeme hizmeti sağlayıcıları, müşterilerine ilişkin pek çok veriyi muhafaza etmektedir. Açık bankacılık sistemi ile ödeme hizmeti sağlayıcılarına iki önemli yükümlülük getirilmektedir. Bunların ilki müşteri ilişkisi içerisinde elde ettikleri finansal verileri müşterilerin istek ve onayları doğrultusunda üçüncü taraf sağlayıcılarla paylaşma, ikincisi ise veri paylaşımı için üçüncü taraf sağlayıcıların erişebileceği arayüz uygulamalarını, sistemlerine entegre etme yükümlülüğüdür.

3. Üçüncü Taraf Sağlayıcı

Üçüncü taraf sağlayıcı, API'ler veya diğer arayüzler kanalıyla ödeme hizmeti kullanıcılarının diğer ödeme hizmeti sağlayıcılarda bulunan verilerine erişim sağlayabilen ödeme hizmeti sağlayıcılarını ifade etmektedir. Ödeme kuruluşları, bankalar, FinTech şirketleri, perakende mağaza zincirleri, sosyal medya ağları veya telekomünikasyon şirketleri öngörülen kanuni şartları sağlamak kaydıyla üçüncü taraf sağlayıcı olabilir[25].

Üçüncü taraf sağlayıcılar müşterilerine hesap bilgi hizmeti sağlayıcısı (AISP) ve ödeme başlatma hizmeti sağlayıcısı (PISP) rolüyle iki farklı kategoride hizmet sağlayabilmektedir[26]. Hesap bilgi hizmeti sağlayıcıları, müşterinin bir veya birden fazla ödeme hizmeti sağlayıcısında

---

[23] Müşteri kavramına 5411 sayılı Kanun'da pek çok noktada değinilmesine karşın, tanımına yer verilmemektedir.

[24] Bu noktada vurgulamak gerekir ki ödeme hizmeti sağlayıcılar; bankaları, ödeme kuruluşlarını ve elektronik para kuruluşlarını da içine alan çatı bir kavramı ifade etmektedir (bkz. 6493 sayılı Kanun, m. 13). Anlam kargaşasına yol açmamak amacıyla çalışmamızda ödeme hizmeti sağlayıcıları, yalnızca müşterilerin hesap ilişkisi içinde olduğu taraf için kullanılırken; üçüncü taraf sağlayıcılar ise açık bankacılık hizmeti sunan diğer ödeme hizmeti sağlayıcılarına karşılık olarak kullanılmıştır.

[25] Zachariadis ve Ozcan, 2017, s. 4; Basel Committee on Banking Supervision, 2019, s. 6 - 16. Literatürde ayrıca üçüncü taraf sağlayıcılardan veri toplayan *Financial Data Aggregator*'dan (FDA, Finansal Veri Derleyenler) bahsedilmekte ve bu kişiler de dördüncü taraf olarak anılmaktadır (Basel Committee on Banking Supervision 2019, s. 6).

[26] Mansfield-Devine, 2016, s. 10; Açık bankacılık kavramının gelecekte yeni hizmet sınıfları oluşturacağı göz önüne alınarak üçüncü taraf sağlayıcıların daha geniş bir kavram olarak değerlendirilmesi gerektiği kanısındayız.

bulunan hesap bilgilerine API'ler veya diğer arayüzler aracılığıyla ve kendisinin izni doğrultusunda erişim sağlayarak ona bu bilgileri tek bir arayüzde sunan sağlayıcılardır[27].

Ödeme başlatma hizmeti sağlayıcıları (PISP) ise talebi doğrultusunda müşterinin ödeme hizmeti sağlayıcısındaki hesabından üçüncü bir kişiye ödeme hizmeti başlatan sağlayıcılardır. Bu işlem, para aktarma olabileceği gibi çevrimiçi bir satın alma da olabilir[28]. Ödeme başlatma hizmeti sağlayıcılarının faaliyetleriyle kullanıcının banka hesabı ile satıcı arasında doğrudan para transferi gerçekleştirilir ve kart kullanım ücretleri ortadan kaldırılır[29].

C. AVRUPA BİRLİĞİ HUKUKUNDA AÇIK BANKACILIĞIN GELİŞİMİ

Açık bankacılık faaliyetlerinin mevzuat altyapısını düzenlemek için iki farklı yaklaşım ön plana çıkmıştır[30]. Singapur, Japonya ve Hindistan'ın uygulandığı **pazara dayalı gelişim** yaklaşımında, açık bankacılık faaliyetleri zorunlu bir aktivite olarak tanımlanmamıştır. Bu yaklaşımda açık bankacılık, piyasa oyuncularının kendi istekleri doğrultusunda TPP'lerle veri paylaşımını kabul etmelerine dayanmaktadır. Kamu otoriteleri de bu sistemi desteklemekte ve bağlayıcı olmayan API düzenleme rehberleri, standartlar çıkartmakta ve teknik özellikler belirleyerek TPP'lere yol göstermektedir. Bunun yanı sıra opsiyonel olarak otoriteler, API'lerin isimleri ve verdikleri hizmetlerin ilan edildiği listeler de yayınlamaktadır.

Avrupa Birliği'nin de içinde bulunduğu **zorunluluk yaklaşımında** ise bankalar ve diğer hesap hizmeti veren ödeme hizmeti sağlayıcıları, ödeme başlatma hizmeti ve hesap bilgi hizmeti veren TPP'ler, müşterilerin verilerine güvenli bir şekilde erişim sağlama imkânını oluşturmakla yükümlü kılınmaktadır. Birleşik Krallık[31] ve Avustralya tarafından da uygulanan bu yaklaşımda düzenleyici idari otoriteden alınacak faaliyet izninin bir sicile kaydedilmesi esas

---

27 Mansfield-Devine, 2016, s. 10.
28 Gün, 2019, s. 13; Zachariadis ve Ozcan, 2017, s. 4.
29 Mansfield-Devine, 2016, s. 10.
30 Remolina, 2019, s. 39.
31 Açık bankacılık kavramının başarılı bir örneği olan İngiltere'nin açık bankacılık konusunda Avrupa Birliği'nden daha kurumsal ve daha ileri bir noktada olduğunu söylemek mümkündür (Basel Committee on Banking Supervision, 2019, s. 5), nitekim PSD2 düzenlemesi bankaları sadece verileri üçüncü taraf sağlayıcılarla paylaşmakla yükümlü kılarken, İngiltere'deki düzenlemeler bankaları TPP'lerin kolayca entegrasyon sağlayabilecekleri, standart bir formatta veri paylaşım yapmaya zorlamaktadır (Manthorpe, 2018). İngiltere'de rekabet otoritesi *Competition and Markets Authority* (CMA) 2016'da hazırladığı raporda (Rapora erişim için Bkz: CMA Resmi İnternet Sitesi Link: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report), bankacılık sisteminde rekabet ortamının zayıf olduğunu, bankacılık sisteminin büyük bankalar güdümünde hareket ettiğini ve küçük bankaların bu sistemde rekabete katılması gerektiğini vurgulayan bir rapor hazırlamıştır. bu gelişmeler bankacılık ve finans alanında inovasyonun arttırılması ile rekabetin geliştirilmesi amacıyla İngiltere'nin açık bankacılık serüvenini başlatmıştır. 2016 yılında İngiltere'de API'lerin standartlaştırılması sürecinin geliştirilmesi için Birleşik Krallık Hazinesi ve *Open Data Institute*'nin ortak çalışması ile 2016 yılında *Open Banking Working Group* (Açık Bankacılık Çalışma Grubu - OBWG) kurulmuştur (Mansfield-Devine, 2016, s. 11; Milne, 2016, s. 4; Meral, 2019, s. 28). OBWG'nin temel amacı Birleşik Krallık'ta açık bankacılık altyapısını oluşturmak ve API'lerin standartlaştırılması gibi PSD2'de yer alan temel hedeflerin gerçekleştirilmesini sağlamaktır (Mansfield-Devine, 2016, s. 11). İngiltere'de dokuz büyük banka Açık Bankacılığın geliştirilmesi ve API'lerin özelliklerini belirlenmesi amacıyla 2016 yılında CMA tarafından oluşturulan *Open Banking Implematation Entitiy* (OBIE – Açık Bankacılık Uygulama Kurumu) bünyesinde birlikte çalışmaya başlamıştır (Remolina, 2019, s. 44). *Financial Conduct Authority* (FCA) API'lerle müşteri verilerine erişim sağlayan TPP'leri regüle etme görevini üstlenmiş ve TPP'leri yetkili kılma faaliyetini üstlenmiştir (Remolina, 2019, s. 41). Bu gelişmeler doğrultusunda piyasadaki rekabeti ve inovasyonu arttırmak amacıyla AB'deki PSD2 süreci de baz alınarak, açık bankacılık süreci 2017 yılında bankaların müşterilerinin verilerini standart bir API formatında paylaşılmaya başlanmasıyla fiiliyata geçmiştir (Manthorpe, 2018).

alınmıştır. Kıta Avrupasında yer alması ve aday ülke olması itibariyle Türkiye'nin de zorunluluk yaklaşımını benimseyeceği söylenebilir.

Avrupa Birliği'nde 1980'lerden itibaren finansal hizmetlerin entegrasyonuna ilişkin politik, ekonomik ve stratejik birçok süreç yaşanmıştır. Avrupa'da tek ve ortak bir pazar oluşturulması amacıyla kabul edilmiş Avrupa Tek Senedi (*Single European Act-1986*), aynı zamanda Avrupa Birliği'nde finansal hizmetler alanında pek çok gelişmeyi tetiklemiştir[32].

Bu konudaki ilk atılım Avrupa Birliği'nin genişleme sürecinin ardından *Single Euro Payment Area* (Avrupa Tek Ödeme Alanı - SEPA)'nın yasal altyapısının oluşturulmasıyla gerçekleştirilmiştir[33]. Avrupa Birliği'nin ikinci büyük atılımı olarak nitelendirebileceğimiz süreçte 2007'de yürürlüğe konulan *Payment Services Directive* (PSD) ve 2008 küresel krizinin ardından *Alternative Investment Fund Manager Directive* (AIFMD 2011), *European Markets Infrastructure Regulation* (EMIR 2012), *Capital Requirements Directive* (CRD IV 2013), *Capital Requirement Regulation* (CRR 2013) ve *Markets in Financial Instruments Directives* (MiFID II 2014) düzenlemeleri yürürlüğe konulmuştur[34]. Finansal hizmetler bakımından köklü değişikliklere sebep olan üçüncü büyük atılım, 2018 yılının ilk yarısında yürürlüğe giren *General Data Protection Regulation* (GDPR) ile *Payment Services Directive 2* gelişmeleri olmuştur[35]. Söz konusu değişiklikler, yeni teknolojilerle birlikte doğal olarak Avrupa'daki ödeme sistemleri çerçevesini tamamen değiştirmiş; bu değişikliklerin bankacılık sistemine entegrasyonu ile nakit yönetiminin daha güvenli ve daha pratik hale getirmesi amaçlanmıştır.

1. Ödeme Hizmetleri Direktifi (2007/64/EC Payment Services Directive)

Avrupa Birliği'nin temel ilkelerinden biri olan ortak tek pazar yaratma amacıyla mal, hizmet, insan ve paranın birlik içerisinde serbest dolaşımının sağlanması ihtiyacı doğrultusunda Avrupa Birliği'nde ödeme sistemlerini tek bir ülke kadar hızlı, güvenli ve pratik olarak gerçekleştirme amacıyla entegrasyonu sağlamak üzere oluşturulan SEPA'nın hukuki altyapı sağlanması için Avrupa Birliği tarafından 13 Kasım 2007'de Ödeme Hizmetlerine İlişkin Avrupa Birliği Direktifi (Payment Services Directive) yürürlüğe konmuştur[36]. Ödeme Sistemlerini bütünleştirme politikasının ilk halkası olan PSD düzenlemesinin gerekçesinde direktifin amacının, SEPA kapsamında AB ülkeleri içinde ödeme sektöründeki oyuncuların oyun alanlarının belirlenmesi, rekabetin arttırılması ve kullanıcıların bu rekabetten faydalanması olarak belirtilmiştir[37].

Avrupa Birliği, PSD düzenlemesi ile inovasyon, rekabet, tüketicinin korunması gibi konuların yeknesaklaştırılmasını hedeflemiştir. Direktif'te üye ülkeler için bir geçiş süreci belirlenmiş olup, AB ülkeleri 1 Kasım 2009 tarihine kadar kendi mevzuatlarına bu Direktifle belirlenen ilkeleri yansıtma zorunluluğuna tabi tutulmuşlardır[38]. PSD düzenlemesinden

[32] Zetzsche ve diğerleri, 2019, s. 11. Avrupa Birliği'nde tek bir piyasanın oluşturulması ve tek para biriminin kabul edilmesi amacıyla kabul edilen Maastricht Antlaşması (1992) bu gelişmelerden birisidir.
[33] Zetzsche ve diğerleri, 2019, s. 11.
[34] Zetzsche ve diğerleri, 2019, s. 6.
[35] Strachan, D., Bonner, S., Bailey, S., Scott, A. ve Gallo, V. (2017). PSD2 and GDPR - friends or foes? *Deloitte Blog*.
[36] Gün, 2019, s. 11; Zetzsche ve diğerleri, 2019, s. 27; Meral, 2019, s. 25.
[37] Eren, 2019, s. 9; Mansfield-Devine, 2016, s. 9.
[38] Eren, 2019, s. 9.

yaklaşık altı sene sonra 27 Haziran 2013 tarihli Resmi Gazete ile ülkemiz mevzuatında yürürlüğe giren, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, içeriği itibari ile PSD'ye paralellik arz etmektedir[39].

2. Ödeme Hizmetleri Direktifi 2 (2015/2366/EC Payment Services Directive 2)

İlk direktifin başarısının ardından, finansal alanda elektronik ödemeler ve dijital bankacılık kapsamındaki yeniliklere karşı ortaya çıkan boşlukların doldurulması ve elektronik ödemeler için daha kolay, daha verimli, daha güvenli gerçekleşmesine imkân sağlayan bir altyapı sağlama amacıyla PSD düzenlemesini geliştirecek yeni bir direktife ihtiyaç duyulmuştur[40]. Bu amaçla Avrupa Komisyonu tarafından 8 Ekim 2015 tarihinde kabul edilen PSD2 Direktifi 12 Ocak 2016 tarihinde yürürlüğe girmiş ve üye ülkelere 13 Ocak 2018 tarihine kadar uyum sağlama yükümlülüğü getirilmiştir[41].

Avrupa'daki ödeme sistemlerini müşteri odaklı bir sistem haline çeviren PSD2, ilk direktifin kapsamını genişletmiş, AB dışındaki ödeme işlemlerini de kapsama dahil etmiş ve ödeme hizmetlerindeki gelişimlerin önünü açarak yeni kurum ve kavramlara yer vermiştir[42]. PSD2'nin bir diğer temel özelliği de ödeme işlemlerine ilişkin olarak teknik standartlar ve yeni güvenlik kriterleri getirmesidir. PSD2, Avrupa Birliği'nde ödemeler piyasasında FinTech'ler başta olmak üzere yeni nesil oyuncuların ve yeni hizmetlerin piyasaya entegrasyonunu hızlandırma amacı ile mobil ve online ödemelerdeki ödeme sistemlerindeki şeffaflığı ve rekabeti arttırma amacı gütmektedir[43].

PSD2'nin Türk hukukuna da sirayet eden önemli yeniliklerinden biri internet üzerinden yapılan ödemeler ve dijital bankacılık faaliyetleri sonucu şekillenen iki yeni ödeme hizmetinin tanımlanarak ödeme hizmeti kapsamının genişletilmesidir[44]. Detayları aşağıda açıklanacak bu iki yeni hizmet; müşterinin talebiyle başka bir ödeme hizmeti sağlayıcısında bulunan müşteri hesabına ilişkin ödeme başlatma hizmetleriyle (payment initiation services), müşterinin ödeme hizmeti sağlayıcılarında bulunan bir veya daha fazla ödeme hesabına ilişkin konsolide edilmiş bilgileri çevrimiçi platformlarda erişebilmesi hizmetleridir (account information services).

PSD2 ile ödeme sistemlerinde faaliyet gösteren kuruluşlar açık bankacılık uygulamalarına sistemlerini entegre etmekle yükümlü kılınmıştır[45]. PSD2'nın 36. maddesinde üye devletlerin ödeme kurumlarının kredi kuruluşlarının ödeme hesap hizmetlerine tarafsız,

---

39 Gün, 2019, s. 11; Gürses, 2019, s. 2.

40 Zetzsche ve diğerleri, 2019, s. 27; Remolina, 2019, s. 40; Meral, 2019, s. 25.

41 Bu iki yıllık uyum süreci Eylül 2019'a kadar uzatılmıştır. Mansfield-Devine, 2016, s. 11; Tsang, 2019, s. 358; Meral, 2019, s. 26.

42 Eren, 2019, s. 9; Zetzsche ve diğerleri, 2019, s. 28 - 31.

43 Zachariadis ve Ozcan, 2017, s. 4; Mansfield-Devine, 2016, s. 8, 9; JP Morgan, 2018 s. 1; PSD2 Avrupa'da ödeme sistemlerinin standardizasyonu maksadıyla tüketiciler için işlem ücretlerine sınırlamalar getirmektedir (Meral, 2019, s. 26). Bu durum 7192 sayılı Kanun'da TCMB'ye verilen yetki ile Türk hukukuna sirayet etmiştir.

44 Zetzsche ve diğerleri, 2019, s. 28; Türk hukukunda dijital bankacılık hizmetlerine ilişkin temel hukuki altyapı BDDK'nın 11 Temmuz 2014 tarih ve 29057 sayılı Resmi Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik ve 14 Haziran 2007 tarihli ve 26643 sayılı Resmî Gazete'de yayımlanan Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ hükümleridir ancak bu düzenlemelerde açık bankacılık altyapısını teşkil edecek bir hükme yer verilmemiştir.

45 Gün, 2019, s. 12; Brodsky ve Oakes, s. 1; Zachariadis ve Ozcan, 2017, s. 4; Remolina, 2019, s. 40.

ayrımcı olmayan ve orantılı olarak erişmesini sağlama yükümlülüğü altında olduğu düzenlenmiştir. Devamında üye devletlerce sağlanacak erişimin ödeme kurumlarının engelsiz ve etkili bir şekilde ödeme hizmetleri sunabilmelerini sağlayacak şekilde kapsamlı olması gerektiği öngörülmüştür. Kredi kuruluşlarının ödeme kurumlarının erişim talebini reddetmesi halinde yetkili makama reddetme sebepleri ile ilgili makul sebepler sunmakla yükümlü olduğu belirtilmiştir. Diğer yandan müşteri ile ödeme hizmeti sağlayıcısı arasındaki ilişkide, ödeme hizmeti sağlayıcısına müşterinin rızasını alma yükümlülüğü getirilmiştir[46].

PSD2'ye göre Avrupa Bankacılık Kurulu (EBA), Direktif'in uygulanmasına ilişkin olarak finansal kuruluşlara rehber çıkarma ve tavsiyeler vermekle sorumludur[47]. EBA tarafından hazırlanan taslak düzenlemeye dayanılarak Avrupa Birliği Komisyonu tarafından 27 Kasım 2017 tarihli ve 2018/389 sayılı Güçlü Müşteri Kimlik Doğrulaması için Düzenleyici Teknik Standartlar ve İletişimin Ortak ve Güvenli Açık Standartları (RTS-SCA) başlıklı yetki devrine dayanan tüzük[48] (*delegated regulation*) kabul edilmiş ve 14 Eylül 2019 itibariyle[49] yürürlüğe girmiştir.

D. TÜRK HUKUKUNDA AÇIK BANKACILIĞIN GELİŞİMİ

Türkiye'de ödeme sistemleri, 2013 yılında çıkarılan 6493 sayılı Kanun'un yürürlüğe girmesi ile ilk defa mevzuat anlamında kendine kanuni bir altyapı sağlamıştır[50]. Kasım 2019'da yürürlüğe giren 7192 sayılı Kanun ile 6493 sayılı Kanun'da ödeme sistemlerini büyük ölçüde etkileyecek nitelikte değişiklikler gerçekleştirilmiştir.

Yürürlükteki hukuk bakımından açık bankacılık sistemine ilişkin olarak beş düzenleme yer almaktadır. Bunlar; (i) 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkındaki Kanun (RG:27.06.2013), (ii) 7192 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (RG:22.11.2019), (iii) Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkındaki Yönetmelik (RG:27.06.2014), (iv) Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ (RG:27.06.2014), (v) Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (RG:15.03.2020) düzenlemeleridir[51]. Çalışmamız kapsamında anılan

---

46 Gürses, 2019, s. 2.

47 Remolina, 2019, s. 41.

48 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

49 Anılan düzenleme 14 Eylül 2019 tarihinden itibaren yürürlüktedir; ancak Avrupa Merkez Bankası'nın Ekim 2019 tarihli görüşüne göre üye ülkeler bu süreyi 31 Aralık 2020'ye erteleme imkânına sahiptir. Nitekim birçok ülkede 31 Aralık 2020'ye ertelenmiştir (Detaylar için kişisel verilerin güvenliğinin sağlanmasına ilişkin başlığa bkz).

50 6493 sayılı Kanun öncesi dönemde ödeme sistemlerine ilişkin konular BDDK tarafından çıkarılan düzenlemeler ile yürütülmüştür.

51 Yönetmelik ve Tebliğ hükümleri, 7192 sayılı Kanun ile 6493 sayılı Kanun'a uyarlılıklarını kısmen kaybetmişlerdir. Bu boşluğun aşılması için 7192 sayılı Kanun Geçici Madde 3'te BDDK'ya yapılan atıfların TCMB'ye yapılmış sayılacağı, BDDK düzenlemelerin yeni düzenlemeler yapılıncaya kadar uygulanmaya devam edeceği öngörülmüştür.

düzenlemelerden (i), (ii) ve (v) numaralı olanlar önemleri itibariyle ayrı bir başlık altında incelenecektir.

1. 6493 Sayılı Kanun

Ödeme ve menkul kıymet mutabakat sistemleri ve hizmetleri alanında taraflar arasındaki ilişkilerin ve bu ilişkilerde kullanılan terimlerin tanımının yasal bir düzenlemede yer alması sağlanarak mevzuat bütünlüğüne ulaşılması amacıyla[52] hazırlanan 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkındaki Kanun 27 Haziran 2013 tarihli Resmi Gazete'de yayımlanmıştır.

6493 sayılı Kanun, Avrupa Birliğinde yaşanan gelişmelere uyumlu olarak zaman içerisinde değişikliklere uğramıştır. Günümüzde bu Kanun, ödeme ve menkul kıymet mutabakat sistemleri, ödeme kuruluşları ve elektronik para kuruluşlarına ilişkin temel hükümler içeren kod kanun niteliğini sürdürmektedir[53].

Bu kanunda ödeme ve menkul kıymet mutabakat sistemleri açısından Türkiye Cumhuriyet Merkez Bankası (TCMB), ödeme kuruluşları ve elektronik para kuruluşları açısından ise Bankacılık Düzenleme ve Denetleme Kurulu[54] yetkili kılınmıştı. Kurul'un yetkileri, 7192 sayılı Kanun'un yürürlüğe girmesiyle TCMB'ye devredilmiştir.

2. 7192 sayılı Kanun

22 Kasım 2019 tarihli Resmi Gazete'de yayımlanan 7192 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, başta elektronik para hizmetleri olmak üzere ödeme sistemlerine önemli yenilikler getirmekte, Bankacılık Düzenleme ve Denetleme Kurulu'na 6493 sayılı Kanun ile tanınmış ödeme sistemleri ve elektronik para alanındaki düzenleyici ve denetleyici yetkileri TCMB'ye aktarmakta ve ödeme sistemleri konusunda Avrupa Birliği mevzuatı ile Türk hukuku arasında yeknesaklığı sağlama amacı taşımaktadır[55].

6493 sayılı Kanun'da, mehaz düzenlemeye uygun olarak açık bankacılık düzenlemesine yer verilmemekteydi[56]. 7192 sayılı Kanun'un 8. maddesi ile 6493 sayılı Kanun'un "*Ödeme Hizmeti*" başlıklı 12. maddesinin birinci fıkrasına *"Ödeme hizmeti kullanıcısının isteği üzerine başka bir ödeme hizmeti sağlayıcısında bulunan ödeme hesabıyla ilgili sunulan ödeme emri başlatma hizmetini,"* ile *"Ödeme hizmeti kullanıcısının onayının alınması koşuluyla, ödeme*

---

52 6493 sayılı Kanun'un Gerekçesinden.

53 Eren, 2019, s. 20.

54 BDDK'nın bu göreve binaen 27 Haziran 2014 tarihinden çıkardığı, Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik ve aynı tarihte çıkardığı Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliği geçerliliğini korumaktadır.

55 7192 sayılı Kanun ile 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun yanı sıra 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, 5411 sayılı Bankacılık Kanunu ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'da da değişiklikler yapılmıştır.

56 Gürses, 2019, s. 2; Türkiye'de bankacılık faaliyeti gerçekleştiren kurumlar bu açık bankacılık benzeri uygulamaları Ekran Kazıma "*Screen Scraper*" yöntemi ile yürütmekteydiler. Screen scraper uygulaması, ekranda yer alan görüntülerden veri toplama ve okunabilir bir metin yaratma mantığıyla hareket etmektedirler.

hizmeti kullanıcısının ödeme hizmeti sağlayıcıları nezdinde bulunan bir veya daha fazla ödeme hesabına ilişkin konsolide edilmiş bilgilerin çevrimiçi platformlarda sunulması hizmetini," ifadeleri eklenerek açık bankacılık uygulamalarına yasal altyapı kazandırılmıştır.

7192 sayılı Kanun'un 9. maddesi ile 6493 sayılı Kanun'a derç edilen 14/A maddesinde hesap bilgi hizmeti sağlayıcıları için bu Kanunda öngörülen pay senetlerinin nakit karşılığı çıkarılması, paylarının tamamının nama yazılı olması ve asgari sermaye yükümlülüğü şartlarının aranmayacağına yer verilmiştir.

PSD2'nın 36. maddesinde düzenlenen ve bankalara müşteri hesaplarına ilişkin bilgileri ödeme kuruluşları ile paylaşmalarına zorunluluğu getiren düzenlemeye 7192 sayılı Kanun'da yer verilmemiştir. Türkiye'deki genel ekonomik çerçevesinde bankaların ekonomik anlamda taşımak zorunda oldukları yük ve benzeri sebepler nedeniyle oluşan bu durumun, Türkiye'de açık bankacılık uygulamalarının etkinliğini azaltacak bir tesirinin olacağını söylemek mümkündür.

7192 sayılı Kanun'un yürürlüğe girmesinden önce müşterilere ödeme hizmeti sunan ve e-para ihracı faaliyetinde bulunan ödeme hizmeti sağlayıcılarla ilgili olarak Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) görevlendirilmişti. Bu dönemde TCMB yalnızca ödeme hizmeti sağlayıcılarının veya diğer finansal kuruluşların üye olarak birbirleri arasında işlem gerçekleştirecekleri ödeme sistemleri ve menkul kıymet mutabakat sistemleri ile ilgili yetkiye sahipti[57].

Bu ikili sistem, 7192 sayılı Kanun'la tek çatı altında toplanmış ve bu Kanun'la Bankacılık Düzenleme ve Denetleme Kurulu ve BDDK'ya ait elektronik para kuruluşlarının ve ödeme hizmetlerinin denetleme ve düzenleme yetkilerinin tamamı TCMB'ye devredilmiştir[58][59]. Yani 7192 sayılı Kanun'la değiştirilmiş 6493 sayılı Kanun, ödeme hizmetlerine ilişkin konularda yetkili otorite olarak açıkça TCMB'yi belirlemiştir (*bkz. m. 12/3, 12/4, 12/5, 12/6, 12/7, 14/5, 14/6*). Üçüncü taraf sağlayıcılar, faaliyetlerine başlamadan önce TCMB'den izin almakla yükümlüdür (m. *14/1, 15, 16, 17*). TCMB, bir ödeme hizmeti sağlayıcısındaki kişisel veriler dahil tüm verilerin, ödeme başlatma hizmeti ve hesap bilgi hizmeti kapsamında başka bir ödeme hizmeti sağlayıcısıyla paylaşılmasına ilişkin her türlü usul ve esası belirlemeye yetkilidir (*m. 14/A/2*).

TCMB tarafından yapılacak düzenlemelerde özellikle API'lerin standartlaştırılması[60], açık bankacılık işlemlerini yürütecek ödeme hizmeti sağlayıcıların bünyelerinde taşımaları gereken özellikler, her bankanın açık bankacılık sistemine katılıp katılamayacağı, sistem

---

57 Deniz**,** 2019, Procompliance.net

58 7192 sayılı Kanun'un Geçici Madde 3 hükmünün üçüncü fıkrasında TCMB tarafından çıkarılacak yönetmeliğin yayımı tarihinden itibaren bir yıl içerisinde ödeme başlatma hizmeti ve hesap bilgi hizmeti niteliğinde ödeme hizmeti sunan ödeme kuruluşlarının TCMB'den izin almak zorunda olduğunu belirtilmiştir.

59 1211 sayılı Türkiye Cumhuriyet Merkez Bankası Kanunu'nun "*Temel Görev ve Yetkiler*" başlıklı 4. maddesinin 3. fıkrasının (f) bendinde yer alan *"Türk Lirasının hacim ve tedavülünü düzenlemek, ödeme ve menkul kıymet transferi ve mutabakat sistemleri kurmak, kurulmuş ve kurulacak sistemlerin kesintisiz işlemesini ve gözetimini sağlamak ve gereken düzenlemeleri yapmak, ödemeler için elektronik ortam da dâhil olmak üzere kullanılacak yöntemleri ve araçları belirlemek,"* ifadesi ile TCMB'ye ödeme sistemleri konusunda geniş bir yetki altyapısı tanınmıştır. Bu yetki TCMB nezdinde Ödeme Sistemleri Genel Müdürlüğünce yürütülmektedir.

60 Türk hukukunda API'lerin ortak bir standart taşıması gerekliliği ve API özelliklerine ilişkin bir düzenlemeye henüz yer verilmemiştir.

denetiminin nasıl yapılacağı gibi konuların daha detaylı irdelenmesi gerektiğini belirtmek mümkündür[61].

3. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

7192 sayılı Kanun'la Türk hukukunda yer bulan açık bankacılık hizmetleri, ilk kez BDDK tarafından hazırlanan ve 15 Mart 2020 tarihli Resmi Gazete'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'le tanımlanmıştır. Buna göre açık bankacılık servisleri, bir elektronik bankacılık hizmeti olarak belirtilmiş (m. 3/1-l) ve *"Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalı"* şeklinde tanımlanmıştır (m. 3/1-a).

Yönetmelik, 1. maddesine göre Yönetmelik hükümleri yalnızca bankaları kapsamaktadır. Yönetmelik'teki açık bankacılığa ilişkin hükümlerin ödeme hizmeti sağlayıcısı sıfatıyla bankalar ve müşterileriyle olan ilişkileri açısından muteber olduğu konusunda bir tereddüt bulunmamaktadır. Ancak Yönetmelik, kanaatimizce ödeme hizmeti sağlayıcılarıyla üçüncü taraf sağlayıcılar arasındaki ilişkileri kapsamamaktadır. Zira aşağıda detaylarını belirteceğimiz üçüncü taraf sağlayıcılar ile ödeme hizmeti sağlayıcıları arasındaki ilişkilerde yetki, 6493 sayılı Kanun uyarınca TCMB'ye aittir. Öte yandan bankaların üçüncü taraf sağlayıcı sıfatıyla açık bankacılık hizmeti sunması durumunda, *ki teknik olarak bankaların 6493 sayılı Kanun'daki şartlar uyarınca bu sıfatla hareket etmesi mümkündür*, anılan Yönetmelik'teki düzenlemelere mi, yoksa TCMB'nin 6493 sayılı Kanun'un yetkilendirme rejimi uyarınca çıkaracağı düzenlemelere mi tabi olacağı hususunda belirsizlik bulunduğu da ifade edilmelidir.

Yönetmeliğin 34. maddesine göre müşteri bilgilerinin görüntülenmesi gibi finansal sonuç doğurmayan işlemler de dâhil olmak üzere tüm elektronik bankacılık hizmetleri için bankaların, müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması zorunlu kılınmıştır. Açık bankacılık servisleri bakımından bu zorunluluğa Yönetmeliğin 41. maddesinin ilk fıkrası ile istisna getirilmiştir.

Yönetmeliğin 41. maddesinin ikinci fıkrası ile açık bankacılık hizmetine ilişkin usul ve esasları belirleme yetkisi Bankacılık Düzenleme ve Denetleme Kurulu'na verilmiştir. Bu noktada 7192 sayılı Kanun'la değiştirilmiş 6493 sayılı Kanun'da açık bankacılık konusunda düzenleme yapmaya yetkili olarak açıkça TCMB'ye görev verilmesine karşın (*bkz. 7192 sayılı Kanun başlığı*) BDDK'nın 15 Mart 2020 tarihinde bu yönetmelik ile açık bankacılık konusunda bazı düzenlemelere yer vermiş olması eleştiriye muhtaçtır. BDDK'nın bu konuda bir düzenleme yapması ve hatta Yönetmeliğin 41. maddesinin ikinci fıkrasıyla kendini yetkili kılması, kanaatimizce hukuka aykırı niteliktedir. Yönetmeliğin kapsamına göre açık bankacılık bağlamında BDDK'nın yalnızca banka ile müşteri arasındaki ilişkilere yönelik düzenleme

[61] Gün, 2019, s. 18.

yapma yetkisinin bulunduğunu; buna karşılık üçüncü taraf sağlayıcılarla ödeme hizmeti sağlayıcılar arasındaki ilişkiler başta olmak üzere açık bankacılık hizmetleri konusunda yetkinin TCMB'ye ait olduğunu ifade etmek gerekir.

E. AÇIK BANKACILIĞA İLİŞKİN KAVRAMLARIN AVRUPA BİRLİĞİ VE TÜRK HUKUKU BAKIMINDAN KARŞILAŞTIRMALI İNCELEMESİ

Açık bankacılık sisteminde rol alan unsurlar arasında, yukarıda değinilen ödeme sistemi, ödeme hizmeti, ödeme hizmeti sağlayıcıları, hesap bilgi hizmetleri, ödeme başlatma hizmetleri, ödeme hizmeti kullanıcısı, tüketici/müşteri, API ve ödeme kuruluşu kavramları ön plana çıkmaktadır.

1. Ödeme Sistemi

Ödeme sistemleri; etkin, hızlı ve güvenli bir altyapı teşkil etmek suretiyle ticari hayatın vazgeçilmez bir öğesi olarak gerçekleştirilen işlem konusu el değiştirecek mal veya hizmet bedelinin alıcı tarafından satıcıya aktarılmasını sağlayan sistemlerdir[62]. PSD2'de ödeme sistemi, *"resmi ve standartlaştırılmış düzenlemelere ve ödeme işlemlerinin işlenmesi, silinmesi ve/veya çözümlenmesine ilişkin ortak kurallara sahip bir para transfer sistemi"* olarak tanımlanmıştır (PSD2 m. 4/7). 6493 sayılı Kanun'da ödeme sistemi üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapı olarak tanımlanmıştır (m. 3/1-v). Tanımlarından hareketle, PSD2'deki tanımın ödeme sistemini para sistemine özgülendiği görülürken, 6493 sayılı Kanun'un Elektronik Fon Transfer ve Elektronik Menkul Kıymet Transfer sistemlerini içine alacak şekilde daha geniş bir yaklaşımı barındırdığı dikkat çekmektedir[63].

2. Ödeme Hizmeti

PSD2'ye göre *"ödeme hizmeti*", Direktif'in ekinde yer alan ödeme hizmetleri listesinde yer verilen hizmetleri ifade eder. Ödeme başlatma hizmetleri ve hesap bilgi hizmetleri birer ödeme hizmeti olarak bu listede yer almışlardır.

Türk hukuku açısından değerlendirdiğimizde, 6493 sayılı Kanun'un 7192 sayılı Kanun ile değiştirilen 12. maddesinin birinci fıkrasında ödeme hizmeti türleri dokuz bent halinde sayılmıştır. Bu fıkranın (f) bendinde ödeme başlatma hizmeti, (g) bendinde hesap bilgi hizmetine ödeme hizmeti türleri arasında yer verilmiştir.

PSD2'de düzenlendiği şekliyle, 6493 sayılı Kanun'da da açık bankacılık ile ilgili hükümlerde her iki hizmet türü için de erişim sağlanacak hesap olarak "*ödeme hizmeti sağlayıcıları nezdindeki ödeme hesabı*" belirtilmiştir. Ödeme hesabı, Kanun'daki tanımı ile, ödeme hizmeti kullanıcısı adına açılan ve ödeme işleminin yürütülmesinde kullanılan hesabı ifade eder. Kanun'un 13.maddesinde ödeme hizmeti sağlayıcısı olarak belirlenen finansal

---

62 Eren, 2019, s. 12; Kirdaban**,** 2011, s. 5 - 6.

63 Avrupa Birliği menkul kıymet transferlerine ilişkin düzenlemelerini 2009/44/EC sayılı Direktif ile değişik 1998/26/EC sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Mutabakatın Nihailiği Direktifi ile yürütmektedir.

kuruluşlar bazında bu durumu ele aldığımızda, 5411 sayılı Kanun kapsamındaki Bankalar nezdindeki mevduat hesapları, Kanun'un m. 14/3 fıkrası kapsamında sadece ödeme işlemi için kullanılıyor olması şartıyla ödeme kuruluşu nezdinde bulunan ödeme hesapları, elektronik para kuruluşlarının bankalar nezdinde tuttukları hesaplar (m. 20/3) ve 6475 sayılı Posta Hizmeti Kanunu'nun 22. maddesi kapsamında ödeme kuruluşu niteliğini haiz Posta ve Telgraf Teşkilatı'nın nezdinde bulunan hesapların da açık bankacılığa konu olabileceği kanaatindeyiz.

3. Ödeme Hizmeti Kullanıcısı (Müşteri)

Bankacılık ekosisteminde müşteri olarak ifade edilen ve açık bankacılık hizmetinin yararlanıcısı konumundaki ödeme hizmeti kullanıcısı, PSD2'de ödeme yapan, ödeme alıcısı veya her ikisi için bir ödeme hizmeti kullanan gerçek veya tüzel kişiyi ifade eder (PSD2 m. 4/10). Direktifte tüketici, direktifin kapsadığı ödeme hizmeti sözleşmelerinde ticari, meslek veya meslek dışında başka amaçlar için hareket eden gerçek kişi olarak tanımlanmıştır. (PSD2 m. 4/20).

6493 sayılı Kanun'da ödeme hizmeti kullanıcısı, *"Gönderen, alıcı veya her ikisi sıfatıyla belirli bir ödeme hizmetinden faydalanan gerçek veya tüzel kişi"* olarak tanımlanmıştır (m. 3/1-ş). Ödeme hizmeti kullanıcısının 6502 sayılı Tüketicinin Korunması Hakkındaki Kanun kapsamında tüketici niteliği incelendiğinde, tüketici, 6502 sayılı Kanun'da *"Ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişi"* olarak tanımlanmıştır (m. 3/1-k). Bu tanımdan hareketle, tüketici ile ödeme hizmeti kullanıcısının kesişiminin belirli bir ödeme hizmetinden, ticari veya mesleki olmayan amaçlarla ödeme hizmetinden faydalanan gerçek veya tüzel kişi olarak belirlemek mümkündür[64]. Dolayısıyla bireysel müşterilerin açık bankacılık faaliyetlerinin tüketici hukukuna tabi olacağı söylenebilecektir. Ticari veya mesleki amaçlarla hareket eden gerçek veya tüzel kişi konumundaki ödeme hizmeti kullanıcıları ise açık bankacılık ilişkilerinden doğan uyuşmazlıklar bakımından tüketici hukukunun kapsamı dışında kalacaktır.

4. Ödeme Hizmeti Sağlayıcısı

PSD2'de açık bir tanıma yer verilmemekle birlikte, ödeme hizmeti sağlayıcısı olarak hizmet verebilecek finansal kurumlar gruplar halinde belirlenmiştir. Bu gruplar; ulusal hukuk ve birlik dışı kurallarda tanımlanan kredi kuruluşları, elektronik para kuruluşları, ulusal kanunlar tarafından ödeme hizmetleri sunma yetkisi tanınan posta ciro kuruluşları, ödeme kuruluşları, para otoritesi veya diğer kamu otoritesi sıfatıyla hareket etmedikleri zaman Avrupa Merkez

[64] 6502 sayılı Kanun'un 49. maddesinde ve Finansal Hizmetlere İlişkin Mesafeli İşlemler Yönetmeliği'nin 2. maddesinin 5. fıkrasında bankacılık işlemlerini mesafeli olarak yapılabileceği belirtilmiştir, Küçük, 2019, s. 1; Ticari amaç dışında bankacılık hizmetlerinden yararlanacak bireysel müşterilerin üçüncü taraf sağlayıcı ile girecekleri hukuki ilişkide bu hizmeti sağlayacak ve KVKK anlamında açık rızayı esas alan sözleşme ilişkisinde bir çerçeve sözleşme ilişkisine girecekleri şüphesizdir. Bu çerçeve sözleşmenin vekâlet sözleşmesi temelli olduğunu değerlendirilirse taraflar arasındaki ilişkinin tüketici hukuku kapsamında değerlendirilmesi önem taşımaktadır. Bu çerçeve sözleşmesi ilişkisinin günümüz şartlarında mesafeli bir sözleşme niteliği arz etmesi uygulamada sıklıkla karşılaşılacak bir konudur. Tüketici sıfatını haiz ödeme hizmeti kullanıcılarının 6502 sayılı Kanun'dan kaynaklanan hak ve yükümlülüklerine ile m. 49'da yer verilen finansal hizmetlere ilişkin mesafeli sözleşmeler incelemelerine bu çalışmada yer verilmeyecektir. Konu hakkında daha ayrıntılı bilgi için Bkz. Akipek, 2019, s. 11 vd.; Güneş, 2018.

Bankası (European Central Bank) ve ulusal merkez bankaları, kamu otoriteleri sıfatıyla hareket etmedikleri zaman Üye Devletler veya bunların bölgesel veya yerel makamlarıdır.

Benzer yaklaşımla 6493 sayılı Kanun'da da açık bir tanıma yer verilmemekte, Kanun'da belirtilen ödeme hizmetlerini sunan kurumlar ödeme hizmeti sağlayıcısı olarak kabul edilmektedir[65]. Buna göre (i) 5411 sayılı Kanun kapsamındaki bankalar, (ii) elektronik para kuruluşları[66], (iii) ödeme kuruluşları ve (iv) Posta ve Telgraf Teşkilatı Anonim Şirketi sınırlı sayıda belirtilen ödeme hizmeti sağlayıcılarıdır (m. 13). 13. maddenin ikinci fıkrasında ödeme hizmetini sunabilecek kişiler yukarıda zikredilen dört grup ile TCMB olarak sınırlandırılmıştır.

Her iki hukuk düzenlemesi açısından hem hesap bilgi hizmeti sağlayıcıları hem de ödeme başlatma hizmeti sağlayıcıları, ödeme hizmeti sağlayıcısı statüsündedir. Dikkat çekilmesi gereken önemli noktalardan biri hesap bilgi hizmeti sağlayıcıları ve ödeme başlatma hizmeti sağlayıcılarına ilişkin PSD2'nin 66 ve 67. maddelerinde yer verilen ayrıntılı düzenlemelere karşılık gelecek hükümlere henüz Türk hukukunda yer verilmemiş olmasıdır.

a) Hesap bilgi hizmeti sağlayıcısı

PSD2'ye göre hesap bilgi hizmeti kavramı, ödeme hizmeti kullanıcısı tarafından ya başka bir ödeme hizmeti sağlayıcısı ya da birden fazla ödeme hizmeti sağlayıcısı tarafından tutulan bir ya da daha fazla ödeme hesabıyla ilgili konsolide bilgi sağlayan çevrimiçi bir hizmet anlamına gelir (PSD2 m. 4/16).

Hesap bilgi hizmeti sağlayıcıları, müşterilere bankalar nezdinde bulunan hesap ve bakiye bilgisini sunan, müşterinin birden fazla banka ve ödeme hizmeti sağlayıcısı nezdinde bulunan hesaplarını konsolide ederek çevrimiçi sistemde hizmet sunan sağlayıcılardır[67]. PSD2'deki tanımı ile hesap bilgi hizmeti sağlayıcısı hesap bilgi hizmetleri çerçevesinde ticari faaliyetleri takip eden bir ödeme hizmeti sağlayıcısı anlamına gelir (PSD2 m. 4/19).

Hesap bilgi hizmeti sağlayıcıları, ödeme başlatma hizmeti sağlayıcılarından farklı olarak aktif bir eylem içerisinde yer almamaktadır. Sadece API'ler vasıtasıyla müşterilerin hesap bilgilerine ve bakiyelere erişim sağlamakta ve bunu müşteriye sunmaktadırlar[68].

Hesap bilgi hizmetine ilişkin esasları düzenleyen PSD2'nin 67. maddesinde kullanıcının açık izninin/rızasının varlığı ve işlemlerin güvenli ve etkin kanallar ile yapılmasına dikkat çekilmiştir. Bu madde ile AISP'lere yüklenen diğer yükümlülüklerden bazıları; hassas ödeme verilerini talep etmemek, yalnızca belirtilen hesapların verisini sağlamak ve kişisel verilerin

---

[65] 6493 sayılı Kanun'da Ödeme hizmeti sağlayıcılarının tanımı yapılmamaktadır. Açık bankacılık faaliyetlerine karşılık gelen hesap bilgi hizmetleri ve ödeme başlatma hizmetleri "*Ödeme Hizmeti*" başlıklı 12. maddede diğer ödeme hizmeti türleri ile birlikte yer almaktadır. Kanuna göre ödeme kuruluşları, ödeme hizmetlerini sağlamak ve gerçekleştirmek için yetkilendirilmiş tüzel kişileri ifade eder. Bu bağlamda TPP'lerin sadece ödeme kuruluşları olduğu çıkarımında bulunulabilir. Ancak Kanunun açık bankacılık hizmet türlerine yer verdiği 12. maddesinin yanı sıra *"Özellik Gösteren Ödeme Hizmetleri"* başlıklı yeni ihdas edilen 14/A maddesinde de açık bankacılık faaliyetlerini gerçekleştirebilecek kişilerin hem ödeme kuruluşları hem de ödeme hizmeti sağlayıcıları olabileceğine işaret eden hükümler yer almaktadır. Ödeme hizmeti sağlayıcıları Kanun hükmünde belirtildiği gibi ödeme kuruluşlarını da içine alan bir kavram olması itibariyle, TPP'leri genel anlamda ödeme hizmeti sağlayıcısı olarak değerlendirilmesinin doğru olacağı kanaatindeyiz.

[66] Elektronik Para Kuruluşları, 6493 sayılı Kanun'da "*Bu Kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişi"* olarak tanımlanmaktadır.

[67] Mansfield-Devine, 2016, s. 10; Meral, 2019, s. 27.

[68] Meral, 2019, s. 27.

korunması hükümlerine bağlılıktan kaynaklı yükümlülükleri yerine getirmektir. PSD2'nin m. 33/2 fıkrasına göre hesap bilgi hizmeti sağlayıcıları, kurulu oldukları ülkenin yetkili makamlarına başvuru yapmak (m. 5/1), hizmet sundukları alanları kapsayan profesyonel bir tazminat sigortası yaptırmak (m. 5/3), kurulu oldukları ülke kaydına sicil kaydı yaptırmak (m. 14) ve ödeme hesabı bilgisine yetkisiz, hileli erişimden kaynaklanan ödeme hizmeti sağlayıcısına veya ödeme hizmeti kullanıcısına hesap yükümlülüğüne karşı karşılaştırılabilir garanti sunma yükümlülüğü altındadır.

b) Ödeme başlatma hizmeti sağlayıcısı

Ödeme başlatma hizmeti sağlayıcıları, müşterinin talebi üzerine ödemeyi başlatan ve müşterilerin satın alma işlemlerinde müşterinin hesabının bulunduğu bankadan para transferini sağlayan hizmet sağlayıcılarıdır (PSD2 m. 4/18)[69].

Ödeme başlatma hizmeti, başka bir ödeme hizmeti sağlayıcısında tutulan bir ödeme hesabıyla ilgili olarak ödeme hizmeti kullanıcısının isteği üzerine bir ödeme emri başlatma hizmeti anlamına gelir (PSD2 m. 4/15). GDRP düzenlemesinin bir sonucu olarak üçüncü taraf sağlayıcıların veriye ulaşmak için öncelikle müşterilerinin onayını almaları gerektirmektedir.

PSD2'de ödeme başlatma hizmetlerine ilişkin önemli hususlar 66. maddede düzenlenmiştir. PSD2 kapsamında AB üyesi devletlere, ödeme hizmeti kullanıcılarının erişebileceği ödeme başlatma hizmeti sağlayıcılarının yararlanma hakkı sağlama yükümlülüğü yüklenmiştir. Bu yükümlülüğe istisna olarak ödeme hizmeti kullanıcısının çevrimiçi erişime sahip olmadığı durumlarda bu yükümlülüğün ortadan kalkacağı belirtilmiştir. Maddede yer alan önemli bir husus, ödeme hizmeti kullanıcısının isteğinin alınmasıdır. Ödeme başlatma hizmeti sağlayıcılarının uyması gereken yükümlülükler PSD2'de ayrıntılı olarak belirtilmiştir (m. 66/3-4).

Ödeme başlatma hizmeti için, ödeme başlatma hizmeti sağlayıcısının ödeme hizmeti kullanıcısının hesabına erişim yetkisinin bulunması gerektirmektedir. Bu durum ödeme başlatma hizmeti sağlayıcısının örtülü olarak hesap bilgi hizmetine de erişiminin bulunması zorunluluğunu doğuracaktır[70].

5. Ödeme Kuruluşu

PSD2'ye göre ödeme kuruluşu, Avrupa Birliği genelinde ödeme hizmetleri sağlamak ve yürütmek üzere Direktif'in 11. maddesi uyarınca verilen yetki uyarınca izin verilen bir tüzel kişiyi ifade etmektedir (m. 4/4). Türk hukukunda ödeme kuruluşu ise, TCMB'den izin almak kaydıyla[71], 6493 sayılı Kanun'un 14. maddesinde öngörülen şartları haiz ve ödeme hizmeti alanında faaliyet sağlamak üzere yetkilendirilen tüzel kişidir. Bu açıdan AB ve Türk hukukunun paralel düzenlemeler ihtiva ettiğini söylemek mümkündür.

---

69 Mansfield-Devine, 2016, s 10; Meral, 2019, s. 27.
70 PSD2, Giriş, 32. Par.
71 7192 sayılı Kanun'dan önce bu konudaki izin Bankacılık Düzenleme ve Denetleme Kurulu tarafından verilmekteydi.

6493 sayılı Kanun'da ödeme kuruluşlarının kuruluş şartları 5411 sayılı Kanun'da bankaların kuruluş şartlarına benzer şekilde ayrıntılı olarak düzenlenmektedir (m. 14/2). Kanuna göre ödeme kuruluşları kredi verme faaliyetinde bulunamaz (m. 14/4). Açık bankacılık faaliyetine özgü olarak 7192 sayılı Kanun ile 6493 sayılı Kanun'a eklenen 14/A maddesinin birinci fıkrasında hesap bilgi hizmeti sunan ödeme kuruluşları; kurulma şartları arasında bulunan pay senetlerini nakit karşılığı çıkarılma, pay senetlerinin tamamının nama yazılı olması ve asgari sermaye yükümlülüğünün aranması şartlarından istisna tutulmuştur. Bu istisna ile hesap bilgi hizmeti alanında ödeme kuruluşu kurmak isteyen girişimcilerin piyasaya girişi oldukça kolaylaştırılmıştır.

II. KİŞİSEL VERİLERİN KORUNMASI PENCERESİNDEN AÇIK BANKACILIK

Verinin parasallaşmasıyla gündeme gelen veri temelli ekonomi, onla temas halinde bulunan her sektörü dönüştürmeye devam etmektedir. İçinde bulunduğumuz algoritmalar çağında veri temelli ekonominin yeni bileşenlerinden birisi de inovasyon ve adil rekabeti amaçlayan açık bankacılık uygulamalarıdır[72]. Bir FinTech ürünü olan açık bankacılık uygulamaları, veri paylaşımı üzerine inşa edilmiştir[73]. Bu nedenle açık bankacılığın kişisel verilerin korunması penceresinden değerlendirilmesi bir zorunluluktur.

Açık bankacılık ve kişisel verilerin korunması arasındaki menfaat dengesi, kişilerin kişisel verilerinin korunması hakkı ile bu verilerin serbest dolaşımının sağlanması suretiyle oluşturulacak katma değerli ürün ve hizmetlere ilişkindir[74]. Açık bankacılık uygulamaları, kişisel verilerin korunmasına yönelik çeşitli riskler[75] de içermektedir. Veriye erişim arayüzlerinde ve veri aktarım protokollerindeki hatalar nedeniyle kullanıcı hesaplarına yetkisiz erişim sağlanması, veri sızıntıları nedeniyle bankaların ve üçüncü taraf sağlayıcıların itibarlarının azalması; bu risklere örnek olarak gösterilebilir. Anılan riskler, ancak gerekli hukuki, teknik ve idari tedbirlerin alınması halinde en aza indirilebilecek ve böylelikle açık bankacılığın avantajlı yönleri ön plana çıkarılabilecektir[76]. Nitekim Avrupa Birliği'nde bu tedbirlerin regüle edildiği GDPR ve PSD2 düzenlemelerinin ortak amaçlarının kullanıcıya verisi üzerinde hakimiyet sağlamak, kullanıcının veri güvenliğini sağlamak ve kullanıcıya veri taşınabilirliği imkânı sunmak olduğu ifade edilmektedir[77].

Çalışmamızın bu kısmında, açık bankacılık uygulamalarıyla kişisel verilerin korunması alanlarının kesişim kümesinde yer alan belirli hukuki problemlere ve değerlendirmelerimize yer

---

[72] Li, 2019, s. 36. Açık bankacılık uygulamaları, verilerin kişisel verilerin korunmasına uygun şekilde dolaşımını sağlayarak katma değerli hizmetlerin artmasına katkı sağlayacaktır (Zetzsche ve diğerleri, 2019, s. 23). Öte yandan açık bankacılık uygulamalarıyla birlikte ödeme hizmetleri sektörüne büyük teknoloji şirketlerinin de girebilecek olması, teknolojik, finansal ve uhdesinde bulundurdukları kişisel verilerden aldığı güçlerle onları bu alanı domine etmesiyle sonuçlanabilecektir. Dolayısıyla bu yönüyle açık bankacılığın rekabeti artırmaktan ziyade haksız rekabete yol açabilme ihtimali de bulunmaktadır (Zetzsche ve diğerleri, 2019, s. 32).

[73] Dijital bir ekonominin gelişmesi için en önemli şey güvenin tesis edilmesidir (Zetzsche ve diğerleri, 2019, s. 16). FinTech ürün ve hizmetleriyle kişisel verilerin korunmasının ortak amacı güveni tesis etmektir (Zunzunegui, s. 31)

[74] Leonard, 2017, s. 46.

[75] Bu risklerin temelinde, bankacılık müşterilerinin sektördeki aktörler tarafından işlenen geniş hacimli veriler bulunmaktadır (Keser, Kaya, Kınıkoğlu, Şahbaz, Alpaslan, ve Sökmen, 2014, s. 12)

[76] Brodsky ve Oakes, 2017, s. 3.

[77] Remolina, 2019, s. 36.

verilecektir. Bu kapsamda sırasıyla (i) açık bankacılığın veri taşınabilirliği hakkıyla ilişkisi; (ii) açık bankacılıkta veri sorumlusunun tespiti, (iii) işlenen verilerin niteliği bakımından kişisel veri, hassas veri ve müşteri sırrının ayrıştırılması, (iv) hesap bilgi hizmeti sağlayıcısı ve ödeme başlatma hizmeti sağlayıcısının istek ve onay alma yükümlülükleriyle, kişisel verilerin korunması penceresinden veri sorumlusunun aydınlatma ve açık rızaya başvurma yükümlülüklerinin karşılaştırılması, (v) kullanıcının kişisel verilerinin kanunlarda açıkça öngörülme veya sözleşme istisnalarına dayalı olarak işlenmesi, (vi) açık bankacılık uygulamalarında idari otoritelerin ve özellikle Türkiye Cumhuriyeti Merkez Bankası'nın rolü ve son olarak (vii) kişisel verilerin korunmasına yönelik gerekli teknik ve idari tedbirlerin alınması yükümlülüğü meseleleri incelenecektir. Meselenin daha kolay anlaşılabilmesi amacıyla, açık bankacılık ilişkisinin taraflarından biri olan ödeme hizmeti sağlayıcısı olarak bankalar üzerinden örneklemeler yapılmıştır.

A. AÇIK BANKACILIK BİR VERİ TAŞINABİLİRLİĞİ UYGULAMASI MIDIR?

Temellerini GDPR'den[78] alan veri taşınabilirliği hakkı (*data portability*), ilgili kişilere kişisel verilerinin bir veri sorumlusundan diğer bir veri sorumlusuna kolaylıkla taşınabilmesi imkânı sağlayan bir hakkı ifade eder[79]. GDPR m. 20/1'e göre ilgili kişiler, kendisiyle ilgili olarak bir veri sorumlusuna sağlamış olduğu verilerden, otomatik yollarla ve açık rıza ya da sözleşme istisnasına dayalı olarak işlenen kişisel verilerini, yapılandırılmış, yaygın bir şekilde kullanılan ve makinelerin okuyabileceği bir formatla alma hakkına sahiptir. Kişi bu verileri, hiçbir yerde kullanmamayı seçebileceği gibi dilerse hizmet almak amacıyla başka bir veri sorumlusuna da iletebilir. GDPR m. 20/2 uyarınca ayrıca ilgili kişiler, teknik imkânların elverişli olması halinde birinci fıkrada bahsedilen şartlarda, kişisel verilerinin doğrudan bir veri sorumlusundan diğer veri sorumlusuna aktarılmasını da talep edebilir[80]. GDPR m. 20/3'ten hareketle veri taşınabilirliği hakkının kullanılması, verileri ileten veri sorumlusu nezdinde kendiliğinden unutulma hakkının kullanılmasını sağlamayacağı gibi, verileri ileten veri sorumlusuyla ilgili kişi

[78] Veri taşınabilirliği hakkı, bugünkü bilinen kapsamıyla ilk kez 2012 yılında Filipin Veri Gizlilik Yasası'nda düzenlenmiştir. Ancak bu yasadaki düzenleme 2012 yılındaki GDPR tasarısının 18. madde hükmüne dayanmaktadır. *Li*'ye veri taşınabilirliği hakkı, dünyada yalnızca ABD Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası (HIPAA) kurallarıyla karşılaştırmalı olarak incelenebilir. Li, 2019, s. 64. Veri taşınabilirliği hakkının kaynağı hakim durumun kötüye kullanılmasıdır (Zetzsche ve diğerleri, 2019, s. 19).

[79] Bu hak Purtova'ya göre, Kıta Avrupasında kişisel verilerin korunmasına yeni bir soluk getiren Alman Federal Anayasa Mahkemesi'nin tanımladığı bireyin kişisel verilerinin geleceğini tayin hakkını mantıksal bir uzantısından ibarettir (Purtova, 2014, s. 15). Veri taşınabilirliği hakkı içerisinde, ilgili kişinin (i) veri sorumlusunun engellemesiyle karşılaşmaksızın kişisel verileri alma hakkını, (ii) aldığı bu verileri başka bir veri sorumlusuna iletme hakkını ve (iii) verilerin doğrudan başka bir veri sorumlusuna iletilme haklarını kapsayan bir çatı haktır (De Hert, Papakonstantinou, Malgieri, Beslay ve Sanchez, 2018, s. 197). Veri taşınabilirliği hakkı, kişinin verisi üzerindeki kontrolünü artırmakta ve ayrıca kişisel verilerin serbest dolaşmasına hizmet etmektedir (Li, 2019, s. 41).

[80] 20. maddenin temel amacının rekabet halindeki hizmet sağlayıcılar arasında bu hakkın kullanılmasını sağlamak olduğu ifade edilmektedir (Voigt ve Von dem Bussche, 2017, s. 175). Örneğin bir kişinin yalnızca görsel türündeki gönderilerin paylaşımı hizmeti sunan bir sosyal medya platformundan, benzer hizmet sunan başka bir sosyal medya platformuna gönderilerinin taşınması talebinde bu tarz bir rekabetin olduğu söylenebilir. Dolayısıyla teknik imkânlar (ör. API) bulunduğu sürece bu talebin GDPR m. 20/2 kapsamında karşılanması gerekir.

arasındaki akdi ilişkinin sonlanması sonucunu da doğurmaz[81]. GDPR m. 20/4'e göre veri taşınabilirliği hakkının kullanılmasının sınırını başkalarının hak ve özgürlükleri oluşturur[82].

İlgili kişinin veri sorumlusu bir banka hesabındaki işlem geçmişinin, yapılandırılmış CSV (*comma-seperated values*) formatında edinilerek yeni başka bir bankanın sistemine yüklenmesi, veri taşınabilirliği hakkının bankacılık sektöründeki uygulamasına örnek olarak gösterilebilir[83]. Bu noktada, kavramların doğru anlaşılmasına katkı sağlamak amacıyla, açık bankacılığın bir veri taşınabilirliği uygulamasından ibaret olup olmadığının incelenmesi gerekir. Sorunun cevaplanabilmesi için açık bankacılık uygulamalarıyla veri taşınabilirliği hakkının uygulanmasının benzer ve farklı yönleri üzerinde durulmasının faydalı olacağı kanaatindeyiz.

Her iki müessese de salt kişisel veri sahipliğine dayalı hakimiyeti ortadan kaldırarak inovatif hizmet esasına dayanan rekabetçi bir düzen oluşturulmasına hizmet eder[84]. Ancak veri taşınabilirliği hakkı, genel olarak kişinin bir hizmet sağlayıcıdan diğer bir hizmet sağlayıcıya geçişini kolaylaştırmak için kullanılırken[85], açık bankacılıkta müşterinin hizmet aldığı bankalarla olan ilişkisini sonlandırmak yerine bunlardaki kişisel verilerinin üçüncü taraflarla paylaşılarak onların ürettiği yeni ürün ve hizmetlerden faydalanma ve dolayısıyla bankaların sunduğu klasik bankacılık hizmetleriyle yeni FinTech hizmetlerini birlikte kullanma amacı bulunur.

Uygulanmaları açısından açık bankacılık ve veri taşınabilirliği hakkı birbirinden ayrışmaktadır. Her şeyden önce, veri taşınabilirliği hakkının talebin gerçekleştiği andan geçmişe dönük kişisel verilerin aktarılmasını hedeflediği ve bu nedenle talebin gerçekleştiği anda *donmuş-statik bir uygulama* olduğu; açık bankacılığın ise talep anından bağımsız olarak var olan ve oluşturulacak tüm kişisel verilerin anlık şekilde paylaşılmasını amaçladığı ve bu nedenle *dinamik bir uygulama* olduğu kanaatindeyiz. Bundan başka açık bankacılık uygulamalarında, bankalar ve FinTech şirketleri arasında çoğunlukla sözleşmeye dayalı veri paylaşımları yapılması öngörülürken; veri taşınabilirliği hakkı ise kullanıcıların salt bu hakkın kullanılmasına ilişkin aktif eylemlerine dayanmakta ve kural olarak akdi bir ilişki olmaksızın gerçekleşmektedir. Ancak GDPR m. 20/2 hükmü uyarınca doğrudan bir veri sorumlusundan diğer veri sorumlusuna yapılacak aktarımlarda da akdi ilişkinin gündeme gelebileceği gözden kaçırılmamalıdır.

Article 29 Working Party (A29WP)[86], veri taşınabilirliği hakkına ilişkin rehberinde, üye ülkelerce ya da Avrupa Birliği düzeyinde veri taşınabilirliği hakkının farklı formlarda kullanılabilmesinin öngörülebileceğini ifade etmiş; farklı formlara dayalı hakların kullanılması talebinin, GDPR kapsamında veri taşınabilirliği hakkının kullanılma talebi anlamına gelmediğini

---

81 Zira ileten veri sorumlusu, verileri iletmesinin ardından, işleme amaçlarıyla bağlantılı, sınırlı ve ölçülü ilkesi uyarınca verileri minimize etme yükümlülüğü doğmadıkça, hakimiyetindeki kişisel verileri silmemektedir (Voigt ve Von dem Bussche, 2017, s. 175).

82 A29WP'nin raporuna göre örneğin ilgili kişinin banka hesabındaki işlem geçmişindeki, üçüncü bir kişinin hesap sahibine bir miktar para aktardığı bilgisinin, başka bir bankaya aktarılması ve orada da aynı amaçlarla işlenmesinin üçüncü kişinin hak ve özgürlüklerine zarar verme ihtimali zayıftır (Article 29 Working Party, 2017, s. 21.)

83 Voigt ve Von dem Bussche, 2017, s. 177.

84 Zetzsche ve diğerleri, 2019, s. 25; De Hert ve diğerleri, 2018, s. 194; Voigt ve Von dem Bussche, 2017, s. 177.

85 Lambert, 2018, s. 231.

86 Kişisel verilerin korunmasıyla ilgili olarak ilgili GDPR hükümleri yürürlüğe girene dek görüş ve rehberler yayınlayarak uygulamaya yön veren ve 95/46 sayılı Direktif'le kurulmuş bağımsız nitelikli çalışma grubudur.

vurgulamıştır. A29WP'ye göre kişinin talebi, PSD2 kapsamında yalnız banka hesap geçmişinin hesap bilgi hizmeti sağlayıcısıyla paylaşılmasına yönelikse bu Direktifin hükümlerine öncelik tanınmalıdır. Öte yandan ilgili kişinin GDPR kapsamında bir veri taşıma talebinin bulunması durumunda, GDPR'nin diğer düzenlemelere göre öncelikli şekilde uygulanması gerekir[87].

İfade edilen farklı yönlerinden hareketle, açık bankacılığın veri taşınabilirliği hakkıyla birebir örtüştüğünü söylemek mümkün değildir[88]. Öte yandan ortak bir amaca hizmet etmeleri nedeniyle, açık bankacılık uygulamalarının veri taşınabilirliği hakkının gelişmiş ve dinamik şekilde uygulandığı alanlardan biri olduğunu söylemek de yanlış olmayacaktır[89]. Nitekim GDPR'de yer alan veri taşınabilirliği hakkının, açık bankacılık uygulamasının tarafı olan banka ve FinTech şirketleri için yükümlülük getirdiği şeklinde yorumlanması[90] da bu fikri destekler niteliktedir.

B. AÇIK BANKACILIK UYGULAMALARINDA VERİ SORUMLUSUNUN TESPİTİ VE ORTAK VERİ SORUMLUSU MESELESİ

Müşteri, nezdinde hesap tutulan ödeme hizmeti sağlayıcısı ve üçüncü taraf sağlayıcıdan müteşekkil üç tarafın bulunduğu açık bankacılık hizmetlerinde, kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan yükümlülüklerin kim tarafından yerine getirileceği, çözümlenmesi gereken bir meseledir. Bunun için ilişkideki veri sorumlularının ve bunların işleme faaliyetleri bakımından hakimiyet alanlarının tespiti gerekir. Çalışmamızda veri sorumlusunun tespitine ilişkin olarak *ödeme hizmeti kullanıcısının gerçek kişi olduğu* varsayımından hareket edilmiştir. Ödeme hizmeti kullanıcısının tüzel kişi olması ve örneğin çalışanlarına açık bankacılık hizmetlerinden faydalandırması durumunda hukuki ilişkinin boyutu değişeceğinden veri sorumlusunun tespiti konusunda da ek değerlendirmelere ihtiyaç duyulacağı şüphesizdir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) göre veri sorumlusu, kişisel verilerin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu[91] olan gerçek veya tüzel kişiyi ifade eder (*m. 3/ı*). Yani veri sorumlusu, kişisel verilerin işlenmesi konusunda, ne işlenecek, nasıl işlenecek, hangi hukuki sebebe dayanılarak işlenecek, hangi sürelerle işlenecek, kimler tarafından erişilebilecek, kimlere aktarılabilecek sorularının cevabını belirleyerek veri kayıt sisteminin temel değişkenlerini tespit eden gerçek veya tüzel kişiyi ifade eder[92]. İlgili kişilerin aydınlatılması, gerekli durumlarda açık rızalarına başvurulması, veri güvenliğinin temini ve veri sorumluları siciline kayıt gibi birçok kanuni yükümlülüğü bulunan veri sorumlusunun bu alandaki en önemli sorumluluk süjesi olduğu söylenebilir.

---

87 Article 29 Working Party, 2017, s. 8.

88 Zetzsche ve diğerleri, 2019, s. 32.

89 Açık bankacılıkla veri taşınabilirliği hakkının ortak yanlarının bulunduğu ve hatta açık bankacılığın inovatif ürün ve hizmetlerde veri taşınabilirliğinin etkisini azaltacağına ilişkin görüş için bkz. Remolina, 2019, s. 36.

90 Brodsky ve Oakes, 2017, s. 7.

91 Katıldığımız bir görüşe göre içerisinde sorumlu geçen bir kavramın yine sorumlu kelimesiyle tanımlanması isabetsizdir (Çekin, 2019, s. 51).

92 Taştan, 2017, s. 70; Article 29 Working Party, 2010, s. 15.

Türk hukuku açısından hem ödeme hizmeti sağlayıcıların hem de üçüncü taraf sağlayıcıların anonim şirket şeklinde örgütlenmesi gerekmektedir[93]. Dolayısıyla açık bankacılık uygulamalarının tarafı olan banka ve üçüncü taraf sağlayıcıların *tüzel kişi* olarak veri sorumlusu olacağı konusunda herhangi bir tereddüt bulunmamaktadır. Problem, hangi işleme faaliyetleri açısından kimin veri sorumlusu olacağı noktasında toplanmaktadır.

Veri sorumlusunun tespiti konusunda A29WP'nin dikkate alınması gereken yaklaşımları bulunmaktadır. Buna göre kişisel verilerin işleme amaç ve vasıtalarının "*belirleyen*" kişinin tespitinde; (i) hukuk kuralının açıkça yetkilendirmesi, (ii) hukukun zımni şekilde yetkilendirmesi, (iii) taraflar arasındaki sözleşme ilişkisi dahil olmak üzere olgusal etkilerin dikkate alınması olmak üzere üç farklı yaklaşım bulunmaktadır[94]. A29WP, üçüncü kategorideki olgusal etkilerin çok farklı şekilde yorumlamaya müsait olması nedeniyle uygulamada "*belirleyen*" kişinin tespitinde ilk iki yaklaşımın yüzde seksen oranında daha güvenli sonuçlar verdiği kanaatindedir[95]. Öte yandan açık bankacılık gibi karmaşık veri işleme durumlarında ise akdi ilişkilerin de dahil olduğu olgusal etkilerin dikkate alınması gerekir. Zira aynı verinin birden çok kişi tarafından işlendiği kompleks veri işleme faaliyetlerinde kurumlar, kendilerini veri sorumlusu olarak görmeme eğilimindedir[96].

Olgusal etkiler kapsamında taraflar arasında akdedilen sözleşme, doğrudan veri sorumlusunun kimliğine işaret etmeyebilir. Sözleşme kapsamında kişisel veri işleme faaliyetlerinden kimin sorumlu olacağına ilişkin zımni hükümler de veri sorumlusunun kimliğinin tespiti için yeterlidir. Ancak sözleşme hükümlerinin, her durumda veri sorumlusunun kimliğini tespit konusunda kesin sonuçlar vermeyeceğini belirtmek gerekir.[97] Sözleşme hükümlerinin yanı sıra, kişisel verilerin işlenmesi bakımından fiilen (*de facto*) yetkileri kimin kullandığı, bu konuda verisi işlenen ilgili kişiler nezdinde oluşan imaj ve buna bağlı olarak ilgili kişilerin makul beklentileri gibi kriterler de veri sorumlusunun tespitinde rol oynayacaktır[98].

Bu önbilgilerle açık bankacılık uygulamalarında veri sorumlusunun kimliğinin, gerçekleşen her bir kişisel veri işleme faaliyeti bakımından ayrı ayrı değerlendirilmesi kanaatindeyiz. Bu kapsamda *teorik* bağlamda öncelikle açık bankacılık uygulamalarındaki temel kişisel veri işleme faaliyetleri tespit edilecek ve ardından her bir işleme faaliyeti açısından, KVKK esas alınmak ve A29WP'nin görüşlerinden faydalanmak suretiyle veri sorumlusunun kimliği tespit edilmeye çalışılacaktır.

Açık bankacılık hizmetlerinde, üç temel işleme faaliyetinin bulunduğundan bahsedilebilir: **(1) Gerçek kişi müşterinin kişisel verilerinin bankacılık hizmetlerinin sunulması amacıyla banka tarafından işlenmesi**: Bu işleme faaliyeti, gerçek kişinin bankayla hukuki

---

93 Ödeme hizmeti sağlayıcılardan biri olan bankalar için bkz. 5411 sayılı Bankacılık Kanunu m. 7. Diğer ödeme hizmeti sağlayıcıların A.Ş. şeklinde örgütlenmesi gerektiği ise 6493 sayılı Kanun'daki hükümlerden çıkarılmaktadır.

94 A29WP'nin yaklaşımına destekleyici bir yaklaşım olarak *Çekin*, nimet külfet dengesine dikkat çekmekte ve kişisel veri işleme faaliyetlerinin nimetlerinden kim daha çok faydalanıyorsa, o derecede sorumlu olması gerektiğini ifade etmektedir (Çekin, 2019, s. 51).

95 Article 29 Working Party, 2010, s. 12.

96 Article 29 Working Party, 2010, s. 13.

97 Article 29 Working Party, 2010, s. 11.

98 Article 29 Working Party, 2010, s. 12.

ilişkisinin kurulmasıyla başlamakta olup müşterinin kimlik bilgilerinden, işlem güvenlik bilgilerine ve işlem geçmişine ilişkin çok çeşitli finansal ve diğer kişisel verileri içermektedir. **(2) Gerçek kişi müşterinin belirli kategorilerdeki kişisel verilerinin banka tarafından üçüncü taraf sağlayıcıya aktarımı ve bununla eş zamanlı olarak üçüncü taraf sağlayıcının bu verileri kendi veri kayıt sistemine kaydetmesi**: Bu işleme faaliyetinde banka örneğin API aracılığıyla kendi veri kayıt sisteminden üçüncü taraf sağlayıcıya gönderilmek üzere veri aktarımında bulunmaktadır. Üçüncü taraf sağlayıcı da bu API aracılığıyla verileri kendi veri kayıt sistemine çekmektedir. **(3) Gerçek kişi müşterinin kişisel verilerinin açık bankacılık ürün ve hizmetlerinden faydalandırılması amacıyla üçüncü taraf sağlayıcı tarafından işlenmesi**: Burada müşterinin API aracılığıyla üçüncü taraf sağlayıcıya aktarılan kişisel verileri, ürün ve hizmetlerin kendisine sunulması amacıyla işlenmektedir. Örneğin bir müşterinin birden çok bankada bulunan bakiye hesap ve işlem geçmişi bilgilerinin, müşteriye yatırım veya harcama tavsiyelerinde bulunması amacıyla üçüncü taraf sağlayıcı tarafından kendi özel algoritmalarıyla işlemesi halinde böyle bir durum söz konusudur.

Üç temel işleme faaliyetinin yanında her bir açık bankacılık hizmet türüne özgü işleme faaliyetleri de gündeme gelebilir. Örneğin ödeme emri başlatma hizmetlerinde, bir müşterinin isteği üzerine başlatılan ödemenin (*gerçek kişi*) alıcısına ait verilerin üçüncü taraf sağlayıcı tarafından işlenmesi halinde ayrı bir kişisel veri işleme faaliyetinden bahsedilir. Bu durumda üçüncü taraf sağlayıcı, alıcının verilerini, ödemenin gerçekleştirilmesi amacıyla ödeme hizmeti sağlayıcıya aktarmaktadır. Söz konusu faaliyet kapsamında işlenen veriler, Avrupa Veri Koruma Kurulu tarafından *sessiz kalan tarafın verileri* (silent party data) olarak adlandırılmıştır[99]. Açık bankacılık çatısı altında tanımlanan hizmet türleri genişledikçe buna benzer spesifik işleme süreçleri de doğacaktır. Ancak çalışmamızda, açık bankacılığın özünü oluşturması itibariyle yalnızca yukarıda ifade ettiğimiz üç temel işleme faaliyeti üzerinden hareket edilecektir.

Temel işleme faaliyetleri üzerinden yapılacak değerlendirmede (1) ve (3) numaralı işleme faaliyetleri bakımından herhangi bir problemle karşılaşılmayacaktır. Öyle ki, (1) numaralı faaliyet bakımından bankanın tek başına veri sorumlusu olduğu konusunda bir tereddüt bulunmamaktadır. Şüphesiz (3) numaralı işleme faaliyeti bakımından da veri sorumlusunun kimliği açıktır. Bu faaliyetler açısından veri sorumlusu, temel veri işleme parametrelerini belirleyen üçüncü taraf sağlayıcıdır. Buna karşılık (2) numaralı işleme faaliyetinin detaylı bir şekilde ele alınması gerekir. Bu faaliyet bakımından veri sorumlusunun kimliğini tespit noktasında, A29WP'nin de isabetle belirttiği üzere, öncelikle hukuk kurallarının doğrudan ya da dolaylı bir yetkilendirmesinin olup olmadığının belirlenmesi gerekir. Buradan bir sonuç alınamaması halinde, içerisinde akdi ilişkilerin de değerlendirildiği olgusal etkilerin dikkate alınması yerinde olacaktır.

Düzenleyici idari otorite sıfatıyla TCMB'nin bu konudaki müstakbel bir düzenlemesinde, açık bankacılık ilişkisindeki veri sorumlusu kimliğinin açıkça yahut zımnen tespitine yönelik bir hükmün bulunması durumunda (2) numaralı işleme faaliyeti bakımından herhangi bir

[99] European Data Protection Board, 2018, s. 2

problemle karşılaşılmayacaktır[100]. Ancak TCMB'nin konuyu regüle etmemesi halinde, kişisel veri işleme amaç ve vasıtalarının kim tarafından belirlendiğinin tespit edilerek veri sorumlusu sıfatının belirlenmesi gerekecektir. Kişisel verilerin aktarımının usul ve esaslarını belirleyen aktarım protokolünün (*örneğin API*) ve bu protokole bağlı veri kayıt sisteminin oluşturulması ve yönetilmesinin kim tarafından "*belirlendiği*", veri sorumlusu kimdir sorusunun da cevabını ortaya çıkaracaktır. Bu kapsamda taraflar arasındaki akdi ilişkinin hükümlerinin, akdi ilişki kapsamında fiili yetkileri kimin kullandığının, ilgili kişiler nezdinde oluşan imajın, ilgili kişilerin makul beklentilerinin ve diğer olgusal etkilerin dikkate alınması gerekir.

Veri sorumlusunun kimliği, sayılan değişkenlere bağlı olarak değişebilecek olmakla birlikte, taraflar arasında herhangi bir akdi ilişkinin bulunmaması halinde (2) numaralı işleme faaliyeti açısından kanaatimizce hem bankanın hem de üçüncü taraf sağlayıcının veri sorumlusu olması durumu söz konusudur. Bir başka deyişle (2) numaralı işleme faaliyeti bakımından, akdi ilişkiyle aksi kararlaştırılmadığı sürece, GDPR'nin isimlendirmesiyle *ortak veri sorumluluğu* söz konusudur. Nitekim A29WP de, örneğin bankayla finansal işlem ileten kişi arasında gerçekleşen kişisel veri işleme faaliyetlerinde hem banka hem de ileten kişinin o işleme faaliyeti açısından ortak veri sorumlusu (joint controller) niteliğini haiz olduğunu belirtmektedir[101]. Ortak veri sorumlusu, GDPR m. 26/1'e göre iki ya da daha fazla sayıda veri sorumlusunun işleme amaç ve vasıtalarını ortak bir şekilde belirlemesi durumunu ifade eder[102].

Ortak veri sorumluluğunun Türk hukukunda henüz düzenlenmemiş olması nedeniyle, bu durumlarda sorumluluk rejimi ancak akdi ilişkiler aracılığıyla düzenlenebilir. Taraflar KVKK'nın ve diğer kanunların emredici normlarına aykırı olmayan akdi hükümlerle, (2) numaralı işleme faaliyeti bakımından ortak veri sorumluluğu halini sürdürebilecekleri gibi, aralarından birini veri işleyen olarak da tayin edebilirler. İlk durumda banka ile üçüncü taraf sağlayıcı arasında bir kişisel veri işleme sözleşmesi yapılarak ortak veri sorumlularının hak ve yükümlülükleri düzenlenebilir[103]. İkinci durumda ise sözleşmeyle kişisel verilerin işleme amaç ve vasıtalarını belirleme yetkisi ve dolayısıyla veri sorumluluğu sıfatı da taraflardan birine bırakılabilir. Bu durumda taraflardan biri veri sorumlusu, diğer taraf ise veri işleyen sıfatını haiz olacak ve sorumluluk rejimi buna göre tayin edilecektir.

---

[100] Bankanın hakimiyet alanında bulunan kişisel veriler dahil tüm verilerin açık bankacılık hizmetleri kapsamında üçüncü taraf sağlayıcılarla paylaşılmasına ilişkin her türlü usul ve esası belirleme yetkisi TCMB'ye aittir (*6493 sayılı Kanun, m. 14/A/2*).

[101] Article 29 Working Party, 2010, s. 20. Bu durumlarda taraflar arasındaki sözleşme ilişkisi dahil olmak üzere olgusal etkilerin belirlemesi yaklaşımından hareketle sorumluluğa ilişkin belirsizliklerin ortadan kaldırılması gerekmektedir (Article 29 Working Party, 2010, s. 24).

[102] Ortak veri sorumlusu kavramı, veri sorumluları arasındaki sorumlulukların açık ve net bir şekilde ayrıştırılmasına hizmet etmektedir (*GDPR, 79. Giriş Paragrafı*). GDPR, m. 26'ya göre ortak veri sorumluları, GDPR'den kaynaklanan yükümlülüklerinin yerine getirilmesi amacıyla kendi sorumluluklarını şeffaf bir şekilde belirlemekle yükümlüdür. Bu yükümlülük, özellikle ilgili kişilerin haklarının kullandırılmasını ve kendilerine bu konuda gerekli bilgilendirmenin yapılmasını kapsar. Ortak veri sorumluları arasındaki sorumluluklar bir düzenlemeyle (örneğin sözleşme) ayrıştırılabilir. Düzenlemenin mahiyeti konusunda Avrupa Birliği'nin ve üye ülkelerin düzenleme yapma hakkı bulunmaktadır. Taraflar arasında yapılan sorumluluk paylaşımı, şeffaf bir şekilde ilgili kişilerin erişimine sunulmalıdır. Yapılan düzenleme çerçevesinde ortak veri sorumlularından biri, ilgili kişiler için irtibat noktası olarak belirlenebilir. Ancak ilgili kişiler GDPR'de yer alan haklarını, bu düzenlemenin şartlarını dikkate almaksızın her bir veri sorumlusuna başvuru hakkına sahiptir.

[103] Kişisel veri işleme sözleşmesi; veri sorumlusu ile veri sorumlusu, veri sorumlusu ile veri işleyen, veri işleyen ile alt veri işleyen arasında yapılan sözleşme türlerinin tamamını kapsayan karma nitelikli bir sözleşmedir (Taştan, 2017, s. 117 vd.).

C. AÇIK BANKACILIK KAPSAMINDA İŞLENEN VERİLERİN HUKUKİ NİTELİĞİ: KİŞİSEL VERİ Mİ, HASSAS VERİ Mİ, MÜŞTERİ SIRRI MI?

Açık bankacılık kapsamında işlenen veriler, kimliği belirli ya da belirlenebilir bir gerçek kişiye ilişkin olduğu sürece "*kişisel veri*" statüsündedir (*KVKK, m. 3/d*). Açık bankacılıkta işlenen verilerden kimlik doğrulama amacı başta olmak üzere müşteriye ait olan ve üçüncü kişilerce ele geçirilmesi halinde müşterinin ayırt edilebilme mekanizmalarının zarar göreceği veya dolandırıcılık yapılmasına imkân verebilecek nitelikteki veriler "*hassas veri*" statüsündedir (*Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, m. 3/o*)[104]. Öte yandan bankacılık faaliyetlerine özgü olarak bankalarla müşteriler arasında hukuki bir ilişki kurulmasından itibaren gerçek ve tüzel kişilere ait veriler, müşteri sırrı statüsünü kazanmaktadır (*5411 sayılı Kanun, m. 73/3*).

Türk hukukundaki normatif düzenlemelerde her üç statü açısından ayrı ayrı olmak üzere çeşitli yükümlülükler öngörülmüştür. Örneğin kişisel veri niteliğini haiz veriler bakımından veri sorumlusunun, KVKK uyarınca ilgili kişiyi aydınlatma, ilgili kişiye haklarını kullandırma, veri güvenliğini sağlama gibi çeşitli yükümlülükleri yerine getirmesi gerekir. Diğer yandan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik hükümleri uyarınca hassas verilerin aktarılmasında uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifreli şekilde saklanması gerekmektedir. Müşteri sırları açısından ise 5411 sayılı Kanun uyarınca ilgili kişinin müşterinin talep ya da talimatının alınması ve bunun belgelendirilmesi de birer yükümlülük mahiyetindedir. Bu kapsamda, üçlü bir ayrımla anılan statülerin kimler açısından bağlayıcı nitelikte olduğunun ve bu veri türlerinin birbirinden nasıl ayrıştırılacağı incelenecektir.

1. Kişisel Veri Niteliğindeki Veriler

İlk olarak hem bankalar hem de üçüncü taraf sağlayıcılar bakımından gerçek kişiyle ilgili belirli veya belirlenebilir nitelikteki tüm veriler, KVKK uyarınca kişisel veri niteliğindedir. Bankalar ve üçüncü taraf sağlayıcılar, bu kapsamda müşterilerin finansal verileri başta olmak üzere genel nitelikli birçok kişisel verisini işlemektedir. Müşterilerin işlem bilgisi, kimlik bilgisi, hizmet kullanım bilgisi, satın alma alışkanlık bilgisi, finansal hedef bilgisi, müsamaha gösterilen risk sınırı bilgisi, hesap bakiye bilgisi, hesap hareketleri ve ayrıca müşteri hakkındaki verilerden hareketle banka algoritmaları aracılığıyla oluşturulan katma değerli kişisel veriler işlenen verilere örnek olarak sayılabilir[105]. Açık bankacılık faaliyetlerinde iki bileşenli kimlik doğrulama sürecinde işlenen biyometrik veriler haricinde, genel olarak özel nitelikli kişisel verilerin işlenmesine rastlamak pek mümkün değildir[106].

---

[104] Hassas veri ibaresi ayrıca *Banka Kartları ve Kredi Kartları Hakkında Yönetmelik* (RG:10.03.2017-26458) hükümlerinde "*kartlara ilişkin hassas veri*" kavramı içerisinde kullanılmıştır.

[105] Tsang, 2019, s. 371 vd.; Remolina, 2019, s. 28.

[106] PSD2 kapsamında yürürlüğe konulan RTS-SCA'da müşterilerin kimliklerinin doğrulanması amacıyla biyometrik verilerin işlenebileceği düzenlenmiştir. Bununla benzer şekilde BDDK tarafından hazırlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğe göre de biyometrik veriler işlenebilecektir (*m. 34/1*). Bankacılık işlemlerinde işlenen biyometrik verilere ilişkin detaylı bilgi için bkz. Özcan, 2020, s. 83 vd.

Netice itibariyle açık bankacılık uygulamalarında kişisel veri niteliğini haiz tüm verilerin işlenmesi bakımından veri sorumlusu sıfatıyla hem bankaların hem de üçüncü taraf sağlayıcıların yükümlülüklerini yerine getirmesi gerekir.

2. Hassas Veri Niteliğindeki Veriler

Bankacılık sektöründeki çeşitli Türk ve AB Hukuku düzenlemelerinde[107], kişisel verilerin korunması ekosistemine yabancı olan "*hassas veri*" kavramına yer verilmektedir. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik hükümlerine göre hassas veri, kimlik doğrulama amacı başta olmak üzere müşteriye ait olan ve üçüncü kişilerce ele geçirilmesi halinde müşterinin ayırt edilebilme mekanizmalarının zarar göreceği veya dolandırıcılık yapılmasına imkân verebilecek nitelikteki verileri ifade eder (m. 3/o)[108]. Verilerin güvenlik sınıflarının tespitine etki eden hassas verilerin Yönetmelik uyarınca farklı güvenlik seviyesine sahip ortamlar arasında aktarımında uçtan uca güvenli iletişimin kullanılması ve şifreli şekilde saklanması esastır. Ayrıca bankanın personeline tahsis ettiği masaüstü, dizüstü ve mobil cihazların hassas veri içermesi halinde, bunların içeriğinin şifrelenmesi ve bu hususun teyidi için sunucu makinelerinin taranması gerekmektedir (m. 9/3).

Önemle vurgulamak gerekir ki, AB hukukunda olduğu gibi Türk hukukunda da *hassas veri* (*sensitive payment data*) kavramıyla KVKK'daki *özel nitelikli kişisel veri (special categories of personal data)* kavramı birbiriyle eş anlamlı nitelikte değildir[109]. Özel nitelikli kişisel veriler KVKK'da sınırlı sayı prensibine tabi olarak belirtilmiştir (m. 6). Buna karşılık hassas veri niteliğini haiz verilerin kategorik olarak sınırlandırılması mümkün değildir. Öyle ki hassas verinin içeriği, bankanın takdirine bağlı olarak teknolojik şartlara ve yapılan bankacılık işlemine göre değişebilecektir[110]. Dolayısıyla hassas veri kavramının, yalnızca bankacılık sektörü açısından daha riskli bir veri grubunu işaret ettiği; buna karşılık kural olarak özel nitelikli veri vasfı taşımadığının altının çizilmesi gerekir. İstisnaen hassas verinin, aynı zamanda özel nitelikli kişisel veri niteliği taşıması da mümkündür. Örneğin kişinin biyometrik veri niteliğindeki

---

[107] Türk hukukundaki düzenlemelere örnek olarak Banka Kartları ve Kredi Kartları Hakkında Yönetmelik (*RG:10.03.2017-26458*) ve Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (*RG:15.03.2020-31069*) gösterilebilir. AB hukukundaki düzenlemelere örnek olarak ise Ödeme Hizmetleri Direktifi 2 (PSD2) ve Güçlü Müşteri Kimlik Doğrulaması için Düzenleyici Teknik Standartlar ve İletişimin Ortak ve Güvenli Açık Standartları (RTS-SCA) düzenlemeleri örnek gösterilebilir.

[108] Açık bankacılığın orijin düzenlemesi olarak kabul edilebilecek Ödeme Hizmetleri Direktifi 2'ye göre (PSD2) hassas ödeme verisi "*kişisel güvenlik kimlik bilgileri de dahil olmak üzere sahtekarlık amacıyla kullanılabilecek veriler"* şeklinde tanımlanmıştır (PSD2, m. 4/32). Hassas ödeme verisi, Türk hukukunda Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine e Denetimine İlişkin Tebliğ'de (RG:27.06.2014-29043), "*kullanıcılar tarafından ödeme emrinin verilmesinde veya kullanıcı kimliğinin doğrulanmasında kullanılan, ele geçirilmesi veya değiştirilmesi halinde dolandırıcılık ya da kullanıcılar adına sahte işlem yapılmasına imkan verebilecek şifre, güvenlik sorusu, sertifika, şifreleme anahtarı ile PIN, kart numarası, son kullanma tarihi, CVV2, CVC2 kodu gibi kuruluşlar tarafından ihraç edilen ödeme araçlarına ilişkin kişisel güvenlik bilgileri*" şeklinde tanımlanmıştır (m. 3/j).

[109] Benzer şekilde AB hukukundaki bankacılık düzenlemelerinde kullanılan "*sensitive data*" ile kişisel verilerin korunması düzenlemelerindeki "*special categories of personal data*" birbiriyle eş anlamlı kavramlar değildir.

[110] AB hukukunda hangi verinin hassas veri olduğunun belirsiz olmasının ilgili düzenlemelere uyum konusunda risk oluşturduğu düşünülmekte; Birleşik Krallık'ta bu risklerin azaltılması amacıyla idari otoriteler tarafından PSD2 ile GDPR'nin öngördüğü yükümlülükler konusunda nasıl bir dengeleme yapılacağına yönelik olarak çalışmalar yapılmaktadır. Bkz. Strachan, D., Bonner, S., Bailey, S., Scott, A. ve Gallo, V. (2017). PSD2 and GDPR - friends or foes? Deloitte Blog.

parmak izi verisi, göz ya da yüze ilişkin örüntü bilgisinin kimlik doğrulama amacıyla kullanılması halinde hem *hassas veri*den hem de *özel nitelikli kişisel veri*den söz edilecektir.

Netice itibariyle, hassas veriler bakımından kural olarak genel nitelikli verilerin işlenme şartlarının dikkate alınması yeterlidir (*KVKK, m. 5*). Bir veri türünün banka tarafından hassas veri olarak nitelendirilmesi, o veriyi tek başına özel nitelikli kişisel veri haline getirmez. Bir hassas verinin, biyometrik veri örneğinde olduğu gibi, ancak Kanun'da, sınırlı sayı ilkesine tabi olarak sayılan özel nitelikli kişisel veri kategorilerinden birini de teşkil etmesi durumunda, o verinin hem özel nitelikli olduğundan hem de hassas veri olduğundan bahsedilebilir. Hassas verilere ilişkin yükümlülüklerin, yürürlükteki hukuka göre yalnızca bankalar tarafından yerine getirilmesi gerekmektedir. TCMB'nin 6493 sayılı Kanun uyarınca yapacağı düzenlemelerde üçüncü taraf sağlayıcılar açısından hassas verilere yönelik bir yükümlülük öngörülmedikçe üçüncü taraf sağlayıcılar açısından hassas verilere ilişkin bir yükümlülüğünün bulunmadığı kanaatindeyiz.

3. Müşteri Sırrı Niteliğindeki Veriler

Bankalar açısından müşterilerin verileri, kişisel veri olmasının yanı sıra aynı zamanda müşteri sırrı niteliğini de haiz olabilir. 5411 sayılı Bankacılık Kanunu'na göre bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, bankacılık faaliyetlerine özgü olarak müşteri sırrı haline gelmektedir (m. 73/3). Tanımından hareketle müşteri sırrı, yalnızca gerçek kişilere ilişkin olduğu sürece kişisel veri kümesiyle kesişmekte; tüzel kişilere ait müşteri sırları ise KVKK'nın kapsamına girmemektedir.[111]

7222 sayılı Kanun'la, 5411 sayılı Bankacılık Kanunu'nun müşteri sırrını düzenleyen 73. maddesinde incelenmeye değer nitelikte bir kural istisna dengesi kurulmuştur. Buna göre kural olarak müşteri sırrı niteliğini haiz veriler, müşterinin *açık rızası alınsa dahi*, ondan gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü taraflara aktarılamaz. İstisnaen söz konusu veriler, sır saklama yükümlülüklerinden ayrıksı tutulan hallerde[112], talep ya da talimatın varlığına bakılmaksızın yalnızca müşterilerin açık rızasıyla yurt içindeki ve yurt dışındaki üçüncü taraflara aktarılabilir.

İlk bakışta müşteriyi korumaya yönelik bir düzenleme gibi anlaşılsa da kanaatimizce anılan kural istisna dengesinin *de lege ferenda* açısından eleştirilmesi, mutlak bir gerekliliktir[113]. Yukarıda açıklandığı üzere gerçek kişiye ait müşteri sırları, aynı zamanda kişisel veri niteliğini de haizdir. Ancak düzenleme, KVKK'yla düzenlenen en önemli kurumlardan biri olan ve özgür iradeyle açıklanan açık rızayı adeta yok saymaktadır. Anılan düzenlemede kişinin KVKK'daki açık rıza gösterdiğine ilişkin irade açıklaması yok sayılmakla yetinilmemiş; kişisel verilerin üçüncü kişilere aktarımının kanuni sınırı, meçhul ve manaen fakir "*talep*" ve "*talimat*" kavramlarına bağlanmıştır. Öte yandan düzenlemedeki "*müşterinin açık rızası alınsa dahi*"

[111] Bankaların sır saklama yükümlülüklerinin istisnaları kapsamında veri aktarımına dair detaylı bilgi için bkz. Özcan, 2020, s. 117 vd. (7222 sayılı Kanun'dan önce yayımlanması nedeniyle bu eserde, Kanun öncesi duruma ilişkin detaylı bilgi yer almaktadır.)

[112] Bkz. 5411 sayılı Bankacılık Kanunu, m. 73/4

[113] Konuya ilişkin diğer eleştiriler için bkz. Dülger, M. V. ve Bakdur, M. (2020). 7222 Sayılı Kanun ile 5411 sayılı Bankacılık Kanunu'nda Yapılan Düzenlemenin KVK Hukuku Açısından Değerlendirilmesi, s. 4 vd.

ifadesinden ne anlaşılması gerektiği de muğlaktır. Bu ifadeyi içeren Bankacılık Kanunu m. 73/3, c. 4 hükmünden, müşteri sırrının yurt içi veya yurt dışına aktarımına ilişkin müşterinin açık rızası alınmamış olmasına rağmen, "*talep*" ya da "*talimatının*" bulunması halinde verilerin yurtdışına aktarılabileceği sonucu da çıkmaktadır. Böyle bir sonuç, Türkiye'nin 20 yıldır hazırlığını yaptığı, bir nev'i kanun ve yönetmelik düzeyindeki otuzdan fazla düzenlemeye can suyu veren ve kod kanun olarak kabul edilen KVKK'da öngörülen yurt içi ve yurt dışı aktarıma dair hükümlerin etkisiz kılınarak telafisi imkânsız zararların doğmasına yol açabilecek niteliktedir.

Bankacılık sektörüne özgü ihtiyaçların dikkate alınarak bu alana özgü düzenlemeler tesis edilmesinde bir sakınca yoktur; ancak hukukun bütünlüğüne zarar verecek düzenlemeler, paydaşlar bakımından hukuki güvenliği sarsma tehlikesi oluşturmaktadır. Kişisel verilerin korunması konusunda Türkiye'nin Amerika Birleşik Devletlerindeki *sektörel yamama* (*patchwork*) yaklaşımını değil, Avrupa Birliğindeki *bütüncül koruma* yaklaşımını esas aldığının göz önünde tutulması gerekir[114]. Bütüncül koruma ancak kişisel verilerin korunmasına ilişkin kod kanun kavram ve hükümlerine halel getirmeyecek düzenlemelerin yapılmasıyla mümkündür. Anılan gerekçeler uyarınca 5411 sayılı Bankacılık Kanunu'nda müşteri sırrına ilişkin düzenlemelerin ivedilikle gözden geçirilmesi kanaatindeyiz.

De lege lata bakımından incelendiğinde ise bankaların, müşteri sırrı niteliğindeki bilgilerin aktarımında, özel ve sonraki kanun olması nedeniyle 7222 sayılı Kanun'la değiştirilmiş 5411 sayılı Kanun'daki şartlara uyma yükümlülüğü bulunmaktadır. Yani bankalar, müşterilerinden açık rıza almış olsalar dahi müşteri sırrı niteliğindeki verilerin üçüncü taraf sağlayıcılara aktarımında, müşterilerden talep veya talimat almakla yükümlüdür.

D. AÇIK BANKACILIĞA DAİR İSTEK VE ONAY ALMA YÜKÜMLÜLÜKLERİYLE, KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN AYDINLATMA VE AÇIK RIZAYA BAŞVURMA YÜKÜMLÜLÜKLERİNİN KARŞILAŞTIRILMASI

Açık bankacılık hizmet tiplerinin (AIS ve PIS) kullanıcıya sunulması için Avrupa Birliği düzenlemeleriyle paralel şekilde bir yandan 6493 sayılı Kanun uyarınca kullanıcının istek veya onayı aranırken[115] (*m. 12/1-f ve g*), diğer yandan kişisel veri işleme faaliyetleri bakımından KVKK uyarınca kullanıcının aydınlatılması (*m. 10*) ve kural olarak onun açık rızasına başvurulması (*m. 5*) gerekir. Bu noktada problem; istek, onay ve açık rızaya ilişkin irade beyanlarının tek hukuki işlemle yerine getirilip getirilmeyeceği noktasında toplanmaktadır. Bir

[114] Capello, L. (2019, 13 Aralık). Surveillance is a fact of life, so make privacy a human right.

[115] İstek ve onay kavramları, mehaz düzenleme PSD2'de *istek* (*request of the payment service user*) ve *açık izin/rıza* (*payment service user's explicit consent*) olarak ifade edilmiştir. Ödeme başlatma hizmeti, PSD2 m. 4/15'e göre ancak ödeme hizmeti kullanıcısının isteği üzerine başlatılabilir. Hesap bilgi hizmeti ise PSD2 m. 67/2-a'ya göre, hesap bilgi hizmeti kullanıcısının açık izni/rızasıyla kendisine sunulabilir.
Avrupa Veri Koruma Kurulu'na göre PSD2'de ki açık rıza kavramıyla GDPR'deki açık rıza kavramı birbirinden farklıdır. Kurul'a göre PSD2'deki açık rıza, akdi bir rızayı ifade etmektedir. Kurul, PSD2'nin 87. giriş paragrafına dayanmak suretiyle ödeme hizmetlerinin her zaman kullanıcıyla ödeme hizmeti sağlayıcısı arasındaki akdi ilişki temeline dayalı olarak sunulduğunu ifade etmiştir (European Data Protection Board, 2018, s. 4).

başka deyişle örneğin açık rızanın alınmış olması, kullanıcının isteğinin ya da onayının alınmış olduğu şeklinde yorumlanabilir mi?

Öncelikle istek ve onaya ilişkin yükümlülüklerin, yalnızca üçüncü taraf sağlayıcılar bakımından gündeme gelebileceğini ifade etmemiz gerekir. Zira 6493 sayılı Kanun'da nezdinde hesap tutulan ödeme hizmeti sağlayıcıları, *örneğin bankalar*, açısından müşteriden istek ve onay almaya yönelik herhangi bir yükümlülük öngörülmemiştir. Bu ilişkide ödeme hizmeti sağlayıcısı sıfatıyla bankalar, açık bankacılık hizmetleriyle ilgili olarak yalnızca 5411 sayılı Bankacılık Kanunu ve KVKK'da öngörülen yükümlülüklerini yerine getirmekle yükümlüdür (*Detaylar için bkz. önceki başlık*). Dolayısıyla müşteri sırlarının yurtiçi ve yurtdışına aktarımına ilişkin olarak 5411 sayılı Kanun'da öngörülen "*talep*" ve "*talimat*" kavramlarıyla, hesap bilgi hizmetleri ve ödeme başlatma hizmetlerinin sunulmasına dair 6493 sayılı Kanun'da öngörülen "*istek*" ve "*onay*" kavramlarının birbirine karıştırılmaması gerekir.

Üçüncü taraf sağlayıcıların KVKK uyarınca, her durum ve şartta aydınlatma yükümlülüğünü (m. 10) yerine getirmesi gerekmektedir[116]. Kişisel verilerin işlenmesi için hukuki sebebin ne olacağı ise, *yani açık rızaya mı yoksa açık rızanın istisnalarına mı başvurulacağı*, üçüncü taraf sağlayıcılar tarafından sundukları ürün ve hizmetlere göre ayrıca değerlendirilmesi gereken hukuki bir risktir.

Üçüncü taraf sağlayıcı, aynı zamanda 6493 sayılı Kanun uyarınca, kullanıcının istek veya onayını almakla yükümlüdür. Kanun'a göre üçüncü taraf sağlayıcı, ödeme başlatma hizmetlerini ancak kullanıcının isteğiyle kendisine sunabilir (*m. 12/1-f*), hesap bilgi hizmetlerinde ise kullanıcının onayına başvurmakla (*m. 12/1-g*) yükümlüdür[117]. Hem istek hem de onay bakımından Kanun'da herhangi bir yöntem öngörülmemiş[118]; bu konu üçüncü taraf sağlayıcıların takdirine bırakılmıştır. Yurtdışı uygulamalarından hareketle üçüncü taraf sağlayıcıların, müşterilerin istek veya onaylarını almak amacıyla KVKK kapsamında hazırladıkları aydınlatma beyanlarının ya da açık rıza beyanlarının ayrı bir işlemle teyit edilmesi yoluna başvurabileceği kanaatindeyiz[119]. Aydınlatma ve açık rıza süreçlerinden ayrı bir işlem olması itibariyle, istek veya onay için yapılan kullanıcı işlemlerinin, veri tabanlarında ayrı bir tabloda tutulması ispat açısından önem arz etmektedir. Zira her ne kadar Kanunda ve ikincil düzenlemelerde buna ilişkin bir düzenleme olmasa da, 6493 sayılı Kanun ve uygulanmasına ilişkin Yönetmelik'in sistematiğinden hareketle istek ve onayın alındığına ilişkin ispat yükünün üçüncü taraf sağlayıcıda olduğu kanaatindeyiz.

Sonuç olarak 6493 sayılı Kanun'un 12/1-f ve g bentleri kapsamında müşteriden "*istek*" veya "*onay*" alma yükümlülükleri, yalnızca üçüncü taraf sağlayıcıları bağlar. Üçüncü taraf sağlayıcıların ayrıca KVKK kapsamında müşterileri aydınlatma ve kural olarak açık rızalarına

[116] Avrupa Birliği ve Türk hukuku açısından aydınlatma yükümlülüğünün karşılaştırmalı incelemesi için bkz. Aşıkoğlu, 2019, s. 42 vd.

[117] Avrupa Birliği Hukuku açısından değerlendirmesi için bkz. Vale, S. B. (2019, 4 Haziran). PSD2, GDPR and Banking Secrecy: What Role for Consent?

[118] PSD2'ye göre verilecek rıza/izin bakımından da herhangi bir şekil ve süreç öngörülmemiştir. Ayrıca PSD2 kapsamında verilen rıza, GDPR hükümlerinin aksine yalnızca belirli bir zaman dilimi içerisinde geri alınabilir (Vale, 2019, s. 2).

[119] Strachan, D., Bonner, S., Bailey, S., Scott, A. ve Gallo, V. (2017). PSD2 and GDPR - friends or foes? *Deloitte Blog*.

başvurma yükümlülükleri bulunmaktadır. Kanaatimizce üçüncü taraf sağlayıcılar nezdinde 6493 sayılı Kanun'da öngörülen istek ve onaya ilişkin yükümlülükler, yalnızca KVKK uyarınca aydınlatma yükümlülüğü ifa edilerek ya da açık rıza alınmak suretiyle yerine getirilmiş sayılmaz. Kanun koyucu, istek ve onay alma işleminin yöntemini üçüncü taraf sağlayıcıya bırakmış olmakla birlikte, kanaatimizce buna ilişkin irade beyanları aydınlatma beyanı ya da açık rıza beyanının kullanıcıya ayrıca teyit ettirilmek suretiyle alınabilecektir. Öte yandan 6493 sayılı Kanun uyarınca TCMB tarafından yapılacak bir düzenlemeyle bu hususun açıklığa kavuşturulması imkânı da bulunmaktadır.

E. AÇIK BANKACILIKTA KULLANICININ KİŞİSEL VERİLERİNİN KANUNLARDA AÇIKÇA ÖNGÖRÜLME VEYA SÖZLEŞME İSTİSNALARINA DAYALI OLARAK İŞLENMESİ

Açık bankacılık kullanıcılarının kişisel verileri, bu hizmeti sunan üçüncü taraf sağlayıcılar tarafından ancak KVKK uyarınca açık rızaya (m. 5/1) ya da açık rızanın istisnalarından birine (m. 5/2) dayanılarak işlenebilir. Unsurlarının eksiksiz bir biçimde var olduğu açık rıza beyanı açısından herhangi bir problemle karşılaşılmayacaktır[120]. Bununla birlikte açık bankacılık uygulamalarında açık rızanın istisnalarından yararlanılıp yararlanılamayacağının incelenmesi gerekir. Çalışmamızda yalnızca kanunlarda açıkça öngörülme (m. 5/2-a) ile sözleşme (m. 5/2-c) istisnalarına değinilecek olmakla birlikte diğer istisnai durumların da gündeme gelebileceğini ifade etmekte fayda vardır[121]. Örneğin Avrupa Veri Koruma Kurulu'na göre PSD2 kapsamında sessiz kalan tarafın verilerinin (silent party data) işlenmesi bakımından sınırlı durumlarda da olsa meşru menfaat istisnasına dahi dayanılabilir (detaylar için veri sorumlusunun tespitine ilişkin başlığa bakınız)[122].

KVKK, m. 5/2-a'da yer alan "*kanunlarda açıkça öngörülme*" istisnasının uygulama alanı bulabilmesi için kanun düzeyindeki bir düzenlemede, kişisel verilerin belirtilen durum ve şartlarla sınırlı olmak üzere kim tarafından işlenebileceğinin hüküm altına alınması gerekir. Üçüncü taraf sağlayıcılar, 6493 sayılı Kanun'a göre ödeme hizmeti sağlayıcılarından biri olarak kabul edilir (*m. 13/1-c*). Anılan kanunun 23. maddesinin ikinci fıkrasında ödeme hizmeti sağlayıcılarının kullanıcıların kişisel verilerini; ödeme usulsüzlüklerini önlemek, araştırmak ve ortaya çıkarmak amacıyla gerekli olan durumlarda işleyebileceği hüküm altına almıştır. Söz konusu hükümde sayılan durumlar açısından, üçüncü taraf sağlayıcıların KVKK m. 5/2-a'da belirtilen "*kanunlarda açıkça öngörülme*" istisnasına dayanarak işleme yapabileceği noktasında bir tereddüt bulunmamaktadır.

Tartışılması gereken bir başka husus, üçüncü taraf sağlayıcının, kullanıcının kişisel verilerini işlerken sözleşmenin kurulması veya ifasına ilişkin istisnaya dayanıp

---

[120] Açık rıza, belirli bir konuya ilişkin olmalı, bilgilendirmeye dayanmalı ve özgür iradeyle açıklanmış olmalıdır. Detaylar için bkz. Taştan, 2017, s. 157 vd.

[121] GDPR'ye göre açık bankacılık uygulamalarında kullanıcının kişisel verilerinin ödeme hizmet çerçeve sözleşmesi, kara para aklama düzenlemeleri veya 2002/58 sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif'in şartlarını taşımak şartıyla doğrudan ticari ileti gönderilmesi gibi durumlarda açık rızaya dayanmaksızın işlenebileceği hakkındaki görüş için bkz. (Vale, 2019, s. 3).

[122] European Data Protection Board, 2018, s. 3.

dayanamayacağıdır. KVKK, m. 5/2-c'ye göre sözleşmenin taraflarına ait kişisel verilerin işlenmesinin "*bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması*" ve gerekli olması durumunda[123], ilgili kişinin açık rızası aranmaz. Kanaatimizce, üçüncü taraf sağlayıcı, kişisel verilerin işlenmesine ilişkin genel ilkelere uymak suretiyle, hem açık bankacılık sözleşmesinin kurulması aşamasında hem de bu sözleşmenin ifası aşamasında açık rızaya başvurmaksızın kullanıcının kişisel verilerini işleyebilir. Nitekim Avrupa Veri Koruma Kurulu da üçüncü taraf sağlayıcıyla ödeme hizmeti kullanıcısı arasındaki sözleşmenin, gerekli şartların bulunması halinde GDPR m. 6/1-b'de belirtilmiş olan istisna kapsamında değerlendirilebileceği kanaatindedir[124]. Örneğin sözleşmenin kurulması aşamasında, ilk talebin kullanıcıdan gelmesi şartıyla[125] üçüncü taraf sağlayıcı, geliştirdiği açık bankacılık ürün ve hizmetlerin kullanıcının ihtiyaçlarını karşılayıp karşılamayacağını tespit etmek amacıyla gerekli olan kişisel verileri işleyebilir. Sözleşmenin ifası açısından da benzer şekilde, kullanıcıların kişisel verileri açık bankacılık ürün ya da hizmetinin sunulması amacıyla üçüncü taraf sağlayıcı tarafından işlenebilecektir.

F. AÇIK BANKACILIK UYGULAMALARINDA İDARİ OTORİTELERİN ve ÖZELLİKLE TÜRKİYE CUMHURİYET MERKEZ BANKASININ ROLÜ

Disiplinler arası bir alan olması itibariyle açık bankacılık, finansal otoritelerin yanı sıra tüketici, rekabet[126] ve kişisel verileri koruma otoritelerini de yakından ilgilendirmektedir[127]. Bu nedenle açık bankacılık uygulamalarında, idari otoritelerin birbiriyle uyum içerisinde ve yetki konusunda bir yarışa girmeksizin çalışması elzemdir[128]. Bundan başka, dijital ekonominin sınır ötesi niteliği dikkate alınarak açık bankacılık kuralları ve standartlar konusunda uluslararası iş birliğine de ihtiyaç vardır. Zira verinin parasallaşmasıyla birlikte açık bankacılık uygulamalarının da uluslararası platformlara taşınması uzak bir gelecekte değildir.[129]

7192 sayılı Kanun'un yürürlüğe girmesinden önce Bankacılık Düzenleme ve Denetleme Kurulu'nda bulunan yetkiler, bu kanunla TCMB'ye devredilmiştir (*Detaylar için bkz. 7192 sayılı Kanun başlığı*). TCMB'nin anılan yetkilerinden hareketle yapacağı düzenlemelerin kritik önemi haiz olduğunu belirtmekte fayda vardır. Yapılacak her düzenleyici işlemde, çalışmamızın konusunu oluşturan açık bankacılık hizmetlerinin disiplinler arası yapısı göz önünde bulundurulmalıdır. TCMB'nin bu noktada özellikle dikkat etmesi gereken ders niteliğinde iki kanunlaştırma süreci bulunmaktadır. Bu noktada özellikle yukarıda ifade ettiğimiz gibi sektörel yamama yaklaşımının değil; bütüncül hukuki koruma yaklaşımının tercih edilmesi gerektiği kanaatindeyiz. Bunun için iki kanunlaştırma sürecine dikkat çekmek gerekir. İlki 5411 sayılı Bankacılık Kanunu'na 7222 sayılı Kanun'la değişiklik getiren müşteri sırrına ilişkin düzenlemelerdir. Söz konusu değişiklikler kişisel verilerin korunmasına ilişkin kod kanunun

[123] Gereklilik kıstasıyla ilgili detaylı bilgi için bkz. Çekin, 2019, s. 93 vd.
[124] European Data Protection Board, 2018, s. 4.
[125] KVKK'da ilk talebin ilgili kişiden gelmiş olması şartı açıkça düzenlenmemiştir; ancak bu şart "*doğrudan doğruya ilgili olma*" ifadesinin bir gereği olarak ortaya çıkmaktadır (Yücedağ, 2017, s. 778).
[126] Nitekim Birleşik Krallık'ta meseleyi gündeme getiren Rekabet ve Piyasalar Kurumu (Competition and Markets Authority) kurumu idi. Bkz. *Açık Bankacılık Kavramı ve Doğuşu* başlığı.
[127] Basel Committee on Banking Supervision, 2019, s. 5.
[128] İşbirliği yapılmaması durumunda örneğin kişisel verilerin korunmasıyla bankacılık düzenlemeleri arasındaki fragmantasyonun derinleşme tehlikesi bulunmaktadır. Tsang, 2019, s. 368 vd.
[129] Remolina, 2019, s. 47.

sistematiğini dikkate almayarak hukuki bir belirsizliğe yol açmıştır (Detaylar için bkz. *Müşteri sırrı niteliğindeki veriler* başlığı). İkincisi ise Bankacılık Düzenleme ve Denetleme Kurumu tarafından hazırlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin 41/2. fıkra hükmüdür. Yukarıda ifade edildiği üzere 7192 sayılı Kanun'la bu konudaki tüm yetkiler TCMB'ye devredilmesine rağmen BDDK bu hükümle açık bankacılık hizmetlerinde kendisini yetkili kılmıştır (Detaylar için bkz. *Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik* başlığı). Benzer durumların yaşanmaması adına TCMB'nin KVKK'nın sistematiğini dikkate alarak ve bu kanun uyarınca Kişisel Verileri Koruma Kurulu'nun yetki alanını ihlal etmeyen düzenlemeler yapması ve kişisel verilere ilişkin düzenlemelerde KVKK'nın 22. maddesinin birinci fıkrasının (h) bendi uyarınca Kişisel Verileri Koruma Kurulu'nun görüşüne başvurması gerekir[130]. Kanaatimizce TCMB'nin konuya yönelik efektif ve disiplinler arası bakış açısı, hem kişisel veri sızıntılarının en aza indirilmesine hem de idari otorite fragmantasyonunun önlenmesine hizmet edecektir.

G. AÇIK BANKACILIK UYGULAMALARINDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK GEREKLİ TEKNİK VE İDARİ TEDBİRLERİN ALINMASI

KVKK'nın 12. maddesine göre veri sorumluları, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek ve muhafazalarını sağlamak amacıyla gerekli teknik ve idari tedbirleri almakla yükümlüdür. Kanun koyucu tarafından belirtilmeyen bu tedbirlere ilişkin olarak günün durum ve şartlarına uygun hareket etmek suretiyle veri sorumlularına yöntem bakımından takdir hakkı tanınmıştır.

Açık bankacılık ilişkisinin tarafı olan banka[131] ve diğer ödeme hizmeti sağlayıcıları da veri sorumlusu sıfatıyla KVKK'nın bu tedbirleri almakla yükümlüdür. Kanuni bir yükümlülük olmasının yanı sıra, önlemler aynı zamanda açık bankacılığın avantajlarının ön plana çıkmasına da hizmet edecektir[132]. Zira Avrupa'da PSD2 öncesinde uygulanan ekran kazıma (*screen scraping*) ve tersine mühendislik (*reverse engineering*) yöntemleri[133], güvenlik konusunda ciddi endişelerin oluşmasına sebep olmuştur[134]. Bu çerçevede öncelikle Avrupa Birliği hukukunda öngörülen tedbirlere ve ardından Türk hukukundaki mevcut duruma yer verilecektir.

Avrupa Birliğinde PSD2'yle hem kişisel verilerin korunmasına hem de açık bankacılık uygulamalarına dair güvenli bir ekosistem ihdas etmek amacıyla çeşitli tedbirler öngörülmüştür. Kişisel verilerin korunmasıyla ilgili olarak GDPR'ye atıf yapılarak ödeme sistemleri ve ödeme hizmeti sağlayıcılarının bu düzenlemeye uygun şekilde işlemede

---

130 Aksi durum, *Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*'te olduğu gibi yürütmeyi durdurma ve iptal gibi yaptırımların gündeme gelmesine sebep olabilir. Bkz. Danıştay 15. Daire'nin 2016/10500 E. sayılı ve 6.7.2017 tarihli kararı.

131 Açık bankacılık hizmetlerinden bağımsız olarak bankacılık sektöründeki veri güvenliği uygulamaları için bkz. Özcan, 2020, s. 171 vd.

132 Brodsky ve Oakes, 2017, s. 3.

133 Kavramların tanımı için bkz. Basel Committee on Banking Supervision, 2019, s. 19.

134 Öte yandan halen eski metodlara izin veren hukuk sistemlerinde açık bankacılık faaliyeti sunan şirketlerin maliyetleri azaltmak için halen bu yollara başvurduğu da bilinmektedir (Basel Committee on Banking Supervision, 2019, s. 17).

bulunması gerektiği hüküm altına alınmıştır (m. 94). Ödeme başlatma hizmeti sağlayıcılarının ve hesap bilgi hizmeti sağlayıcılarının; ödeme hizmeti kullanıcısının açık iznine tabi olarak sunmak ve açık izninin kapsamı dışındaki verilere erişmemek, ödeme hizmeti kullanıcısının kişisel güvenlik bilgileriyle ilgili gerekli güvenlik tedbirlerini almak, ödeme hizmeti sağlayıcılarıyla güvenli bir iletişimin teminini sağlamak (*secure communication*), ödeme hizmeti kullanıcısının hassas verilerini talep etmemek ve işlememek, ödeme hizmeti kullanıcısından hizmetin sunulması için gereğinden fazla veri talep etmemek, işlenen verileri başka bir amaçla kullanmamak konusunda Direktif'ten kaynaklanan çeşitli yükümlülükleri bulunmaktadır (m. 66 ve m. 67). Anılan yükümlülükler çerçevesinde ödeme hizmeti sağlayıcılar, ödeme hizmeti kullanıcılarının hesaplarına çevrimiçi erişiminde, uzaktan bir kanal vasıtasıyla yaptığı tüm işlemlerde ve elektronik olarak başlattığı ödeme işlemlerinde güçlü müşteri kimlik doğrulamasına (*strong customer authentication*) tabi kılınmıştır (m. 97/1). Anılan yükümlülükler hesap bilgi hizmeti sağlayıcıları ve ödeme başlatma hizmeti sağlayıcıları açısından da geçerlidir (m. 97/4). Ödeme hizmeti sağlayıcılar, ödeme hizmeti kullanıcılarının kişisel güvenlik kimlik bilgilerinin gizliliğini ve bütünlüğünü korumak için yeterli güvenlik önlemlerini almakla yükümlüdür (m. 97/3). Kullanıcıların elektronik olarak uzaktan başlattığı ödeme işlemlerinde ödeme hizmeti sağlayıcılar; işlemi, alıcı ve tutar bilgisine dinamik şekilde bağlamayı da içeren (*dynamic linking*) güçlü müşteri kimlik doğrulaması sürecini uygulamakla yükümlüdür (m. 97/2).

Anılan yükümlülüklerle ilgili teknik standartların oluşturulması amacıyla Avrupa Bankacılık Kurulu (EBA) yetkili kılınmıştır (m. 98/1). Ödeme hizmeti kullanıcılarının kişisel verilerinin korunması ve ödeme hizmeti sağlayıcıları arasında adil bir rekabetin tesis edilerek korunması dahil birçok amaçla yetkili kılınan Avrupa Bankacılık Kurulu taslak düzenlemeyi hazırlayarak Avrupa Birliği Komisyonu'na iletmiştir. Komisyon taslağa dayanarak 27 Kasım 2017 tarihli ve 2018/389 sayılı Güçlü Müşteri Kimlik Doğrulaması için Düzenleyici Teknik Standartlar ve İletişimin Ortak ve Güvenli Açık Standartları (RTS-SCA) başlıklı yetki devrine dayanan tüzüğü (*delegated regulation*) kabul etmiştir. Düzenleme, güçlü müşteri kimlik doğrulamasına, dinamik bağlantılamaya ve ödeme hizmeti sağlayıcılarla üçüncü taraf niteliğindeki hesap bilgi hizmeti sağlayıcıları ve ödeme başlatma hizmeti sağlayıcıları arasındaki güvenli iletişime dair teknik standartlar içermektedir.

Kişisel verilerin korunmasına da hizmet eden RTS-SCA yükümlülüklerinin temelinde güçlü müşteri kimlik doğrulaması yatmaktadır. Güçlü müşteri kimlik doğrulaması; (i) kullanıcının bilgisi, (ii) kullanıcının sahipliği ya da (iii) kullanıcının biyometrik özelliği olarak sınıflandırılmış ögelerden iki veya daha fazlasının kullanılmasına dayanan ve bu ögelerden birinin ihlalinin öteki ögelerin güvenilirliğini tehlikeye atmadığı ve böylelikle kimlik doğrulama verisinin gizliliğini korumak üzere tasarlanan doğrulamayı ifade etmektedir (PSD2, m. 4/30). Kimlik doğrulamada bu ögelerden en az ikisinin kullanılması şartı, doğrulamaya aynı zamanda çok faktörlü kimlik doğrulama niteliğini kazandırmaktadır[135]. Kullanıcının bilgisi için bir şifre, PIN kodu, soru cümlesi ya da örüntü; kullanıcının sahipliği için belirli bir SIM kart, mobil cihaz,

[135] Günümüzde büyük kart dağıtıcı şirketler (*Visa*, *Mastercard* ve *Amex*) tarafından sunulmaya başlanan 3D Secure 2.0 hizmetleri bu kapsamda RTS-SCA'nin gerekliliklerini çoğu zaman karşılamaktadır (Zhang, K. (2020, 2 Mart). The new standard for payment security is on its way with SCA.

giyilebilir cihaz, akıllı kart; kullanıcının biyometrik özelliği için parmak izi, yüz örüntüsü, ses örüntüsü, DNA imzası, iris şekline ilişkin bilgiler doğrulamadaki sınıflandırmalara örnek olarak gösterilebilir. Her bir öge için hangi güvenlik özelliklerinin bulunması gerektiği de RTS-SCA'da açıklanmıştır[136]. İstisnai durumlardan birine[137] girmediği sürece, tüm hizmet sağlayıcıları[138], güçlü müşteri kimlik doğrulamasına tabidir (RTS-SCA m. 4-9).

Ödeme hizmeti sağlayıcılarının, ödeme hizmeti kullanıcılarının kişisel güvenlik bilgilerinin gizliliğini ve bütünlüğünü koruma konusundaki yükümlülüğünün detaylarını içeren RTS-SCA, aynı zamanda doğrulama bilgilerinin korunmasına da hizmet eden hükümler ihtiva etmektedir. Buna göre, verilerin doğrulama sürecinde kısmi şekilde maskelenmesi, verilerin açık metin şeklinde saklanmaması, yetkisiz erişimden korunması, verilerin işlenmesinde güçlü ve yaygın şekilde tanınan sektör standartlarına uygun güvenli ortamların tercih edilmesi, gerekmesi halinde verilerin güvenli yollardan imhası ve etkisiz kılınmasına ilişkin cihaz ve yazılımların temini gibi tedbirlerin alınması gerekir (RTS-SCA m. 22-27).

RTS-SCA'da aynı zamanda ödeme hizmeti sağlayıcıları arasındaki iletişimin ortak ve güvenli standartlar üzerinden gerçekleştirilmesi amacıyla çok çeşitli yükümlülükler öngörülmektedir (RTS-SCA m. 28-36). Açık bankacılık uygulamalarında, API'lerin kullanılması gerekliliği de bu yükümlülüklerden doğmaktadır. Ödeme hizmeti sağlayıcıları, ödeme hizmeti kullanıcısı tarafından yapılan tüm işlemlerin geçmişe etkili olarak ve tüm yönleriyle takip edilebilir olmasını sağlamakla yükümlüdür (RTS-SCA m. 29)[139]. Bankalar ve kredi kuruluşları, hakimiyetlerinde bulundurdukları kişisel veriler dahil verileri, hesap bilgi hizmeti sağlayıcısı ve ödeme başlatma hizmeti sağlayıcılarla paylaşacakları arayüzler konusunda RTS-SCA m. 30 ila 36. maddelerdeki gereklilikleri karşılamak zorundadır. Paylaşım konusunda bankaların genel olarak iki seçeneğe sahip olduğu söylenebilir[140]. Bankalar, RTS-SCA m. 30 ve devamındaki şartları taşımak şartıyla API'lere başvurabilecekleri gibi, yine gerekli koşulları taşımak kaydıyla ekran kazıma[141] yöntemine de başvurabilirler. Bir API standardı öngörmeyen RTS-SCA, bu konuda banka ve kredi kuruluşları bakımından Avrupa ve dünyadaki standart düzenleyen kurumların standartlarına[142] uyum yükümlülüğü öngörmektedir. Anılan iki yoldan birini tercih eden bankaların her halükarda, iletişimi güvenli şekilde şifreleme yoluyla yapmaları, verilere erişim amacıyla yapılan oturumların güvenliğinin sağlanması, kişisel güvenlik kimlik bilgileriyle doğrulama kodlarının ödeme hizmeti sağlayıcısı personeli tarafından okunabilir formatta tutulmaması gibi önlemleri almakla yükümlüdür (RTS-SCA m. 35).

---

136 RTS-SCA; 6. Giriş paragrafı.

137 RTS-SCA m. 10 ila 18.

138 PSD2 m. 97.

139 Buna göre yapılan işlemlerin izlenebilmesi için her bir oturuma benzersiz bir tanımlayıcının atanması, log tutulması ve zaman damgasının bulunması gerekmektedir (RTS-SCA m. 29/2).

140 RTS-SCA, m. 30.

141 Yani RTS-SCA, ekran kazımayı tamamen yasaklamamakta, belirlenen koşulların yerine getirilmesi halinde bu yönteme müsaade etmeye devam etmektedir. Bankalar, beklenmeyen durumlar için API'lerin çalışmaması halinde, bahsi geçen ekran kazıma yöntemini aktif edebilirler (RTS-SCA m. 33).

142 Bu kapsamda bölgesel ve yerel API standardizasyon çalışmaları devam etmektedir (Basel Committee on Banking Supervision, 2019, s. 18). Örneğin Doğu Bloku Avrupa Ülkeleri (CEE) pazarlarında bulunan 350 banka, standardize edilmiş oluşturulan listeden (Open Banking API-Birleşik Krallık, Berlin Group-Almanya, STET-Fransa Polish API, Slovak API vb.) API'lerden birini seçerek düzenlemelere uyum sağlamaya çalışmaktadır (Remolina, 2019, s. 37).

RTS-SCA'da ayrıca, kişisel veriler dahil verilerin, taraflar arasında güvenli şekilde aktarılması için, ödeme hizmeti sağlayıcılarının 36. maddedeki yükümlülüklere uygun hareket etmesi gerekir. Buna göre tarafların ödeme hizmeti kullanıcılarının hassas verilerini paylaşmaması; kimlik doğrulama ya da verilerin paylaşılması aşamalarında beklenmeyen durum ve hataların meydana gelmesi halinde hesap bilgi hizmeti sağlayıcılarının ve ödeme başlatma hizmeti sağlayıcılarının banka ve kredi kartı kuruluşları tarafından bilgilendirilmesi; hesap bilgi hizmeti sağlayıcılarının kullanıcının rızası dışındaki bilgilere erişmeme konusunda gerekli tedbirleri alması; ödeme başlatma hizmeti sağlayıcılarının ödeme hizmeti kullanıcısının talebi üzerine doğrudan ödeme işleminin başlatıldığı durumlarda ondan aldığı bilgiyi aynı şekilde banka ve kredi kuruluşuna iletmesi gibi yükümlülüklere uyulması gerekir (RTS-SCA m. 36).

Türk hukukunda 6493 sayılı Kanun'un 14/A/2 madde hükmü uyarınca kişisel veriler dahil tüm verilerin, ödeme hizmeti sağlayıcısıyla üçüncü taraf sağlayıcı arasında paylaşılmasına ilişkin her türlü usul ve esası belirlemeye yetkili olan TCMB'nin yetkisinin kapsamına, güvenlik tedbirlerinin belirlemesinin de girdiği kanaatindeyiz. Yani hem ödeme hizmeti sağlayıcıları hem de üçüncü taraf sağlayıcılar açısından hangi güvenlik tedbirlerinin alınacağı konusunda yetki, TCMB'ye aittir. Ancak henüz açık bankacılık kapsamında işlenen kişisel verilerin muhafazasına dair TCMB tarafından bir düzenleme yapılmamıştır. BDDK tarafından çıkarılmış olan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te öngörülen güvenlik tedbirleri ise yalnızca bankalara yöneliktir. Buna göre bankalar, çalışmamızın konusuyla bağlantılı olarak açık bankacılık hizmetlerinde ödeme hizmeti sağlayıcısı sıfatıyla bu tedbirleri almakla yükümlüdür (*Detaylar için bkz. Yönetmelik başlığı*).

Açık bankacılık hizmetlerinde Avrupa Birliği Hukukundaki benzer tedbirlerin Türk hukukunda da öngörülmesi gerektiği konusunda bir tereddüt bulunmamaktadır. Bu kapsamda özellikle (i) kullanıcılar için çok faktörlü kimlik doğrulamasının öngörülmesi ve kişisel güvenlik bilgilerinin korunması amacıyla gerekli tedbirlerin belirlenmesi, (ii) açık bankacılık aktörleri arasındaki iletişimin ve veri paylaşımının güvenli şekilde temini için iletişim ve arayüz standartlarının belirlenmesi, (iii) böylelikle verilerin takibi ve paylaşılan verilerin sınırlandırılması hususları başta olmak üzere PSD2 ve RTS-SCA düzenlemeleri dikkate alınmalıdır. TCMB'nin bu düzenlemeleri esas alarak ve kanuni bir şart olması itibariyle (bkz. KVKK m. 22/h) Kişisel Verileri Koruma Kurulu'ndan görüş almak suretiyle gerekli düzenlemeleri yapması beklenmektedir. Ayrıca etkili tedbirler vasıtasıyla kullanıcıların korunması ile açık bankacılık sektöründe faaliyet gösterecek ödeme hizmeti sağlayıcıları bakımından doğacak maliyetler arasındaki dengenin gözetilmesi, açık bankacılığın Türkiye'de bir momentum yakalaması açısından önemlidir.

SONUÇ

İngiltere orjinli açık bankacılık uygulamaları, finansal teknolojilerin bankacılık ve ödeme sistemlerine yansıması noktasında yeni bir dönemi başlatmıştır. Her ne kadar şimdilik sadece hesap bilgi hizmeti ile ödeme başlatma hizmetinin ifade etse de, açık bankacılık sistemi, finans sektöründe dijitalleşmenin artması ve buna bağlı olarak verinin parasallaşması hareketlerini içeren genel bir süreç olarak değerlendirilmelidir. Bu sistemin anlaşılması için üzerine konumlandığı ödeme sistemleri evrenindeki ödeme hizmeti kullanıcısı, ödeme hizmeti sağlayıcısı ve üçüncü taraf sağlayıcıların iyi kavranması gerekmektedir. Nitekim açık bankacılık ilişkileri de bünyesinde bu aktörlerin bulunduğu üçlü sözleşme ilişkilerinden oluşmaktadır.

Ödeme sistemi evreninin Avrupa Birliği'nde PSD2 düzenlemesi ile getirilen düzenlemeler ile 6493 sayılı Kanun'a 7192 sayılı Kanun ile getirilen yeniliklerle paralellikler arz etmekte olup, düzenlemeler açısından arada önemli farklılıklar bulunmaktadır. Ülkemizde ödeme sistemlerine ilişkin yetkileri Bankacılık Düzenleme ve Denetleme Kurulu'ndan Türkiye Cumhuriyet Merkez Bankası'na geçişi ile düzenlemeler konusundaki eksikliklerin yakın gelecekte çıkarılacak düzenlemelere konu olacağını öngörmekteyiz.

Açık bankacılık, getirdiği faydaların dışında rekabet, tüketici hakları, bankacılık ve ödemeler sisteminde sektöründe paydaşların ve düzenleyici idari otoritelerin çokluğu nedeniyle mevzuat altyapısında ve uygulamada yoğun tartışmalara sebep olacaktır. Güncel bir eğilim olarak "*bankacılığın geleceği*" şeklinde isimlendirilen açık bankacılığın geleceğinin bu tartışmalar ışığında nasıl bir yol izleyeceği ise idari otoriteler ve paydaşlar arasındaki işbirliğine göre değişkenlik gösterebilecektir.

Çalışmamızın özünü teşkil eden kısımda, açık bankacılık uygulamalarının kişisel verilerin korunması ekosistemindeki karşılıkları ve muhtemel yedi temel problem üzerinden hareket edilmiştir. Meselenin anlaşılmasına katkı sağlaması adına incelenen ilk sorun, açık bankacılık uygulamalarının veri taşınabilirliği hakkının bir uygulanmasından ibaret olup olmadığına ilişkindir. Her ne kadar her iki müessese de inovatif hizmet esasına dayanan rekabetçi düzenin oluşturulması amacına hizmet etse de; kullanılma amaçlarındaki farklılık; verilerin paylaşımında kapsam yönünden veri taşınabirliği hakkının statik bir uygulamayken açık bankacılığın dinamik bir uygulamayı ifade ettiği; akdi temele dayanma açısından farklılık arz eden hususlar nedeniyle iki kavramın birbiriyle örtüştüğünü söylemek mümkün değildir.

İkinci problem açık bankacılık uygulamalarındaki kişisel veri işleme faaliyetlerinde veri sorumlusunun kim olduğuna dairdir. Veri sorumluluğu, işleme faaliyetine bağlı olarak

değişeceğinden açık bankacılık uygulamalarındaki temel veri işleme faaliyetlerinin belirlenmesi gerekir. Kanaatimizce açık bankacılık faaliyetlerinde; (1) gerçek kişi müşterinin kişisel verilerinin bankacılık hizmetlerinin sunulması amacıyla banka tarafından işlenmesi, (2) gerçek kişi müşterinin belirli kategorilerdeki kişisel verilerinin banka tarafından üçüncü taraf sağlayıcıya aktarımı ve bununla eş zamanlı olarak üçüncü taraf sağlayıcının bu verileri kendi veri kayıt sistemine kaydetmesi ve (3) gerçek kişi müşterinin kişisel verilerinin açık bankacılık ürün ve hizmetlerinden faydalandırılması amacıyla üçüncü taraf sağlayıcı tarafından işlenmesi şeklinde üçlü bir ayrıma tabi tutulmalıdır. (1) ve (3) numaralı işleme faaliyetleri bakımından sırasıyla banka ve üçüncü taraf sağlayıcıların veri sorumlusu olacağı konusunda herhangi bir tereddüt bulunmamaktadır. (2) numaralı işleme faaliyetinde ise taraflar arasında herhangi bir işleme faaliyetinin bulunmaması halinde ve TCMB tarafından aksine bir düzenleme yapılmadığı müddetçe, ortak veri sorumluluğu söz konusudur. Türk hukukunda henüz düzenlenmeyen bu durumda taraflar, kişisel veri işleme sözleşmesi aracılığıyla ortak veri sorumluluğu halini sürdürebilecekleri gibi, aralarından birini veri işleyen olarak da tayin edebilirler.

Üçüncü sorun açık bankacılık faaliyetlerinde işlenen verilerin niteliği bakımından kişisel veri, hassas veri ve müşteri sırrının nasıl ayrıştırılacağı ve hangi statünün ve bu statünün getirdiği yükümlülüklerin kimler açısından bağlayıcı olduğu hususundadır. Kişisel veriler açısından hem bankalar hem de üçüncü taraf sağlayıcılar veri sorumlusu sıfatıyla kendi hakimiyet alanlarındaki işleme faaliyetlerine ilişkin yükümlülüklerden sorumludur. Hassas veriler, KVKK kapsamında kural olarak özel nitelikli kişisel veriyi teşkil etmez. Ancak istisnaen hem hassas veri niteliğinde taşıyan hem de KVKK'da sayılan özel nitelikli kişisel veri kategorilerinden birine giren veriler bakımından her iki statü ve bu statünün yükümlülükleri geçerli olacaktır. Böyle bir durum olmadığı sürece hassas verilere ilişkin yükümlülüklerin muhatabı, yürürlükteki hukuka göre yalnızca bankalardır. Müşteri sırrı niteliğini haiz verilerden yalnızca gerçek kişilere ait olanlar KVKK kapsamında değerlendirilebilir. Bu kapsamda *de lege lata* bakımından müşteri sırrı statüsündeki verilerin, bankalar tarafından 5411 sayılı Bankacılık Kanunu'ndaki gerekli şartlar göz önüne alınarak işlenmesi gerekir. *De lege feranda* bakımından değerlendirildiğinde 5411 sayılı Bankacılık Kanunu'nun 73. maddesinde 7222 sayılı Kanun'la yapılan müşteri sırlarının aktarımına ilişkin değişikliğin; kişilerin KVKK kapsamındaki irade beyanlarını yok sayarak telafisi imkânsız zararlara yol açabilecek olması, hukuki bütünlüğe zarar vermesi ve Türkiye'yi meseleye ilişkin genel yaklaşımından saptırması sebepleriyle ivedilikle gözden geçirilmesi gerekmektedir.

Dördüncü problem istek, onay ve açık rızaya ilişkin yükümlülüklerin üçüncü taraf sağlayıcılar tarafından tek hukuki işlemle yerine getirilip getirilmeyeceği noktasında toplanmaktadır. Kanaatimizce üçüncü taraf sağlayıcılar nezdinde 6493 sayılı Kanun'da öngörülen istek ve onaya ilişkin yükümlülükler, yalnızca KVKK uyarınca aydınlatma yükümlülüğü ifa edilerek ya da açık rıza alınmak suretiyle yerine getirilmiş sayılmaz. İstek ve onaya ilişkin irade beyanları aydınlatma beyanı ya da açık rıza beyanının kullanıcıya ayrıca teyit ettirilmek suretiyle alınabileceği görüşündeyiz. Öte yandan 6493 sayılı Kanun uyarınca

TCMB tarafından yapılacak bir düzenlemeyle bu hususun açıklığa kavuşturulması imkânı da bulunmaktadır.

Beşinci sorun olarak açık bankacılık kapsamında işlenen verilerin, açık rızanın istisnalarından kanunlarda açıkça öngörülme ve sözleşmenin ifasıyla ilişkili işleme kapsamında değerlendirilip değerlendirilemeyeceği incelenmiştir. Kanun düzeyindeki normatif bir düzenlemede, kişisel verilerin belirtilen durum ve şartlarla sınırlı olmak üzere kim tarafından işlenebileceği hüküm altına alındığı sürece, üçüncü taraf sağlayıcılar ya da ödeme hizmeti sağlayıcıları kanunlarda açıkça öngörülme istisnasına dayanabilir. Öte yandan üçüncü taraf sağlayıcılar, kişisel verilerin işlenmesine ilişkin genel ilkelere uymak suretiyle, hem açık bankacılık sözleşmesinin kurulması aşamasında hem de bu sözleşmenin ifası aşamasında açık rızaya başvurmaksızın kullanıcının kişisel verilerini işleyebilecektir.

Altıncı problem olarak açık bankacılık uygulamalarında birden fazla idari otoritenin yetki alanında bulunması itibariyle idari otorite fragmantasyonu üzerinde durulmuştur. 7192 sayılı Kanun'un yürürlüğe girmesinden önce Bankacılık Düzenleme ve Denetleme Kurulu'nda bulunan yetkiler, bu kanunla TCMB'ye devredilmiştir. Dolayısıyla açık bankacılık uygulamalarında kişisel verilerin paylaşılmasına ilişkin düzenlemeler başta olmak üzere ilgili tüm düzenlemeleri yapma yetkisi TCMB'ye aittir. Bu yetkinin TCMB tarafından kanuni yükümlülükler gözetilerek etkili bir şekilde kullanımı, açık bankacılığın avantajlarını ön plana çıkaracak ve kişisel verilerin korunmasına ilişkin riskleri azaltacaktır.

Yedinci ve son problem olarak açık bankacılık ilişkilerinin tarafı olan ödeme hizmeti sağlayıcılarının veri sorumlusu olduğu işleme süreçleri bakımından gerekli teknik ve idari tedbirleri alma yükümlülüğü ele alınmıştır. Bu hususta Avrupa'da PSD2 ve RTS-SCA düzenlemeleriyle tüm ödeme hizmeti sağlayıcılar bakımından gerekli güvenlik tedbirleri Direktif ve Regülasyon düzeyinde belirlenmiştir. Türk hukukunda ise henüz ödeme hizmeti sağlayıcılarının tamamını kapsayacak bir düzenleme bulunmamaktadır. BDDK tarafından çıkarılan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin kapsamında yalnızca bankalar bulunmaktadır. Tüm ödeme hizmeti sağlayıcılar açısından güvenlik tedbirlerinin belirlenmesi yetkisi TCMB'ye aittir. Kanuni bir şart olması itibariyle Kişisel Verileri Koruma Kurulundan görüş almak suretiyle Avrupa Birliği uygulamasının takip edilerek etkili ve fakat sektöre lüzumundan fazla yük getirmeyecek güvenlik tedbirleri belirlenmesi, Türkiye'de açık bankacılık konusunda bir momentum yakalanmasını sağlayacaktır.

Netice itibariyle açık bankacılık uygulamalarının, yaptığı regülasyonlarla tüm dünya ülkelerini etkileyen Avrupa Birliğinde dahi (*Brüksel etkisi* olarak anılır) birçok risk ve belirsizliği beraberinde getirdiği açıktır. Düzenleyici idari otoritelerin birbirleriyle ve paydaşlarla yapacağı etkili iş birliği oranında bu risk ve belirsizlikler aşılacak ve açık bankacılık uygulamaları kişisel veriler bakımından bir tehdit olmaktan uzaklaşacaktır.

KAYNAKÇA

Article 29 Working Party. (2010). *Opinion 1/2010 on the concepts of "controller" and "processor"*.

Article 29 Working Party. (2017). *Guidelines on the right to data portability*.

Akipek Öcal, Ş. (2019). Finansal Hizmetlere İlişkin Mesafeli Sözleşmeler. İ. Y. Aktürk (Ed.), *Tüketici Hukukunun Güncel Sorunları Sempozyumu (20 Kasım 2018)* içinde. Ankara.

Aşıkoğlu, Ş. İ. (2019). Veri Sorumlularının Aydınlatma Yükümlülüğü - Avrupa Birliği ve Türk Hukukunda-. *Kişisel Verileri Koruma Dergisi*, *1*(2), 25.

Basel Committee on Banking Supervision. (2019). *Report on Open Banking and Application Programming Interfaces*. Basel Committee on Banking Supervision.

Bozkurt, T. (2017). Bankacılık Kanunu'nun 62. Maddesinin Hukukî Niteliği, Uygulama Alanı ve Mülkiyet ve Miras Hakkı Yönünden Anayasa'ya Aykırılığı Sorunu. *Ticaret ve Fikri Mülkiyet Hukuku Dergisi*, *3*(1), 23–46.

Brodsky, L. ve Oakes, L. (2017). Data sharing and open banking. McKinsey&Company.

Çekin, M. S. (2019). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu* (2. Baskı.). İstanbul: On İki Levha.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. ve Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193-203.

Eren, E. (2019). *Türk Hukukunda Merkezi Takas Kuruluşları, Merkezi Karşı Taraf Uygulaması ve Tezgâh Üstü Türev Araçların Merkezi Takası*. İstanbul: On İki Levha.

European Banking Authority. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06)*.

European Data Protection Board. (2018). *Letter regarding the PSD2 Directive*.

Gün, U. (2019). Bankacılık Hukukunda Yeni Kavram: Açık Bankacılık. *Finans Hukuku Gündemi Dergisi*, (2), 35–59.

Güneş, Z. N. (2018). *Finansal Hizmetlere İlişkin Mesafeli Sözleşmeler*. Ankara: Yetkin.

Gürses, D. (2019). Mevcut Türk Hukuk Düzeninde "Açık Bankacılık" Mümkün Müdür? *Finans Hukuku Gündemi Dergisi*, (2), 15–22.

Keser, L., Kaya, M. B., Kınıkoğlu, B., Şahbaz, U., Alpaslan, İ. B. ve Sökmen, A. (2014). *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*. İstanbul Bilgi Üniversitesi, TEPAV.

Kirdaban, M. İ. (2011). *Finansal Sistem İçerisinde Ödeme Sistemleri ve Hizmetleri: Türkiye Örneğinde Gözetim ve Avrupa Birliği Süreci*. (Yayımlanmamış doktora tezi). Gazi Üniversitesi.

Küçük, Y. (2019). Bankacılık Alanında Dijitalleşmenin Önündeki Tüketici Mevzuatı. *Finans Hukuku Gündemi Dergisi*, (2), 59–64.

Lambert, P. (2018). *Understanding the New European Data Protection Rules*. Boca Raton, FL: Auerbach.

Leonard, P. (2017). *Regulatory trends and emerging practices in access to customer data, portability and data sharing in the financial services sector (Paper for Banking & Financial Services Law Association Annual Conference)*. SSRN.

Li, W. (2019). *Data Portability as a New Means of Data Protection? Examining the Right to Data Portability in the EU General Data Protection Regulation*. (Yayımlanmamış doktora tezi). University of Edinburgh.

Mansfield-Devine, S. (2016). Open banking: Opportunity and danger. *Computer Fraud and Security*, (10), 8–13.

Meral, Y. (2019). Açık Bankacılığa Geçiş ve Avrupa Birliği Ödeme Hizmetleri Kurallarının (PSD 2) Rolü. *Bankacılar Dergisi*, (110), 25–37.

Milne, A. (2016). Competition Policy and the Financial Technology Revolution in Banking. *DigiWorld Economic Journal*, (103), 145–161.

Özcan, G. (2020). *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*. İstanbul: On İki Levha.

Purtova, N. (2014). Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table … and back on again? *Computer Law & Security Review*, *30*(1), 6-24.

Remolina, N. (2019, Ekim). Open Banking: Regulatory challenges for a new form of financial intermediation in a data-driven world (SMU Centre for AI & Data Governance Research Paper No. 2019/05). Elsevier BV.

Taştan, F. G. (2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması* (2. Baskı). İstanbul: On İki Levha.

Tsang, C.-Y. (2019). From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech. *University of Illinois Journal of Law, Technology & Policy*, *2019*(2), 355–404.

Usta, A. (2019). *Açık Bankacılık: Bankacılığın Geleceği*. Fintech İstanbul.

Voigt, P. ve Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Cham: Springer.

Yücedağ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, *LXXV*(2), 765-790.

Zachariadis, M. ve Ozcan, P. (2017). *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*.

Zetzsche, D. A., Arner, D. W., Buckley, R. P. ve Weber, R. H. (2019). *The Future of Data-Driven Finance and RegTech Lessons from EU Big Bang II*. University of New South Wales Law Research Series.

Zunzunegui, F. (2018). Digitalisation of Payment Services (Ibero-American Institute for Law and Finance Working Paper Series 5/2018,).

Elektronik Kaynaklar

Capello, L. (2019, 13 Aralık). Surveillance is a fact of life, so make privacy a human right. 8 Nisan 2020 tarihinde https://amp.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right adresinden erişildi.

CMA Resmi İnternet Sitesi. 8 Nisan 2020 tarihinde https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report adresinden erişildi.

Deniz, V. (2019, Aralık). Ödeme Hizmetleri, E-Para ve Açık Bankacılık Hakkındaki 7192 Sayılı Kanun ve Getirdikleri. *Procompliance.net*. 8 Nisan 2020 tarihinde https://www.procompliance.net/odeme-hizmetleri-e-para-ve-acik-bankacilik-hakkindaki-7192-sayili-kanun-ve-getirdikleri/ adresinden erişildi.

Dülger, M. V. ve Bakdur, M. (2020). 7222 Sayılı Kanun ile 5411 sayılı Bankacılık Kanunu'nda Yapılan Düzenlemenin KVK Hukuku Açısından Değerlendirilmesi. 8 Nisan 2020 tarihinde Academia.edu adresinden erişildi.

European Banking Authority. 8 Nisan 2020 tarihinde https://eba.europa.eu/ adresinden erişildi.

J.P.Morgan. (2018). Everything you need to know about APIs and the shift to Open Banking. *JP Morgan Treasury Services*. 8 Nisan 2020 tarihinde https://www.jpmorgan.com/global/treasury-services/open-banking adresinden erişildi.

Manthorpe, R. (2018,17 Nisan). What is Open Banking and PSD2? 8 Nisan 2020 tarihinde https://www.wired.co.uk/article/open-banking-cma-psd2-explained adresinden erişildi.

Open Banking Implematation Entity. 8 Nisan 2020 tarihinde https://standards.openbanking.org.uk/ adresinden erişildi.

Open Data Institute. 8 Nisan 2020 tarihinde https://theodi.org/adresinden erişildi.

ÖDED. (2017). Avrupa Birliği Ödeme Hizmeti Direktifi 2 Çevirisi. 8 Nisan 2020 tarihinde https://oded.com.tr/psd-2/ adresinden erişildi.

ProCompliance. (2018). Açık Bankacılık I. 8 Nisan 2020 tarihinde https://www.procompliance.net/acik-bankacilik-i/ adresinden erişildi.

ProCompliance. Açık Bankacılık II - Dünya Uygulamaları. 8 Nisan 2020 tarihinde https://www.procompliance.net/acik-bankacilik-ii-dunya-uygulamalari/ adresinden erişildi.

Strachan, D., Bonner, S., Bailey, S., Scott, A. ve Gallo, V. (2017). PSD2 and GDPR - friends or foes? *Deloitte Blog*. 8 Nisan 2020 tarihinde https://blogs.deloitte.co.uk/financialservices/2017/08/psd2-and-gdpr-friends-or-foes.html adresinden erişildi.

Vale, S. B. (2019, 4 Haziran). PSD2, GDPR and Banking Secrecy: What Role for Consent? 8 Nisan 2020 tarihinde https://www.lexology.com/library/detail.aspx?g=09534fc1-7f28-46c6-a7cb-20574fefe9de adresinden erişildi.

Zhang, K. (2020, 2 Mart). The new standard for payment security is on its way with SCA. 8 Nisan 2020 tarihinde https://www.lexology.com/library/detail.aspx?g=6ed70be9-e430-4de6-b07f-cf01bb1180b1 adresinden erişildi.

Pymnts. Deep Dive: What Does Open Banking Mean For Turkish Banks? 8 Nisan 2020 tarihinde https://www.pymnts.com/news/regulation/2020/deep-dive-what-does-open-banking-mean-for-turkish-banks/ adresinden erişildi.

KISALTMALAR

A29WP	Article 29 Working Party
AB	Avrupa Birliği
AISP	Account Information Service Providers (Hesap Bilgi Hizmeti Sağlayıcıları)
API	Application Programming Interface (Uygulama Programlama Arayüzü)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
GDPR	European Union General Data Protection Regulation (Avrupa Birliği Genel Veri Koruma Tüzüğü)
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
OBWG	Open Banking Working Group (Açık Bankacılık Çalışma Grubu)
par.	Paragraf
PISP	Payment Initiation Service Providers (Ödeme Başlatma Hizmeti Sağlayıcıları)
PSD	2007/64/EC Payment Services Directive (Ödeme Hizmetleri Direktifi)
PSD2	2015/2366/EC Payment Services Directive 2 (Ödeme Hizmetleri Direktifi 2)
RG	Resmî Gazete
RTS-SCA	Commission Delegated Regulation EU/2018/389 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Güçlü Müşteri Kimlik Doğrulaması için Düzenleyici Teknik Standartlar ve İletişimin Ortak ve Güvenli Açık Standartlarına Dair Tüzük)
SEPA	Single Euro Payments Area (Avrupa Tek Ödeme Alanı)
TBK	6098 sayılı Türk Borçlar Kanunu
TCMB	Türkiye Cumhuriyet Merkez Bankası
TPP	Third Party Provider (Üçüncü Taraf Sağlayıcı)