AÇIK BANKACILIK RİSKLERİ

Açık Bankacılık ve Müşteri Verilerinin Paylaşılması

Hilal Durmaz
Hilal.durmaz@sabanciuniv.edu

İçindekiler

Tanım ve Kısaltmalar

Kısaltma	Tanım	Açıklama	İngilizce Tanım	İngilzice Kısaltma
HHS	Hesap Hizmeti Sağlayıcı	Nezdinde ödeme hesabı bulunan ödeme hizmeti sağlayıcısı; banka,ÖDK, EPK, PTT gibi.	Account Servicing Payment Service Provider	ASPSP
ÖBHS	Ödeme Emri Başlatma Hizmeti Sağlayıcı	Kanunun 12 inci maddesinin birinci fıkrasının (f) bendinde tanımlanan ödeme hizmetini (ödeme emri başlatma hizmetini) sunan tüzel kişi	Payment Initiation Service Provider	PISP
HBHS	Hesap Bilgisi Hizmeti Sağlayıcı	Kanunun 12 inci maddesinin birinci fıkrasının (g) bendinde tanımlanan ödeme hizmetini (hesap bilgisi hizmetini) sunan tüzel kişi	Account Information Service Provider	AISP
YÖS	Yetkili Ödeme Hizmeti Sağlayıcılar	Ödeme emri başlatma hizmeti ve/veya hesap bilgisi hizmeti sunan tüzel kişiliklerin genel adı.	Third Party Payment Service Providers	TPP
GKD	Güçlü Kimlik Doğrulama	Kimlik doğrulamada kullanılan ve bir bileşenin ele geçirilmesinin diğer	Strong Customer Authentication	SCA

		bileşenin güvenliğini tehlikeye atmayacağı en az iki bileşenden oluşan, bu iki bileşenin de müşterinin bildiği, sahip olduğu veya biyometrik bir karakteristiği olan unsur sınıflarından farklı ikisine ait olacak şekilde seçildiği yöntem		
ÖHK	Ödeme Hizmeti Kullanıcısı	Gönderen, alıcı veya her ikisi sıfatıyla belirli bir ödeme hizmetinden faydalanan gerçek veya tüzel kişi	Payment Service User	PSU
ÖH	Ödeme Hesabı	Ödeme hizmeti kullanıcısı adına açılan ve ödeme işleminin yürütülmesinde kullanılan hesabı	Payment Account	PA
İDK	İşlem Doğrulama Kodu	Kimlik doğrulama yöntemlerinden biriyle kendisini sisteme tanıtan bir müşterinin gerçekleştirmek istediği işleme özgü olmak ve belirli bir geçerlilik süresi içinde işlem onayında kullanılmak üzere oluşturulan, işlemin niteliğine bağlı olarak kişiye onay anında ilgili işlem bilgisi ile birlikte gösterilen, alıcı veya tutarın değişmesiyle geçersiz hale gelen bilgi	Authentication Code (Dynamic Linking)	AC

(Öztaner, 2021)

1.Giriş

Teknolojinin gelişmesi tüm alanlara olduğu gibi bankacılık alanında da önemli gelişmelere yol açmıştır. Bill Gates'in, "Bankacılık lazım, fakat artık bankalara ihtiyacımız yok" sözü tam olarak da günümüzdeki müşterilerin bankacılık deneyimini açıklamaktadır. Müşteriler şubelere gitmeden ATM/İnternet/Mobil kanallar üzerinden bankacılık işlemelerini kolay ve hızlı yöntemler ile tamamlayabilmektedir. Birden çok bankada hesabı olan müşteriler için ise bu durum daha fazla zaman almaktadır çünkü her bankanın uygulaması ayrıdır. Müşterilerin bankacılık deneyimini iyileştirmek için dünyada ve Türkiye'de "Açık Bankacılık" kavramı ortaya çıkmıştır böylece müşterilerin tüm bankalardaki bilgiler tek bir uygulama altında toplanabilecektir. Açık Bankacılığı basitçe tanımlamak gerekirse bir müşterinin bir ödeme kuruluşunun uygulamasından diğer kuruluşlardaki hesap bilgilerine erişim sağlayabilmesi ve para transferi gerçekleştirmesidir. Açık Bankacılık ile Açık Veri diyebiliriz. Peki Dünyada bu sistem nasıl karşılanıyor? Bilgi güvenliği ihlali sağlanıyor mu? Hukuksal boyuttaki değerlendirmeler neler? Türkiye' Açık Bankacılık için nasıl aksiyon alıyor?

2. Açık Bankacılık 'ta API Kullanımı

Açık bankacılığın bel kemiği olarak API'leri gösterebiliriz. API sisteminin nasıl işlediğini benzetme yaparak şöyle bir örnek ile açıklamak mümkündür. Sipariş verebileceğiniz bir menüyle bir restorandaki bir masada oturduğunuzu varsayın. Mutfak, siparişinizi hazırlayacak "sistem"in bir parçasıdır. Eksik olan şey, siparişinizi mutfağa iletecek ve yiyeceğinizi masanıza geri teslim edecek kritik bir bağlantıdır. Garson ya da API burada devreye girmektedir. Garson ya da API, siparişleri alan ve mutfağa yani sisteme ne yapacağını söyleyen aracıdır. Sonrasında garson cevabı size geri iletir, bu örnekte cevap, yiyecek ve içecekler olmaktadır (İşNet, 2021)

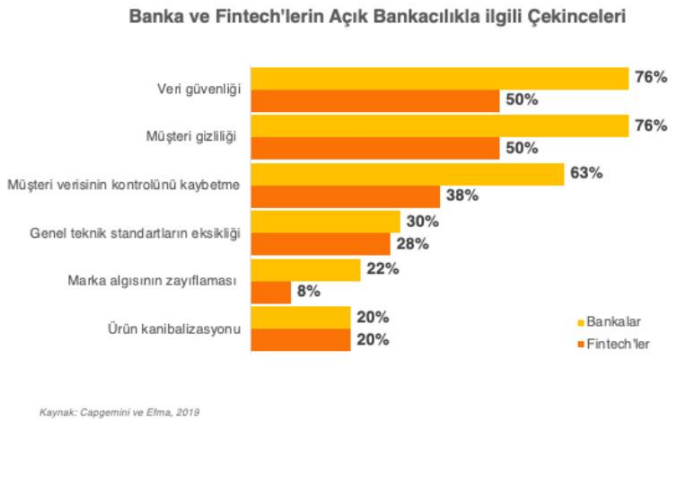
Günümüzde API uygulamaları veri alışverişine uygun, işlevsel ve güvenliğe dayalı iş modelleriyle ekonomik ve finansal süreçlere hâkim olmuştur. API'ler sayesinde bankacılık faaliyetlerinde entegrasyon, hız ve üçüncü şahıs sağlayıcılarla ortaklık unsurları ön plana çıkmıştır (Coste & Miclea, 2019) Bankalar kendi ödeme uygulamalarını ya da bankacılık hizmetlerini diğer ödeme kuruluşlarına API'ler sayesinde sunmaktadır. Kullanımları yasal düzenlemeye Avrupa Birliği tarafından tabi tutulmuştur.2015 yılında yayınlanan bu yasal düzenlemenin amacı, mobil bankacılık ve elektronik ödeme hizmetlerinin giderek yaygınlaşması ve müşteri taleplerine yeterince karşılık verilememesi, güvenlik açıklarının ortaya çıkması ve müşteri

memnuniyetsizliğin oluşması. Bu sorunların giderilmesi için PSD2 (Payment Service Directive) yayınlanmıştır ve Avrupa Birliği Ülkelerinin 2018 yılına kadar API hizmeti sağlayabilir hale gelmesi zorunlu olmuştur. Fakat verilen ödeme hizmetleri yetkisi geri alınabilmektedir bunun amacı Avrupa Birliği kurumlarına güvenin sağlanmasıdır.

Fintek kuruluşları API'ler sayesinde ödeme hizmetlerinde ciddi bir pazar payına sahip olma yolunda ilerliyorlar. Bugün sokakta ve televizyonlarda reklamını gördüğümüz "Papara" uygulaması aslında bankaların API'lerini kullanarak müşterinin ödeme ve fatura işlemlerini gerçekleştirmektedir. Örneğin bir müşteri Papara uygulaması üzerinden bir kişiye para göndermek istediğinde İş Bankası API'si üzerinden işlem yapılıyor ve müşterinin bilgileri banka ile paylaşılmış oluyor. Fakat müşteri sadece Papara uygulamasını bilmektedir. Gönderici ve alıcı bilgilerinin banka ile paylaşıldığının kaç müşteri farkındadır?

API'lerin çalışma mantığı tamamen bilgi paylaşımına dayanmaktadır. Açık bankacılık 'ta API'ler önemli rol oynamaktadır. (Sivathanu, 2019) Açık bankacılığın Hindistan'daki etkilerini 945 müşteri üzerinde uygulanan anket ile "Teknoloji Hazırlık ve Kabul" modeli bağlamında incelemiştir. Ankete katılan kişiler güvenlik konusunda endişeliyken uygulamaya ise daha ılımlı yaklaşmıştır. Müşterilerin bilgilerini güvende tutmak ve onlara güven sağlamak ödeme kuruluşları için öncelikli olmalıdır. Birçok kuruluş açık bankacılığın getirdiği avantajları kara dönüştürme hedefine girerek güvenlik riskini geri plana atmamalıdır. API'lerde toplanan geçmiş verilerin analiz edilmesi suretiyle, müşterilerin bankacılık işlemleri çerçevesindeki alışkanlıkları ve eğilimleri tespit edilebiliyor. Böylece, söz konusu müşteriye özel tekliflerin sunulabilmesi ve piyasada müşterinin ihtiyaçları doğrultusunda hazırlanan yeni bankacılık ürünlerinin aktif hale getirilmesi mümkün olabiliyor. (Kolcuoğlu, 2021)Ödeme kuruluşları API'ler sayesinde müşterinin diğer bankalardaki bilgilerini erişebilecek; bu durum müşterini daha iyi tanımasını ve onlara yeni kampanyalar sunmasını sağlayacaktır.

Akbank geliştirdiği API'lerini hizmete açan ilk banka olurken Türkiye İş Bankası en geniş bankacılık hizmetini sunmaktadır. Şu an dünyada ve Türkiye'de ödeme kuruluşları açık bankacılık sistemine geçiş için API geliştirmek onları kullanıma açmaya çalışmaktadır. Fakat müşterilerin olduğu kadar bankaları ve fintek kuruluşlarının da çekinceleri bulunmaktadır. Yapılan araştırmaya göre bankalar ve fintk kuruluşlar en fazla veri güvenliğini ve müşteri gizliliğinin sağlanması, müşteri verisinin kontrolünü kaybetme konusunda çekinceler yaşamaktadır.



[1]

Ödeme kuruluşlarının yaşadığı çekincelerden dolayı müşteri verilerinin ne kadar açacakları ve aldıkları bilgi paylaşım kararları onların piyasadaki durumlarını belirleyecektir. Bankaların geliştirdiği API'ler müşterilerin bilgilerini paylaşmasına göre ayrılmaktadır. Price water house Coopers'ın (PWC) (2017) raporunda bankaların açık bankacılık stratejileri ortaya konmuş ve bankalar açıklık seviyeleri ile yarattıkları değerlere göre aşağıdaki dört sınıfa ayrılmıştır:

• Asgari seviyedeki açıklık, düşük katma değer ve PSD2 ile düşük uyum (Uyumluluk).

• Düşük açıklık ve geliştirilen yeni hizmetlerle sağlanan işlevselliğin ortaya çıkardığı yüksek katma değer(Rekabetçilik).

• Üçüncü taraf sağlayıcılarla tam uyum sonucunda gerçekleşen maksimum açıklık ve düşük değer önerisi(Yayılmacılık).

• Açık bankacılık ekosistemiyle gerçekleşen gelişmiş veri ve bilgi paylaşımıyla sunulan tam açıklık ve yüksek değer teklif (Dönüşümcülük) (ŞAHİN & CANTÜRK, 2020)

Açık Bankacılık Riskleri ve Güvenlik Önlemleri

Açık bankacılık bankalara sunduğu avantajlarla birlikte riskleri de beraberinde getirmektedir. Ödeme işlemlerinde üçüncü taraf sağlayıcılar yer alacaktır bu nedenle banka müşterileri ile iletişim kurabilecek ve yeni teklifler sunabilecektir. Müşteri tarafından bakıldığında iyi olsa da bankalar için önemli bir gelir kaybına sebep olabilir. 7192 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları hakkında olan kanunlarda değişiklik yapılmıştır. Bu değişikliklerden biri de Türkiye Ödeme ve Elektronik Para Kuruluşları Birliğinin

[1] https://webrazzi.com/2019/12/11/acik-bankacilik-neler-vadediyor/

kurulmasına karar verilmiştir. Birliğin görev ve yetkileri temel olarak mesleğin gelişmesini sağlamak amacıyla eğitim, tanıtım ve araştırma faaliyetlerinde bulunmak, üye kuruluş mensuplarının uyacakları meslek ilkeleri ve standartlarını belirlemek, üyeleri arasında haksız rekabeti önlemek amacıyla gerekli her türlü tedbiri almak ve uygulamak, üyelerin ilan ve reklamlarında uyacakları esas ve şartları tür, şekil, nitelik ve miktar itibarıyla tespit etmek, üyeler ve bireysel müşterileri arasındaki ihtilafların değerlendirilmesi ve çözüme kavuşturulmasını temin etmek üzere hazırlayacağı ve Bankaca onaylanan usul ve esaslar dâhilinde hakem heyeti oluşturmak ve Kanunda sayılan diğer görevleri yerine getirmektir. (ŞAHİNER, 2021)

Müşteri verilerinin paylaşılması güvenlik açığı oluşturacaktır ve kötü niyetli yazılımların saldırısı daha fazla olacaktır. Müşterilerin bankalara olan güvenleri zedelenecektir. Müşteriler için yasadışı veri kullanımı, giriş bilgilerine erişilmesi, kişisel verilerin gizliliği risk oluşturacaktır. Açık bankacılık uygulamaları geçişinde bankaların güvenlik konusunda PSD2'da yer alan maddelere dikkat etmesi gerekmektedir. Köklü bankalar anasistem üzerinden hizmet vermektedir açık bankacılık uygulamalarına entegre olabilmeleri için açık sisteme geçmeleri ve altyapısal dönüşümü tamamlamalıdır.

BDDK tarafından yayınlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te müşterilerin veri paylaşımı ile ilgili önemli maddeler yer almaktadır. Açık Bankacılık uygulamalarında müşteriden yazılı şekilde ya da kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte bir talep alınmasını zorunlu hale getirmiştir açık rıza kabul edilmemektedir. Güçlü kimlik doğrulama yapılması da zorunlu hale getirilmiştir. SCA (Strong Customer Authentication), müşterinin bir tanesinin açığa çıkması durumunda diğerlerinin güvenilirliğine zarar getirmeyecek şekilde bildiği, sahip olduğu veya biyometrik karakteristiği olan birbirinden bağımsız iki ya da daha fazla farklı eleman ile bu doğrulama elemanlarının gizliliğini koruyacak biçimde doğrulanmasıdır. Esasında BDDK'nın yönetiminde olan çeşitli bankacılık mevzuatlarında da yer alan ve "iki faktörlü kimlik doğrulama" olarak tanımlanan bir piyasa standardı olarak düşünülebilir. (Aktaş, 2021)

Müşterilerin veri güvenliği aslında sistemin ve tarafların güvenilir olması ile başlamaktadır. Ödeme Hizmetleri Veri Paylaşım Servisleri kapsamında TCMB tarafından verilen yetkilendirme kodu ve kuruluşu türü bilgilerini içeren elektronik sertifikalar kullanılır. Bu sertifikalar BKM API geçidi kullanımı sırasında YÖS ve HHS'lerin kimlikliklerinin doğrulanması için kullanılmaktadır.

Türkiye'de Açık Bankacılık Sistemi

Merkez Bankası 12 Kasım 2019'da güncellenen "6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" un 12nci maddesi ile PSD2'de bulunan "**Ödeme Emri Başlatma Hizmeti**" ve "**Hesap Bilgisi Hizmeti**" için belgeler yayınlaşmış ve katılımcıları bilgilendirmiştir.

Yetkili ödeme hizmet sağlayıcıları (YÖS) aslında üçüncü taraf hizmet sağlayıcıları olarak da geçer; ödeme hizmet kullanıcılarının ödeme ve hesap bilgileri servisine erişmesine olanak sağlamaktadır. Bu kapsamda iki tane YÖS bulunmaktadır **Ödeme Emri Başlatma** ve **Hesap Bilgisi Sağlayıcı Hizmeti.**

Bir banka uygulamasından diğer bankadaki hesaplara erişim sağlanabilmesi için müşterinin açık rızası alınması gerekmektedir. Örneğin: müşteri İş Bankası uygulamasına giriş yaptığında Akbank'taki hesaplarına erişim sağlamak istediğinde erişim izni vermeli ve erişimin bitiş tarihini belirlemelidir. Hangi bilgilere erişim sağlanacağı müşteri tarafından seçilmelidir bakiye, hesap bilgisi, hesap hareketi gibi. Müşterinin rızası alındıktan sonra Akbank uygulamasına yönlendirilecek ve erişim iznine tabi olan hesaplarını seçebilecektir. Akbank uygulamasında seçim işlemleri tamamlandığında tekrar İş Bankası uygulamasına geri dönülecek ve işlemlerine devam edebilecektir. Peki bu akış ne kadar güvenli?

Finansal hizmetler açısından bakıldığında, açık bankacılık sisteminde müşterinin hizmet aldığı bankanın internet ya da mobil bankacılığı üzerinden giriş yapabilmesi için şifresini ve kullanıcı bilgilerini üçüncü şahıslarla paylaşılacağından veri güvenliğinin sabote edilmesi durumunda ve banka işletmelerinin şüpheli işlemleri ayırt etmesinin zorlaşması gibi önemli ölçüde güvenlik kaygılarını ortaya çıkarmaktadır. Bununla birlikte birçok ülkede açık bankacılık sistemi kullanılmaya devam edilmektedir (Basel Committee on Banking Supervision, 2019)

Bir uygulamadan diğer bir uygulamaya geçerken müşterinin kimliğini doğrulamak için giriş yapması gerekmektedir. BKM API geçişi kullanılmaktadır bu geçiş sırasında sertifikasyon / yetki / kayıt kontrolü yapılmaktadır. API katmanının temel prensipleri bulunmaktadır.

- HHS tarafından sunulan ödeme hizmetleri veri paylaşım serilerini kullanan yetkilendirilmiş ödeme hizmet sağlayıcıların TCMB tarafından ilgili ödeme hizmeti için yetkilendirilmiş olduğu kontrol edilir.

- HHS ve yetkilendirilmiş ödeme hizmet sağlayıcılar arasında bağlantı uçtan uca güvenli bir şekilde sağlanır. Bu amaçla iletim katmanında TLS (asgari 1.2 sürümü) ile şifreli iletişim sağlanır.

- Uçtan uca güvenli iletişim, mesaj şifreleme ve mesaj imzalama işlevleri nitelikli elektronik sertifikalar kullanılarak sağlanır. (Öztaner, 2021)

Ödeme Hizmetleri Yönergesi (PSD2)

Yönerge, üye devletlere, kuracakları yahut belirleyecekleri yetkili makamlar eliyle ödeme hizmet sağlayıcıları üzerinde kontrol ve gözetim (337/35 sayılı Ödeme Hizmetleri Yönergesi m.23) imkânı sağlamaktadır. Bu durum müşteri açısından güvenin ve memnuniyetin sağlanmasına da yol açacaktır. Örneğin, Merkez Bankası diğer bankaları kontrol etmektedir ve sorun olması durumunda parasal ceza yaptırımı bulunmaktadır. Açık Bankacılık 'ta ise BKM tarafından diğer ödeme kuruluşları API güvenlik katmanı ile kontrol ve gözetimde olacaktır. Peki sistemsel güvenliğin sağlanması müşteriler için yeterli olacak mıdır? Açık bankacılığın esasında müşteri verilerinin API'ler sayesinde üçüncü kuruluşlarla paylaşılarak işlemlerin yapılmasının sağlanmasıdır. Fakat bu durum Bankacılık Kanunu ile ters düşmektedir. 5411 sayılı Bankacılık Kanunu'nun "Sırların Saklanması" başlıklı 73. maddesinde açıkça "Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tâbidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder." denilmektedir. Bankaların birbirleri ile müşteri verisi paylaşması durumunda gizlilik sözleşmesi imzalanması gerekirken Açık Bankacılık için yayınlanan yürürlükte bir böyle bir anlaşma bulunmamaktadır. BDDK tarafından yayınlanan BANKALARIN BİLGİ SİSTEMLERİ VE ELEKTRONİK BANKACILIK HİZMETLERİ HAKKINDA Yönetmelik'te Açık Bankacılık tanımı "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" olarak yer almaktadır. Burada ödeme hizmeti başlatma faaliyeti çıkarımı yapılırken hesap bilgilerinin paylaşılması veya birden çok bankadaki bilgilerin tutulması kısmı yer almamaktadır. Kişisel Verilen Korunması Kanunu 'da açık bankacılık ile ters düşmektedir çünkü

bankalar müşterilerden açık rıza alsa dahi müşterinin ayrıca bir talimat vermesi gerekmektedir. Fakat açık bankacılık kapsamında sadece müşterinin açık rızasından bahsedilmektedir. Bu talimata dair yayınlanmış herhangi bir belge taslağı bulunmamaktadır. Diğer bir problem ise, açık bankacılık dünya çapında uygulamaya geçiyor bu nedenle müşteriler sadece Türkiye'deki hesaplarını değil yurt dışındaki bankaların hesaplarını da tek bir uygulama üzerinden kullanabilmelidir fakat bankacılık kanuna göre müşteri verilerinin yurt dışına aktarılması ve oradaki ödeme kuruluşları ile paylaşılmasına ilişkin özel düzenlemeler bulunuyor. (KOLCUOĞLU, 2021) Bilgilerin yurt dışına açılması ayrı bir konuyken Türkiye'de yaşayan yabancı uyruklu müşteriler içinde ayrı bir sorun bulunuyor. Kimlik kontrollerinde TCKN/VKN/YKN kimlik tipleri bulunmaktadır. Ama ülkemizde yaşayan birçok yabancı müşteri yabancı kimlik numarasına sahip değildir ve pasaport numarası ile müşteri olabilmektedir. Bu durumda bu müşteriler açık bankacılık uygulamasını kullanamayacaktır.

Bankadaki müşteri verileri app'ler sayesinde diğer ödeme kuruluşlarına açılması durumunda artık verinin sahipliği kimde olacağı da açık noktalardan biri. Müşterinin hesap bilgileri çalındığında, hesabından izinsiz para girişi/ çıkışı olması durumunda burada sorumlu hangi ödeme kuruluşu olacaktır? Zira aynı verinin birden çok kişi tarafından işlendiği kompleks veri işleme faaliyetlerinde kurumlar, kendilerini veri sorumlusu olarak görmeme eğilimindedir (Article 29 Working Party, 2010)

3.Sonuç

Açık bankacılık hizmetinden yararlanmak isteyen müşterilerin verilerini de açması gerekmektedir fakat bunun sınırı ve bu işlemin sonuçları nelerdir müşteriler tarafından bilinmemektedir. Bu konuda bankaların ve ödeme kuruluşlarının alabileceği en iyi aksiyonlar yürürlükteki maddelere uygun sistemlerini geliştirmeleri ve müşterilere daha fazla bilgi verilmesidir. BDDK tarafından yayınlanan yönetmelik ve Avrupa birliği tarafından yayınlanan ödeme hizmetleri direktifleri müşteri verilerinin korunması ve dolandırıcılığa karşı önlemlere ağrılık vermiştir. PSD2'ya göre Ödeme başlatma hizmeti sağlayıcısı: "ödeme hizmeti kullanıcısının hassas ödeme verilerini saklamamak" ile yükümlüdür aynı şekilde hesap bilgileri hizmet sağlayıcısı "veri koruma kurallarına uygun olarak, ödeme hizmeti kullanıcısı tarafından açıkça talep edilen hesap bilgileri hizmetini sunmak dışında başka amaçlar için herhangi bir veriyi kullanmamak, bunlara erişmemek veya depolamamak." Maddesini yerine getirmek ile yükümlüdür. (Ödeme ve Elektronik Para

Derneği(ÖDED), 2021) Kısacası bütün yönetmelikler müşteri verilerinin güvenliğini sağlanması için açık ve net maddeler içermektedir. Bu yükümlülükleri yerine getirmeyen kuruluşlara yaptırım ve para cezası uygulanmaktadır. TCMB tarafından uygulanacak olan ceza yeni Kanun'la beraber 6493 sayılı Kanun'da yer alan idari para cezası tutarları yeniden değerleme oranı göz önünde bulundurularak güncellenmiş ve 20.000TL- 500.000TL'den 40.000TL- 900.000TL'ye çıkarılmıştır. (Deniz, 2019) bunlardan en ağır ceza itibar kaybıdır. Günümüzde sosyal medya sayesinde bir müşterinin başına gelen kötü bir deneyim anında birçok kullanıcı tarafından öğrenilmektedir. Bu nedenle açık bankacılık gibi karmaşık ve insanlara güven verilmesi gereken bir uygulamada ufak bir güvenlik açığı ya da müşteri memnuniyetsizliği ödeme kuruluşunun çok fazla müşteri kaybetmesine neden olacaktır.

Bankalar ve fintek kuruluşları yönetmeliğe uyum sağlamak ve gelişen teknolojinin gerisinde kalmamak için API'lerini geliştirmeye çalışmaktadır. Açık bankacılıkta kullanılan API'ler token'lar sayesinde daha güvenilir bir bilgi alışverişi gerçekleşecektir. Güçlü kimlik kontrolü ile de müşteri bilgileri kontrol edilecektir. Türkiye'de yaklaşık 1 yıl içerisinde tüm bankaların açık bankacılık uygulaması devreye girecektir. Dünyada da çalışmalar devam etmektedir.

Kaynakça

Aktaş, M. (2021, Eylül 03). *PSD2 Strong Customer Authentication (SCA) — Güçlü Müşteri Doğrulaması — 1*. Mustafa Aktaş: https://mustafa-aktas.medium.com/psd2-strong-customer-authentication-sca-g%C3%BC%C3%A7l%C3%BC-m%C3%BC%C5%9Fteri-do%C4%9Frulamas%C4%B1-1-cdebecc0fef1 adresinden alındı

Article 29 Working Party. (2010). Opinion 1/2010 on the concepts of “controller” and “processor”. s. 13.

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

Coste, R., & Miclea, L. (2019). API Testing for Payment Service Directive2 and Open Banking. *International Journal of Modeling and Optimization*, 8.

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

İşNet. (2021, Eylül 2). https://www.isnet.net.tr/BlogIcerik/api-nedir-isnet-blog adresinden alındı

Kolcuoğlu, A. (2021, Nisan 26). *Açık Bankacılık*. Dünya: https://www.dunya.com/kose-yazisi/acik-bankacilik/619071 adresinden alındı

KOLCUOĞLU, A. U. (2021, Mayıs 25). *DUNYA*. https://www.dunya.com/kose-yazisi/acik-bankacilik-mevzuati-ve-kisisel-verilerin-korunmasi/622237 adresinden alındı

Ödeme ve Elektronik Para Derneği(ÖDED). (2021, Eylül 06). *ÖDED*. https://oded.com.tr/psd-2/ adresinden alındı

Öztaner, S. M. (2021, Ağustos 25). Ödeme Emri Başlatma ve Hesap Bilgisi Hizmetleri API Standartları.

Sivathanu, B. (2019, JULY). An Empirical Study on the Intention to Use Open Banking in India. *Information Resouces Management Journal*, 27-47. https://scholar.google.com/scholar?start=0&q=hukuk+ve+teknoloji&hl=en&as_sdt=0,5 adresinden alındı

ŞAHİN, B. Ş., & CANTÜRK, B. C. (2020, Eylül 17). Türkiye’deki Hukuki Altyapı ve Ödeme Hizmetleri Yönergesi 2 Bağlamında API Teknolojisi ve Açık Bankacılık. s. 21.

ŞAHİNER, A. D. (2021, eylül 3). *GKS LEGAL*. GKS LEGAL HUKUK BÜROSU: https://www.gkslegal.com/acik-bankacilik-ve-psd2/ adresinden alındı