Araştırma Makalesi / Research Article

Açık Bankacılığa Geçiş ve Avrupa Birliği Ödeme Hizmetleri Kurallarının (PSD2) Rolü

Dr. Öğr. Üyesi Yurdagül Meral*

Öz

Avrupa Birliği, Eylül 2019'da ödeme sistemleri ile ilgili yeni kuralları uygulamaya başlayacaktır. İkinci Ödeme Hizmetleri (PSD2) yönergesi gereği, 'açık bankacılığa geçiş'in ilk adımını, bankaların, müşteri verileri/hesap bilgileri ve alt yapılarını üçüncü taraflara erişilebilir hale getirmeleri zorunluluğu oluşturmaktadır. İlgili kurallar Avrupa Birliği ve diğer ülkeler arasındaki ödemeleri de kapsamaktadır. Bu araştırmanın amacı, yeni kuralların uygulamasının getirdiği avantajlar, riskler ve olası sonuçlarını araştırmaktır. Literatür taraması sonucunda, Avrupa Birliği ile ödeme ilişkisi olan diğer ülkelerinde olası riskler için önlemler, yerel mevzuat güncellemesi, özellikle bankaların müşteri veri ve hesap bilgilerini ödeme hizmetleri kurumları ile güvenle paylaşmak için sistemlerinde gerekli önlemleri almaları önerilmektedir.

Anahtar Kelimeler: Avrupa Birliği, Açık Bankacılık Rejimi, Ödeme Hizmetleri, (PSD2).
JEL Sınıflandırılması: F10, F13.

Transition to Open Banking Regime and Role of European Union Payment Services (PSD2) Rules

Abstract

European Union will start implementing new rules on payment systems as of September 2019. First step of 'open banking' is banks sharing their data/ account information with third party payment services companies. Payment between European Union and other countries are subject to these rules. The aim of this study is to investigate the advantages, risks and possible consequences of the implementation of new rules. As a result of literature review, countries who have relationship with European Union including Turkey, must take necessary precautions about risks,update local legislation and especially banks must adapt their systems as per PSD2 rules.

Keywords: European Union, Open Banking Regime, Payment Services, (PSD2).
JEL Classification: F10, F13.

1. Giriş

Kuruluşundan bu yana, 'tek pazar' ana hedefi doğrultusunda, mal, hizmet, para ve insanın serbestçe hareket etmesini sağlamak olan (European Union, 2019), Avrupa Birliği, dünya ticaretinin yüzde 34'ünü elinde tutan en büyük ticari birlik olarak, kuruluş hedeflerini gerçekleştirmeye devam etmektedir (Meral, 2019). Bu hedefler doğrultusunda, ödemeler için de tek pazar (İç Pazar) oluşturmak amacıyla, ilk kez 2007 yılında yayınlanan orijinal Ödeme Hizmetleri Yönergesi ile ödeme hizmetleri için kurallar ve yönergeler belirlenmiştir. AB, basitleştirilmiş ödeme işlemleri ile yeni katılımcılarla rekabeti teşvik etmiştir. Ayrıca, Tek Avro

* İstanbul Medipol Üniversitesi, İşletme ve Yönetim Bilimleri Fakültesi, Uluslararası Ticaret ve Finans Bölüm Başkanı, https://orcid.org/0000-0001-9244-1994.

Makalenin Gönderilme Tarihi:29/05/2019 Kabul Tarihi: 29/08/2019

Ödemeler Alanı (SEPA) için yasal platform oluşturulmuştur. AB ve Avrupa Ekonomik Bölgesi'ndeki ödeme hizmetlerini ve ödeme hizmeti sağlayıcılarını düzenlemek ve böylece ödemeler için tek bir pazar oluşturmak ve tüketicilerin haklarını korumak amacıyla 2007'de tanıtılan orijinal Ödeme Hizmetleri Yönergesine dayanarak tasarlanan (Politou, 2019), ikinci Ödeme Hizmetleri Yönergesi, yeni hizmetleri ve yeni oyuncular kapsayan ve e-ödemeler için rekabetçi bir pazarın gelişimini teşvik için ek iş modelleri belirleyerek ilk yönergenin kapsamını genişletmektedir (Giambelluca ve Masi, 2016).

14 Eylül 2019'da (FCA, 2019) ertelenmediği takdirde, yürürlüğe girmesi planlanan PSD2, Türkçe'ye çevrilmiştir (Ödeme ve Elektronik Para Derneği, 2017). AB, 'ödemeler tek pazar' uygulamaları için PSD2 ile standart, daha iyi ve daha verimli bir ödemeler sistemi, özellikle bankalar dışında da yeni katılımcılarla sektörde yeniliği teşvik etmek, internet ve mobil ödeme yöntemlerinde şeffaflığın arttırılması, fiyatların uyumlaştırılması, maliyetlerin düşürülmesi ve ödemelerde güvenliğin geliştirilmesini amaçlamaktadır (Mansfield-Devine, 2016).

Avrupa Parlamentosu, İkinci Ödeme Hizmetleri Yönergesi (bundan sonra PSD2 olarak anılacaktır) ile yenilikçiliği teşvik ederek tüketicilerin mal ve hizmetlere ödeme yapmalarını daha kolay, daha hızlı, daha güvenli ödeme ve Avrupa'daki ödeme sistemlerinin standardizasyonu amacıyla tüketiciler için işlem ücretlerine sınırlama ve düşük ücretlerin iadelerine daha katı kurallar koyan kısıtlamalar getirmektedir. PSD2, Değişim Ücreti Yönetmeliği kapsamındaki ödeme araçlarının kullanımı ve (SEPA) Yönetmeliği kapsamındaki ödeme hizmetleri için ek ücret ödemesine sınır getirilmiştir (EU Regulation, 2015). Örneğin, havayolları veya etkinlik organizatörleri gibi şirketlerin işlem değerinin üstüne ek bir kart ücreti talep etmelerine izin verilmeyecektir. Tüketiciler, ödeme hizmeti sağlayıcısının Avrupa Ekonomik Bölgesi'nin (AEB) dışında olmasına rağmen işlemlerin yanı sıra AEB dışı para birimlerindeki ödemeler içinde korunacaktır. AB, rekabeti ve verimliliği arttırmak için yeni katılımcıların, ödemeler sektörüne girmesi ile Avrupa bankalarının ödeme alt yapılarını ve müşteri verilerini sektöre yeni giren Üçüncü Taraf Finansal Hizmet Sağlayıcıları'na açılması kuralı getirilmiştir. Yönergenin temel amacı, bankalar ve yeni ödeme hizmeti sağlayıcıları için düzenlemeleri standartlaştırmak, ödeme hizmetleri için tek bir entegre pazar oluşturmak, şeffaflık, adil rekabet ve müşterilere fayda sağlayacak yeni ödeme hizmetleri için giriş engellerinin ortadan kaldırılması olarak tanımlanmaktadır. PSD2'nin, AB ülkeleri, ulusal yasalara uygulanması ile bankaların, müşterilerinin verileri üzerindeki tekellerinin ortadan kaybolacağını, banka (gerçek ve tüzel) müşterilerinin, üçüncü taraf sağlayıcılara, hesap verilerini bankalarından alma izni vermelerini sağladığını ve üçüncü taraf sağlayıcıların daha sonra, örneğin, kullanıcılar için doğrudan banka hesaplarından ödeme başlatabileceği öne sürülmektedir (Soland, 2017).

PSD2, kullanıcılar için daha esnek bankacılık sağlamayı amaçlamaktadır; bu, müşterilerin yeni çözümleri oluşturmak için orijinal hesaplarından para transferi yapmak zorunda kalmadan bireysel çözümleri uygun gördükleri şekilde karıştırabilir ve eşleştirebilecekleri anlamına gelmektedir. Buna ayrıca fatura ödeme veya sosyal medya aracılığıyla para transferi gibi bankacılık dışı çözümler de dahil edilecektir (Noctor, 2018).

Ödeme sektörüne yeni giriş yapan yeni katılımcılar, yenilikçi teknolojiler ve artan düzenleme, gelir akışlarını korumak, artan müşteri beklentilerini karşılamak ve rekabet avantajlarının aşınmasına karşı koymak için her zamankinden daha fazlasını yapmak zorunda oldukları için geleneksel bankalara büyük zorluklar getirmektedir. PSD2, bankaların veri altyapısını üçüncü taraflara açma kuralı ile müşterilere daha iyi ürünler ve ödeme hizmetleri sunabilmesi kuralı getirmektedir ancak aslında bu yeni ödeme teklifleri finans teknolojisi endüstrisi tarafından desteklenmekte ve bir süredir uygulanmaktadır. Bu nedenle iyi uygulama ve yeterli yönetişimi sağlamak için düzenleyici bir çerçeve sağlamak üzere PSD2 yürürlüğe girmiştir (Tengur, 2017).

PSD2'nin stratejik hedeflerinden birisi, tüm üye ülkeleri tek bir dijital pazarda düzenlemektir. Bu girişim, ilk Sınır Ötesi Hizmetler Yönergesi altında ve sınır ötesi ödemeleri iyileştirmeyi ve birleşik bir pazar yaratmayı hedefleyen Tek Avro Bölgesi Ödemeler Alanı (SEPA) ile başlamıştır. PSD2 yönergesi ise daha önce birçoğu düzenlenmemiş olan ve ödeme hizmetleri yelpazesi içinde faaliyet gösteren daha küçük ödeme kurumlarını ve ilgili finans teknolojisi (FinTech) kurumları artık PSD2 ile bir "ödeme kurumu" olarak tanımlanarak, kapsama girmektedir. Kurulan bankacılık işletmeleri, diğer bankaların müşterilerine hem mevcut hem de yeni hizmetler sunarak, yani finans teknolojisi oyuncuları olma fırsatını benimsemek için davet edilmektedir, bunu örnek olarak, birkaç banka (ING, KBC ve Belfius) tarafından desteklenen bir mobil ödeme teklifi olan Payconiq (Payconiq, 2018) verilebilir.

1.1. PSD2 Süreci

PSD2, 13 Ocak 2016'da tüm üye ülkelerde yürürlüğe girmesine rağmen, yönergenin ulusal yasa ve yönetmeliklerine dahil etmesi için iki yıllık bir süre gerekmektedir. Güçlü müşteri kimlik doğrulaması ve güvenli iletişim için gereksinimleri tanımlayan Teknik Standartlar Kurallarına (RTS- Regulatory Technical Standards), uyulmak zorunda olunduğundan, yürürlüğe girme tarihinden 18 ay sonra, yani Eylül 2019'da uygulamaya başlayacaktır (Politou, 2019).

PSD2 kuralları gereği, Hesap Hizmeti Ödeme Hizmeti Sağlayıcıları (ASPSP-Account Servicing Payment Service Providers) olarak da bilinen bankacılık kurumlarının, müşterilerinin hesaplarıyla ilgili kişisel bilgilerinin ve müşterilerinin hesaplarının Üçüncü Taraf Ödeme Hizmet Sağlayıcılarına (TPPs-Third Party Payment Service Providers) açık erişim yetkisi vermelerini gerektirmektedir. Bankacılık kurumlarının açık erişim yetkisi verdikleri, Üçüncü Taraf Ödeme Sağlayıcıları aracılığıyla, perakendeciler ve bankalar arasında bağlantı sağlanacaktır. Üçüncü Taraf Hizmet Sağlayıcıları iki gruptan oluşmaktadır.

1. Hesap Bilgileri Hizmet Sağlayıcıları (AISPs-Account Information Service Providers) Grubu: Müşterilerine hesap ve bakiye genel bilgisi veren, müşterileri istediği zaman bir veya birden fazla bankadaki hesap bilgilerini konsolide şekilde bir platform aracılığı ile online olarak müşteriye sunulması hizmetidir. Bu sayede müşteriler finans durumlarını kolaylıkla yönetebileceklerdir.

2. Ödeme Başlatma Hizmet Sağlayıcıları (PISPs-Payment Initiation Services Providers) Grubu: Müşterileri adına ödemeyi başlatan ve satıcılara paranın yolda olduğu güvencesini veren, müşterilerinin online satın alma işlemlerini para transferi yöntemi ile hesabının bulunduğu banka dışında üçüncü parti ödeme sağlayıcısı aracılığı ile gerçekleştirebildiği bir hizmettir.

Her Üçüncü Taraf Ödeme Sağlayıcı (TPP) kurumu, iki gruptan birine girecektir.

Ödeme Başlatma Hizmet Sağlayıcısı (PISP- Payment Initiation Services Providers): Bankalar tarafından sağlanan uygulama arayüzleri (bundan böyle API olarak anılacaktır) kullanarak kullanıcı adına ödeme işlemini başlatır (müşteri bu izinlere erişim izni verdiyse). Fonlar doğrudan kullanıcının banka hesabından satıcıya taşınır ve genellikle ödeme kartı şirketleri tarafından tahsil edilen ücretleri ortadan kaldırmaktadır.

Hesap Bilgileri Hizmet Sağlayıcıları (AISP-Account Information Service Providers): Müşteri hesaplarına bağlanarak ve sadece bilgi alabilmektedir. Ödeme Başlatma Hizmet Sağlayıcıları ise ödeme taleplerini başlatmak için bankaların sistemlerine güvenli kanallardan bağlanabilmektedir. Bu yeni oyuncular, tüketicilere geleneksel bankacılık alanlarına göre daha fazla seçenek sunacak ve daha geniş bir hizmet yelpazesiyle gelir elde ederek ekonomiye katkıda bulunacaktır. Bu kuruluşlar, kullanıcıların banka bilgilerine erişerek, örneğin, tek bir kullanıcının birden fazla banka hesabındaki bilgilerini tek bir kaynaktan toplayabilir. Bu bilgilere erişim yetkisi ile erişilen bilgiler bağlamında yeni uygulamalar ve

hizmetler oluşturmalarına olanak sağlayacak ve bunun, yenilikçi hizmetler oluşturmak için mevcut bankacılık sektörüyle bağlantısı olmayan teknoloji girişimlerini etkileyeceği umut edilmektedir (Mansfield-Devine, 2016).

Porcedda (2018), Avrupa Komisyonu tarafından belirlenen hedefi, politika belgeleri, yasal analizler ve ihlaller yasasıyla ilgili akademik literatürle zenginleştirilmiş bir değerlendirme ölçütü olarak kullanarak düzenleme yama çalışmasını değerlendirmesinde, siber güvenlik ihlallerine ilişkin düzenleyici çerçevenin, güvenlik önlemlerinin işleyişi, hem düzenleyici makamların hem de kamuoyu hakkında farkındalık konusunda gerekli karşılıklı öğrenme seviyesini sağlamada başarısız olabileceğini öne sürmektedir.

Steennot (2018), ilk versiyon ile PSD2'yi karşılaştırdığı çalışmasında, PSD2'de yetkisiz ödeme işlemleri sorumluluğu ile ilgili kuralların, PSD1 kurallarına benzermiş gibi görünse dahi, bu kurallara daha yakından bakıldığında, tüketicilerin korunmasına yönelik önemli etkisi olacak birkaç değişiklik yapıldığı açıkça görüldüğünü, güçlü müşteri kimlik doğrulaması gerekliliği ve ödeme hizmeti sağlayıcısının, güçlü müşteri doğrulaması kullanılmadığında bile, ödemeyi yapan kişiyi sorumlu tutma yükümlülüğü bulunmaması nedeniyle, tüketicinin korumasının arttırıldığını belirtmektedir. Tüm bu iyileştirmeler ile kişisel güvenlik bilgilerini güvenli tutulması halinde, PSD2 kapsamında risklerin çok sınırlı hale geldiğini öne sürmektedir.

Ödeme Hizmetleri Direktifi (Payment Services Directory) kuralları ile bankalar, API hizmetleri aracılığıyla üçüncü parti hizmet sağlayıcılarına, yani 'Ödeme Hizmetleri Sağlayıcıları" kurumlarına, müşteri bilgilerini erişime açacaktır. Bankalar dışında yeni oluşturulan bu grupla, bankalar arasında rekabet oluşturularak, yeni oyuncularla ödeme piyasasını, daha verimli hale getirmek amaçlanmıştır. Yeni yönerge PSD2 ile AB dışı ödeme işlemleri kapsam içine alınmış, bankaların müşteri bilgilerini, Hesap Bilgileri Hizmet Sağlayıcıları (Account Information Service Providers), Ödeme Başlatma Hizmet Sağlayıcıları (Payment Initiation Service Providers) ile paylaşımında, bilgi güvenliğinin sağlanabilmesi için ileri güvenlik yöntemleri belirlenmiştir. Bankaların hesap bilgilerini üçüncü taraflarla paylaşma kuralı, cep telefonlarında, numaraların taşınabilmesi gibi, banka hesabının da, bir başka bankaya, hesap numarası değişmeksizin taşınabilmesine olanak sağlanmıştır (Coşkun, 2018).

2. Açık Bankacılık ve PSD2

Bankacılık sektörü, uzun bir süredir sıkı bir şekilde kontrol edilerek, düzenlemeler yapılmıştır. Düzenleyici gelişmeler, Avrupa bankacılık piyasalarının yapısını şekillendiren önemli bir faktördür. 1 Ocak 1993'ten itibaren Avrupa mevzuatı (Maastricht Antlaşması), mevcut engelleri ortadan kaldırarak veya azaltarak ve finansal hizmetler için tek AB pazarını sunarak "dünyanın en büyük ve en açık bankacılık pazarını" yaratmıştır (Casu, B. and Girardone, A., 2009).

AB'nin düzenleyici reformuna paralel olarak, 2015'te, İngiltere Hükümetinin, bankacılıkta açık bir API standardı tasarımı için bir çerçeve sunmak amacıyla Açık Bankacılık Çalışma Grubu (OBWG-Open Banking Working Group) kurulması talebini takiben, ertesi yıl, Rekabet ve Piyasa Otoritesi (CMA-Competition and Markets Authority), çeşitli geçici öneriler yayınlamıştır. İngiltere'de açık bankacılığın temelini oluşturan ortak teknik standartların oluşturulması amacıyla bir tüzel kişilik oluşturmak üzere dokuz büyük İngiltere bankasını görevlendirmiştir. PSD2'nin aksine, İngiltere'deki Açık Bankacılık girişimi, gerekli API'lerin tanımlanması ve geliştirilmesinin yanı sıra güvenlik ve mesajlaşma standartları da daha açık bir şekilde yer almaktadır (Zachariadis and Ozcan, 2017).

PSD2 ve İngiltere'deki Açık Bankacılık henüz ulusal hukuka aktarılmamış olsa dahi, birçok sağlayıcı yeni ödemeler ekosisteminin yaratacağı fırsatlardan yararlanmak için stratejilerini belirlemeye başlamıştır. Ancak, böyle bir düzenlemenin etkisinin ne olacağı ve

bunun gerçekten de piyasadaki yeni oyuncular için nasıl ve ne şekilde yeni fırsatlar yaratıp yaratmayacağı henüz net değildir. Telekomünikasyon, enerji ve ulaştırma gibi çeşitli AB ağ endüstrilerindeki rekabeti artırmak amacıyla yapılan önceki reformları, genellikle uzun vadeli düşük fiyat seviyeleri, genişletilmiş çıktılar ve işgücü verimliliği kazanımlarıyla ilişkilendirilmiştir (Martin, et al., 2005). Sonuçta, bu tür reformların, tüketicilerin refahını iyileştirdiğini ve Ar-Ge ve inovasyondaki daha iyi hizmet ve yatırım kalitesine yol açtığını doğrulamaya meyilli olduğunu göstermektedir. Bununla birlikte, bu tür sonuçlar genellikle sanayi katılımcılarının ve iş piyasasının yeni ekonomik durumlara uyum sağlama kapasitesine bağlıdır (Zachariadis and Ozcan, 2017).

AB'de PSD2 ve İngiltere'de Açık Bankacılık girişiminin, düzenleyici çerçeveleri ile 'Platform Bankacılık' kavramlarının Avrupa'da tüm bankacılık sektörüne uygulanması için fırsat oluşturmaktadır. Bankaların API'lerini (özellikle ödeme başlatma hizmeti ve hesap bilgileri hizmetini) açmak ve müşteri verilerini paylaşmalarını istemek, bir platform iş modelinin uygulanması ve bankacılığın etkileri üzerine bir fırsat sağlamaktadır. "Platform Bankacılık" (BaaP-Banking as a Platform) oluşturulması için kurulan bu hareket, bankaların bir platform strateji modeli benimseyebilecekleri ve rekabet kurallarını değiştirebilecekleri yerleri tanımlamaktadır. Bunu yaparken, bankaların finansal aracılar olarak rollerini tekrar gözden geçirmeleri ve "platformun her tarafındaki katılımcılara değerli yeni ürünler ve hizmetler sunan çevrimiçi otomatik araçlar ve sistemler" sağlayarak yeniden aracı olmaya hazır olmaları gerektirmektedir. (Parker et al., 2016).

Ancak, AB, PSD2 düzenlemesinin, ödemeler ve bankacılık verileri üzerinde büyük etkisi olabilir. Yeni düzenleyici rejimin cevapsız bıraktığı güvenlik ve verilerin gizliliği hakkında hala cevaplanmamış bazı ciddi soruların olduğu sorgulanmaktadır (Mansfield-Devine, 2016).

Bankaların itibarları güvene dayalı olduğundan, güven için dev bütçeler ayırarak harcamalar yapmaktadır. Bankalar özel düzenlemelere tabi olarak denetlenmektedir. PSD2'de müşteri verilerinin korunması, güvenliği ve gizliliğinden bankalar sorumlu tutulmaktadır. Ancak üçüncü taraf uygulamalara arayüzler (API) aracılığıyla verileri sunmak zorunda kalınca, üçüncü taraflarla, aynı güvenlik standardını benimsemek zorunda kalacakları için, bankaların verilerin güvenli olmasını sağlayabilmelerinin tek yolu, teknolojiyi ve mobil uygulamalarında sahip oldukları önlemleri almak ve temel olarak uygulama aracılığıyla bir yetki vermeye zorlamaktır. Bu şekilde, üçüncü tarafın verilere erişmesine izin verilmeden önce, son kullanıcı ile doğrudan iletişim kurularak, yetki alınması olarak önerilmektedir (Noctor, 2018).

Teknoloji sektöründeki Apple, Google, Microsoft ve Linux gibi firmalar, aynı zamanda diğer sektörlerdeki Airbnb, Uber, eBay, YouTube, Facebook, VISA, MasterCard, vb. firmalar bu iki prensibi başarılı dijital platformlar oluşturmak ve avantaj sağlamak için kullanmaktadır. Bu platformların yeni değer yaratma ve tedarik kaynaklarını çekme yeteneğine de sahip olduklarından, örneğin, iPhone ürünü ile Apple, yalnızca örgütsel kaynaklarını kullanarak bu kadar çok sayıda uygulama geliştiremezdi. Bunun yerine, ürünlerini açıp özelliklerini, açık API'ler aracılığıyla tüm geliştiriciler topluluğunun kullanımına sunarak, hem miktar açısından (uygulama sayısı) hem de uygulama açısından çok daha yüksek oranda yeni değer kaynakları yaratmıştır (Zachariadis and Ozcan, 2017). Nitekim dijital platform bağlamında, açık API'ler, kuruluşların bir yazılım platformuna dayalı temel bir işlevselliği paylaşabilecekleri ve dış geliştiricilere onunla birlikte çalışan modüller üretme fırsatı sunabilecekleri sınır kaynakları olarak kabul edilmektedir (Tiwana et al., 2010; Ghazawneh and Henfridsson, 2013). Dikkatli bir şekilde üretilmiş ve işaretlenmiş API belgeleri ekosistemi geliştirmeye ve genişletmeye yardımcı olabilir ve yeni oyuncuların yanı sıra firma dışından gelen bilgi ve yetenekleri davet edebilir (Van de Ven, 2005).

Açık bankacılık yani üçüncü taraflara, API (arayüz) uygulama programlama aracılığıyla müşteri verilerine veya ödeme işlevine erişim sağlama, başka bir deyişle veri ve işlevsellik paylaşımları diye tanımlanan 'açık bankacılık', PwC'nin konu ile ilgili yaptığı araştırmaya göre,

ankete katılan bankaların sadece yüzde 47'sinin konuyu takip ettiği ifade edilmektedir (PwC, 2017).

Politou, (2019) araştırmasında, PSD2'nin kaçınılmaz bir şekilde, ödemeleri değiştireceğini ve elektronik ödemelerdeki her şeyi etkileyeceğini belirtmiştir. Örneğin, bankaların müşterilerin verileri üzerindeki tekelini bozacağını, çünkü Facebook gibi işletmelerin, bireylerin hesap verilerine erişim izni vermeleri halinde, bankalarından hesap bakiye bilgilerini alarak onlar adına ödeme yapmalarını sağlayabileceğini öne sürmektedir. PSD2 mevzuatının, tüm ödeme paydaşları arasında veri paylaşımını kolaylaştırdığı ve oluşumdaki veri bakımından zengin tüketicinin yeni ürünler üretmek için onu kullanabilecek üçüncü taraflara geçmesine izin verdiği için açık bankacılık rejimi için atılmış önemli bir adım olduğunu belirtmektedir. Bu bağlamda, bankaların, üçüncü taraf hizmet sağlayıcıların, çevrelerine kendi ürünlerini ve hizmetlerini kurabilmek için, verilerine güvenli bir şekilde ulaşmalarını sağlamak için Uygulama Programlama Arayüzleri (API'ler) oluşturmaları gerekecektir. Müşterilerinin harcama alışkanlıkları veya kredi geçmişini temel alarak, tüketicilerin profillerini oluşturmaları, PSD2'nin kaçınılmaz olarak katkıda bulunacağı yeni ve saygın bir hizmet olarak kabul edileceğini öne sürmektedir.

Steennot (2018), çalışmasında PSD2'nin kapsamını genişlettiğini ve yetkisiz işlemler için mükellefi liyakat derecesini daha da azalttığını, örneğin, ödeme yapılmasını kanıtlamak için destekleyici kanıtlar talep ederek, mükellef müşterilerin kimlik doğrulaması yapılmaması durumunda mükellefi sorumlu tutmayı imkansız hale getirdiğini göstermektedir. Dolandırıcılık veya ağır ihmal ve yetkisiz işlemler, bir ödeme başlatma servisi aracılığıyla başlatıldığında da aynı kurallar uygulanmaktadır (Steennot, 2018).

Borgogno ve Colangelo, (2018) araştırmalarında, Avrupa Birliği Komisyonu, Uygulama Programları Arayüzleri (API) kullanımının özel ve kamu kurumlarında anahtar bir rol oynadığını ancak API'ler üzerinden veri paylaşımının karmaşık bir uygulama süreci gerektirdiğini ve standardizasyon girişimlerinin başarısı için şart olduğunu vurgulamaktadır.

Noctor (2018), PSD2 kurallarının verdiği yetki ile hem tüketicilerin hem de işletmelerin tüm banka müşterilerinin finansmanlarını yönetmek için bankaların artık Üçüncü Taraf Hizmet Sağlayıcı'larına, müşterilerinin hesaplarına erişebilmelerine izin vermek için arayüz uygulama programı (API) sağlamak zorunda olduklarına dikkat çekmiştir. Bu uygulamanın, nasıl çalışacağı, erişimin ne kadar güvenli olacağı, hangi risklerin ortaya çıkacağı ve kimler için risk doğuracağının sorgulanması gerektiğini belirtmektedir. Söz konusu uygulamanın kırıldıktan ve (API) arayüzlere erişildikten sonra, sistemi meşru bir müşteri olarak tanıma ve API (arayüz)'nın bağlanmasına izin verilen herhangi bir şeye erişmelerini sağlamak, sistemi kandırmak için bunların kullanılabileceğini iddia etmektedir. Müşterinin hesabının hangi bankaya bağlı olduğuna bağlı olarak, aynı hesaba erişmek için kullanılan üçüncü taraf uygulamasının, verilere erişmek için farklı bir API (arayüz), oluşturmak zorunda kalacağını ve bu bağlantısız yaklaşımın ise hem uygulama geliştiricileri hem de son kullanıcıları için işleri daha karmaşık hale getireceğini öne sürmektedir. Cep telefonu sistemleri, kendi uygulamalarını ayrı tutarak, son kullanıcının gizliliğinin daha iyi korunmasını sağlamaktadır. Ancak, bu konu bankalar ve üçüncü taraf arasında gerekli bağlantı uygulamaları söz konusu olduğunda her türlü soruna neden olabilir. İki uygulamanın bağlanacağı nokta aynı zamanda en savunmasız nokta, saldırganların birinden diğerine giden verileri yakalayabileceği, hatta zararlı yazılımları ele geçirebileceği nokta. Kullanıcı üçüncü taraf uygulamasının bankacılık bilgilerine erişmesine izin verdiğinde, kötü niyetli uygulamanın da erişim kazanması da mümkün olmaktadır.

3. AB Yeni Ödeme Sistemi PSD2 Uygulama Riskleri ve Güvenlik Önlemleri

Yeni ödeme ve bilgi erişim mekanizmaları dolandırıcılık, veri ihlalleri ve siber saldırılar gibi tehditlere karşı savunmasız olabilir. Dolayısıyla düzenleme, bu tehditleri hafifletmek ve tüketici varlıklarını güvence altına almak için bir güvenlik temeli oluşturmayı amaçlamaktadır.

Çevrimiçi ödeme işlemleri için ‘güçlü müşteri kimlik doğrulaması’ kullanımını gerektirir. Asgari şartlar, iki faktörlü kimlik doğrulaması, bankacılık sektörü tarafından zaten yaygın olarak benimsenmiş bir norm kullanımı içindir. Ödeme Hizmetleri Sağlayıcıları Kurumlarının, müşterilerini sahtekarlık ve veri ihlallerinden korumak için atılan adımları ayrıntılı bir risk değerlendirmesi içeren bir güvenlik politikası belgesi sağlamaları ve önemli operasyonel ve güvenlik olaylarını tespit etmek ve raporlamak için olay yönetimi prosedürleri oluşturmaları gerekecektir. Düzenleyici kurumlara yıllık inceleme ve raporlama için de gereksinimler vardır. Hesap hizmeti ödeme hizmeti sağlayıcıları, üçüncü taraf ödeme sağlayıcılarına erişime izin vermeli, ancak tüm ödeme hizmetleri sağlayıcıları, ödeme hizmeti kullanıcısının erişim kimlik bilgilerinin gizliliğini ve bütünlüğünü korumak için yeterli güvenlik önlemlerinin uygulanmasını sağlamalıdır. Güçlü müşteri kimlik doğrulaması ve güvenli açık iletişim standartları dahil olmak üzere, yayınlanan yasal teknik standartların (RTS-Regulatory Technical Standards) gerekliliklerini yerine getirecek düzenlemeler yapılmalıdır (Politou, 2019).

Goode (2018), bankalar ile ilgili çalışmasında, bankaların, yeni müşterileri daha iyi tanımlamak, mevcut müşterileri güvenli bir şekilde doğrulamak, yüksek değerli işlemleri korumak ve sahtekarlıkla mücadele etmek için her yerde biyometrik teknolojiyi kullandıklarını, bu teknolojinin tüm kanallardaki bankacılık müşterilerinin kimliğini doğrulamak ve güvenceye almak için tek güvenilir yol olduğunu, bu nedenle, bankaların, PSD2’nin teşvik ettiği biyometrik teknoloji kullanımını, verileri üçüncü taraflara açılması için Açık Bankacılık arayüzlerinde (API) de güvenilir olarak kullanması gerektiğini belirtmiştir.

McDowell (2019) çalışmasında, PSD2’deki Güçlü Müşteri Kimlik Doğrulama zorunluluğu için biyometrik kullanılmasını önerme nedenini, Verizon (2017) raporuna göre, kişisel veri ihlallerinin yüzde 80’inin zayıf veya çalışmış şifrelerden yararlanan saldırılardan kaynaklandığını, bu nedenle, biyometrik kullanımında, bu verilerin üçüncü kişilerce kullanımı mümkün olmadığı için biyometrik kullanımı olarak açıklamaktadır.

Cook, (2017) da araştırmasında, Biyometrik Teknoloji Dijital bankacılığın ilerlemesi, bankacılık sektörünün geleceğini tamamen değiştirdiğini ve bu değişimde, en önemli faktörlerden birisinin biyometrik teknoloji biçimindeki dijital kimlik güvencesi olduğunu kabul etmekle birlikte, geleneksel bankaların çoğunun eski miras sistemlerine sahip olduğunu ve dijital dönüşüm ile birlikte, mevcut müşterilere hizmet ederken ve yenilerini çekerken neredeyse tamamen yeni bir banka oluşturmak gibi çok zor olduğunu, bankaların yasama değişikliği ve yeni rekabet tehdidi de dahil olmak üzere birçok baskıya maruz kaldığı bir zamanda ortaya çıktığını belirtmiştir.

Mobil bankacılık kullanımı da dijital dönüşümle birlikte olağanüstü artmıştır. Gelişmiş ülkelerdeki yetişkin akıllı telefon kullanıcılarının yüzde 43'ü banka hesaplarını kontrol etmek için mobil cihazlarını kullanmaktadır (Deloitte, 2017).

PSD2 versiyonunda, Londra merkezli Avrupa Bankacılık Otoritesi (EBA), teknik detayların çoğunun tanımlanmasında öncü bir rol üstlenmektedir. Düzenleyici Teknik Standardı (RTS- Regulatory Technical Standards), PSD2 ile aynı tarihlerde yürürlüğe girmek üzere yerel düzenleyiciler için ilkeleri tanımlamaktadır. Bunlar, çok faktörlü kimlik doğrulamasına dayalı, bankalar için güçlü kimlik doğrulama (Avrupa Bankacılık Otoritesi, 2015), mevcut AB elektronik kimlik düzenlemelerinin (e-kimliklerin) arttırılması gibi konular olabilir. Güçlü kimlik doğrulama standartları muafiyetinin, PSD1 versiyonunda sadece telekomünikasyon şirketleri tarafından kullanılması amaçlanmıştır. Ancak diğer birçok firma suiistimali nedeniyle PSD2’de beklenenden daha az muafiyet içeren güvenli iletişim standartları beklenmektedir (Mansfield-Devine, 2016).

Yeni kurallar, çevrimiçi ödemelerin yapılma şeklini değiştirecek ve müşterilerin bir işlem gerçekleştirmek için aşağıdaki üç tanımlayıcıdan en az ikisini sunmaları gerekecektir. 1) Kullanıcıların bildikleri bir PIN kodu veya parola 2) Sahip oldukları cep telefonu veya donanım belirteci ve/veya 3) 'Oldukları' bir şey yani (parmak izi doğrulama veya yüz tanıma).

Yenilikçiler öncelikle süreçteki kullanıcı deneyiminden ödün vermeden en iyi şekilde nasıl uyulacağını bulmak için çalışmalıdır. Gerekli tanımlayıcıların tümü bir akıllı telefon aracılığıyla doğrulanabilir, bu nedenle ödeme uygulamaları, Google Pay veya Apple Pay gibi popüler olan kullanıcı arayüzü/kullanıcı deneyimini çoğaltmaya çalışmalıdır (Nuggets, 2019).

Walters ve Jacobs (2019), PSD2 ile ilgili analizleri sonucunda, hizmet sağlayıcıları aracılığı ile tüketicinin yüksek düzeyde korunacağı ve ödeme işlemlerinin güvenliği ve sahtekarlığa karşı korunma garantisi verileceği belirtilmesine karşın önceliğin ödeme hizmetleri için pazarın gelişmesi olduğunu, güvenlik ve gizliliğin ikinci planda kaldığı gerekçesiyle eleştirerek, kullanıcıların gizli bilgilerinin yeterince korunmadığını öne sürmektedir. Bankaların, hizmet sağlayıcılarının şifre süreçlerine güvenmeleri gerekmektedir. Ayrıca, tüm bu taahhütlere karşın, PSD2'nin 'hesap bilgi tanımı'nın çok geniş ve çeşitli hizmetleri kapsadığı için ödeme hizmeti sağlayıcılarının özel arayüzünün (API) düzgün çalışmaması durumunda, geri çekilme seçeneğine rağmen, kullanıcı hesabına sınırsız erişim sağlayarak, kullanıcıların kişisel verilerini yeterli şekilde korumadığını öne sürmektedir.

Ödeme hizmeti sağlayıcıların da ayrıca gizli ödeme verisi talep etmeleri ve kullanıcı tarafından açıkça talep edilen hesap bilgileri hizmetinin sağlanması dışındaki amaçlarla herhangi bir verinin kullanılmaması ve bunlara erişilmesi yasaktır. (Donnelly, 2016).

Fuster'ın ayrıntılı analizinde açıkladığı gibi, PSD2'nin, ödeme sahtekarlığı önleme, soruşturma veya tespit etme adı altında, "örneğin genellikle veri madenciliği veya profilleme teknikleri genellikle hileli dolandırıcılık ile hile dışı ödemeleri birbirinden ayırt etmek için kullanılmak amaçlanmalıyken, ödeme sahtekarlığı ile tamamen ilgisi olmayan kişilerin kişisel verilerinin işlenmesi gibi süreçlere kapı açtığını vurgulamaktadır (Fuster, 2016).

Genel olarak, PSD2'nin geniş kapsamı, pek çok endüstriyel ve bankacılık paydaşı tarafından, genel olarak bankacılığın geleceği için bir temel teşkil eden oyun değiştirici bir girişim olarak kabul edilirken, bir yandan da düşük güvenlik standartları nedeniyle bankacılık endüstrisi tarafından ise finansal olmayan kurumlara düşük güvenlik standartları nedeniyle eleştirilmekte ve diğer yandan, veri koruma konularını ele almakta ve bankacılık işlem verilerini açarak ve bütünüyle bir finansal profilin oluşturulmasına katkıda bulunmaktadır (Mansfield-Devine, 2016).

Orme (2019) ise PSD2 yönergesinin (Financial Conduct Authority, 2018) 'güçlü müşteri kimlik doğrulaması' şartı nedeniyle, "Kripto Para Birimleri'nin kullanılmasının, güçlü müşteri kimlik doğrulaması şartına uygun olduğunu ve bitcoin gibi kripto para birimlerinin kullanılabileceğini önermektedir.

Güvenlik önlemi ile ilgili bir başka çözüm önerisi ise Bankacılık endüstrisi, PSD2 kurallarına bağlı kalırken, uygulamaların manipülasyonunu önlerken güvenli veri erişimi ve izin yönetimi sağlamanın bir yolunu bulmaya ihtiyaç duyacaktır. Bunu yapmanın bir yolu, üçüncü taraf uygulamaların müşteri verilerine ne kadar süre erişebileceğini izlemek için ekranlar veya izinleri yönetmenin bir yolunu sağlamak ve müşterinin üçüncü taraf uygulamalarının verilen erişim izinleri için mutlu olduğunu teyit etmektir. Bankalar, kullanıcıların başvuruda tercihlerini belirleyebilmelerine izin vermektedir, ancak üçüncü taraf uygulamasında izin tercihlerini kontrol edemeyeceklerdir (Noctor, 2018).

Colangelo ve Maggiolino (2019) araştırmalarında, dijital teknolojilerin kullanımını ve gelişimini eleştirerek, pasif ve güçsüz dijital tüketici hakkında endişelendiklerini ve bu duruma tepki verilmesi gerektiğini ileri sürmektedir. Avrupa Birliğinin yeni düzenlemeleri ile tüketicilerin dijital pazarlarda nihayet öncü bir rol üstlenmeleri için fırsat olduğunu, tüketicileri güçlendirmek ve kişisel verilerinin yönetiminde özerk ve bağımsız karar alabilmeleri için yeni kurallar olması gerektiğini öne sürmektedir.

Avrupa Birliği üye ülkeleri de PSD2 uygulaması ile ilgili eleştirilerde bulunmaktadır (Pantlin, 2018).

Hollanda Veri Koruma Kurumu, PSD2 gizlilik hükümlerini özellikle eleştirmektedir. Eşi görülmemiş bir hamleyle, Hollanda Veri Koruma Otoritesi (Autoriteit Persoons Gegevens, "AP"), PSD2 uygulanmasına ilişkin istenmeyen ve eleştirel bir görüş yayınlamıştır. Hollanda Veri Koruma Otoritesi'nin görüşüne göre, mevcut yasa taslağı birkaç cephede tatmin edici değildir. Diğer şeylerin yanı sıra, düzenleyici kullanılan dilin teknolojik olarak nötr olması gerektiğini, Genel Veri Koruma Yönetmeliğinin bir anlaşmazlık durumunda daima öncelikli olması gerektiğini savunmaktadır. PSD2 uygulaması öncesi Gizlilik Etki Değerlendirmesi yapılması gerektiğini ve ayrıca, PSD2'deki veri koruma hükümleri konusunda düzenleyici yargı yetkisine Hollanda Ulusal Bankasının değil, kendilerinin sahip olması gerektiğini savunmaktadır.

Norveç Veri Koruma Kurumu (DPA- Norwegian Data Protection Authority), PSD2'nin gizlilik için getirdiği zorlukları inceleyen bir rapor yayınlamıştır. PSD2'nin büyük teknoloji şirketleri de dahil olmak üzere yeni oyuncuların finansal sektöre ve ödeme başlatma hizmetleri ve hesap bilgilendirme hizmetlerinin sektöre girmesini sağladığını, bankalar bu nedenle, müşterilerinin işlem ayrıntıları üzerindeki tekellerini yitirmekte olduğunun belirtildiği raporda, ayrıca bankacılık sektörü dışındaki şirketlerin, banka veri ve altyapısı üzerinde yeni hizmetler yaratabileceği öngörülmüştür. Piyasadaki rekabetlerini korumak için, bankalar ve sigorta şirketleri gibi geleneksel oyuncuların, yeni oyuncular ile yeni ittifaklar ve ortaklıklar kurarak cevap verebilecekleri önerilmektedir. Raporda, geleneksel bankaların ve sigorta şirketlerinin Norveç'teki tüketiciler arasında yüksek güven duyma eğiliminde olduklarını ve finansal hizmetlerin güvenli olmasını bekledikleri ifade edilmektedir. Norveçli tüketiciler, gizli finansal verilerinin yüksek düzeyde korunmayı hak ettiğini ve finansal sektörde gizli bilgilerin korunması sağlayan kurumların rekabet avantajını yaşayacağı ifade edilmektedir. Raporda ayrıca müşteri gizliliğini en iyi şekilde korumak için finansal hizmet sağlayıcılarına önerilerde bulunmaktadır. Bu öneriler; gizli verileri korumanın, işin merkezinde olması ve iş modelleri uygulanmadan önce iş modellerinin tartışıldığı bir etik konsey komitesi kurulması, müşterilere açıklık ve şeffaflık sağlayan çözümler oluşturulmalı, müşterilerin mümkün olduğunca hangi kişisel verileri paylaşmak istediklerini ve bu verilerin hangi amaçla kullanılabileceğini seçebilecekleri kullanıcı dostu çözümler oluşturulmalı, vergi gizliliğini geliştiren teknoloji kullanılmalı, şeffaflığı artırmak ve Genel Veri Koruma Yönetmeliğine uyum sağlamak için sertifika mekanizmaları, gizlilik mühürleri ve işaretleri geliştirilmeli, sigorta, bankacılık ve finans teknoloji şirketleri standartlar geliştirmek için araştırma yapmalı ve yeni arayüzlerin (API) geliştirilmesinden önce veya sigorta şirketleri, ürün sağlayıcıları ile ortaklığa girmeden önce gerekli risk değerlendirmeleri yapılmalıdır. İşlemin gizliliği açısından yüksek bir risk oluşturduğu durumlarda, Genel Veri Koruma Yönetmeliğindeki gerekliliklere uymak için bir veri koruma etki değerlendirmesi yapılmalıdır. Söz konusu raporda, tüm bunların uygulanması ile tasarım çözümleriyle gizliliğin etkin, iyi ve yenilikçi kullanımı, yeni banka ve sigorta hizmetlerine uzun vadede rekabetçi bir avantaj sağlayabileceği ifade edilmiştir.

İngiltere'nin ise Avrupa Birliği'nden ayrılmayı planlamasına rağmen, İngiltere'deki bankalar ve diğer işletmelerin, PSD2 sürecine dikkat etmelerini gerektirmektedir. PSD2, İngiltere AB'den ayrılmadan önce yürürlüğe gireceği için Brexit sürecinin belirsiz zaman çizelgesi göz önüne alındığında, İngiltere'deki işletmelerin ve özellikle bankaların, PSD2'nin gerekliliklerine en az bir veya iki yıl, muhtemelen daha uzun bir süre boyunca uymaları gerekebilir. Bu, örneğin, bankaların gerekli API'leri uygulamaya koymaları gerekeceği anlamına gelir. Bu süreçten geçtikten sonra, İngiltere'nin AB dışına çıkar çıkmaz bu hizmetleri terk etmeleri pek mümkün olmayabilir. (Mansfield-Devine, 2016).

4. Sonuç

PSD2, AB ülkelerini kapsayan kurallar olsa dahi aslında taraflardan yalnızca birinin AB'de olduğu durumlarda da diğer tarafı da dolaylı olarak ilgilendirmektedir. PSD2 AB ülkeleriyle AB dışı ülkelerin arasında gerçekleşen para transferlerinde AB ülkelerinin uyması gereken kural ve koşulları belirlemişse de, AB ile ticari ilişkileri olan ülkelerin PSD2 işlemlerinden

etkileneceği göz önünde tutulmalıdır. Nitekim Türkiye de, henüz AB'ye tam üye olmasa da gerek Gümrük Birliği Antlaşması nedeniyle ürünlerin serbest dolaşımı, gerekse de bölge olarak çok yakın olduğundan, karşılıklı olarak ithalat ve ihracat çok yoğundur. Türkiye'nin 2018'de toplam 165 milyar dolarlık ihracatının, yüzde 50'sini, 85 milyar dolarlık AB'ne ihracatı oluşturmaktadır. Türkiye'nin 223 milyar dolarlık ithalatının ise 84 milyar dolarlık kısmı AB ülkelerinden yapılmaktadır. Bu nedenle çok yoğun dış ticaret ilişkilerimizin olduğu AB ülkeleri ile ödemelerin bir tarafının AB ülkesi yani PSD2 kapsamında yapılacağının göz önünde tutularak, sadece sistemsel değil, tahsil edilecek masraflarda uygulanacak kısıtlamalara değin, işlemlerin etkilenmesi doğaldır.

Bu nedenle, örneğin Türk bankalarının, 'elektronik dış ticaret' yani 'online' sipariş vererek, kredi kartıyla ödeme yapmak isteyen bir AB ülkesi vatandaşı ile PSD2 kapsamında, verilerini üçüncü taraf ödeme hizmetleri sağlayıcıları ile paylaşabilmek için gerekli güvenlik önlemlerini almaları gerekmektedir. Türkiye için PSD2'ye uyum için strateji ve mevzuatsal değişikliklerin yapılması önemlidir. Özellikle Bankacılık Kanunu ile müşteri bilgilerinin üçüncü taraflarla paylaşımı konusunda yasal düzenlemeler mevcut olduğundan, mevzuatın bu doğrultuda uyumlu hale getirilmesi uygun olacaktır.

AB tam üyelik kapsamında, AB müktesabatına uyum kapsamında PSD2'nin ülkemize de geleceği göz önünde tutularak, sistemsel alt yapı ve inovasyonun şimdiden uygun hale getirilmesi, sadece bankacılık sektörü değil AB ile dış ticaret ilişkileri olan ithalat ve ihracatçıların rekabet edebilmesi için de önemlidir. Yaklaşık 170 milyar dolarlık ödemenin Türkiye ve AB ülkeleri arasında sorunsuz, düşük masrafla, PSD2 gereksinimlerine uygun olarak gerçekleştirilmesi, ödemelerde gecikmelerin yaşanmaması ve teknik alt yapının, PSD2'ye uygun olarak düzenlenmesi çok önem taşımaktadır.

Bu nedenle, henüz bir zorunluluk olmasa dahi, ilgili kurumlar tarafından (yasal düzenlemeler için BDDK, Türkiye Bankalar Birliği, bankalar, finans kuruluşları, ithalat ve ihracatçılar birlikleri vb.) şimdiden gereken önlemlerin alınması ile olası sorunların önlenmesi gerektiği önerilmektedir.

Kaynakça

Borgogno, O., & Colangelo, G. (2019). Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs. *Computer Law & Security Review*.

Casu, B., & Girardone, C. (2009). Competition Issues in European Banking. *Journal of Financial Regulation and Compliance*, *17*(2), 119-133.

Colangelo, G., & Maggiolino, M. (2019). From Fragile To Smart Consumers: Shifting Paradigm For The Digital Era. *Computer Law & Security Review*.

Coşkun, F. (2018). Finans Oyuncularına Yeni Oyun Alanı: PSD2. Fintechtime Kış 2018. 25 Mayıs 2019 tarihinde http://fintechtime.com/tr/2018/01/odeme-hizmetleri-direktifi-2-psd2-yururluge-girdi/ adresinden erişildi.

Deloitte. (2017). 'Technology, Media and Telecommunications Predictions 2017'. 25 Mayıs 2019 tarihinde, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf adresinden erişildi.

Donnelly, M. (2016). Payments in the digital market: Evaluating the contribution of Payment Services Directive II. *Computer Law & Security Review*, *32*(6), 827-839.

European Banking Authority. (2015). Regulatory Technical Standards on strong customer authentication and secure communication under PSD2. 25 Mayıs 2019 tarihinde https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 adresinden erişildi.

European Union. (2017). 24.Mayıs.2019 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN adresinden erişildi.

European Union.(2019). The EU in Brief. 24 Mayıs 2019 tarihinde https://europa.eu/european-union/about-eu/eu-in-brief_en adresinden erişildi.

Financial Conduct Authority. (2018). FCA Finalises Revised Payment Services Directive (PSD2) requirements. 25 Mayıs 2019 tarihinde, https://www.fca.org.uk/news/press-releases/fca-finalises-revised-psd2-requirements adresinden erişildi.

Financial Conduct Authority. (2019). FCA Response to European Banking Authority's Opinion on Strong Customer Authentication. 29 Ağustos 2019 tarihinde, https://www.fca.org.uk/news/statements/fca-response-european-banking-authority%E2%80%99s-opinion-strong-customer-authentication adresinden erişildi.

European Union. (2015). Regulation (EU) 2015/751 of the European Parliament and of The Council of 29 April 2015 on interchange fees for card-based payment transactions. 29 Ağustos 2019 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN adresinden erişildi.

Fuster, G. G. (2016). EU Data Protection and Future Payment Services. *In Bitcoin and Mobile Payments* (pp. 181-201). Palgrave Macmillan, London.

Giambelluca, G., & Masi, P. (2016). The Regulatory Machine: An Institutional Approach to Innovative Payments in Europe. In *Bitcoin and Mobile Payments* (pp. 3-25). Palgrave Macmillan, London.

Goode, A. (2018). Biometrics For Banking: Best Practices and Barriers to Adoption. *Biometric Technology Today*, *2018*(10), 5-7.

Johnson, A. (2019). How Biometrics (And Blockchain) Could Save Bricks-And-Mortar Retail. *Biometric Technology Today*, *2019* (3), 8-10.

Mansfield-Devine, S. (2016). Open Banking: Opportunity and Danger. *Computer Fraud & Security*, *2016*(10), 8-13.

Martin, R., Roma, M., & Vansteenkiste, I. (2005). *Regulatory Reforms in Selected EU Network Industries* (No. 28). ECB Occasional Paper. McDowell, B. (2019). Three Ways in Which GDPR Impacts Authentication. Computer Fraud and Security.

Mondaq.com. (2018). European Union: EU Regulatory Technical Standards For Strong Customer Authentication Enter Into Force. 24 Mayıs 2019 tarihinde, http://www.mondaq.com/uk/x/686420/Financial+Services/EU+Regulatory+Technical+Standards+for+Strong+Customer+ Authentication+Enter+Into+Force adresinden erişildi.

Nick Pantlin, 2018, European National News, Computer Law and Security Review

Noctor, M. (2018). PSD2: Is The Banking Industry Prepared? *Computer Fraud & Security*, *2018*(6), 9-11.

Ödeme ve Elektronik Para Derneği (ÖDED). (2017). Avrupa Birliği Ödeme Hizmetleri Direktifi 2. 24 Mayıs 2018 tarihinde https://oded2016.files.wordpress.com/2017/12/oded_avrupa_birligi_odeme_hizmetleri_direktifi_2.pdf adresinden erişildi.

Parker, G., van Alstyne, M., & Choudary, S. (2016). How Networked Markets are Transforming the Economy and How to Make them to Work for You.

Payconiq. (2018). About Us. 25 Mayıs 2019 tarihinde, https://www.payconiq.com/en/about-us/ adresinden erişildi.

Politou, E., Alepis, E., & Patsakis, C. (2019). Profiling Tax and Financial Behaviour With Big Data Under the GDPR. *Computer Law & Security Review*.

Porcedda, M. G. (2018). Patching the Patchwork: Appraising The EU Regulatory Framework On Cyber Security Breaches. *Computer Law & Security Review*, *34*(5), 1077-1098.

Price Water House. (2017). Waiting until the Eleventh Hour European banks' reaction to PSD2. 25 Mayıs 2019 tarihinde https://www.pwc.com.tr/payment-services-europe adresinden erişildi.

Soland, B. (2017). Second Payment Services, 25 Mayıs 2019 tarihinde, https://www.nexusgroup.com/blog/psd2-second-payment-services-3-minutes/ adresinden erişildi.

Steennot, R. (2018). Reduced Payer's Liability For Unauthorized Payment Transactions Under The Second Payment Services Directive (PSD2). *Computer Law & Security Review*, *34*(4), 954-964.

Steve Cook, (2017). Selfie Banking: Is It A Reality?, Biometric Technology Today.

Tengur, S. (2017) PSD2: Understanding the new payments regulation in Europe. 25.Mayıs.2019 tarihinde https://blogs.sas.com/content/sascom/2017/08/18/psd2-demystifying-beast/ adresinden erişildi.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research*, *21*(4), 675-687.

Van de Ven, A.H. (2005) "Running in Packs to Develop Knowledge Intensive Technologies." MIS Quarterly, 29, 365–378.

Verizon Report. (2017). 'Data Breach Investigations Report 2017'. 25 Mayıs 2019 tarihinde https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/ adresinden erişildi.

Wolters, P. T. J., & Jacobs, B. P. F. (2019). The Security of Access to Accounts Under the PSD2. *Computer Law & Security Review*, *35*(1), 29-41.

Yüksel, S., Dinçer, H., & Meral, Y. (2019). Financial Analysis of International Energy Trade: A Strategic Outlook for EU-15. Energies, 12(3), 431.

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