BANKALARCA KULLANILACAK UZAKTAN KİMLİK TESPİTİ YÖNTEMLERİNE VE ELEKTRONİK ORTAMDA SÖZLEŞME İLİŞKİSİNİN KURULMASINA İLİŞKİN YÖNETMELİK

1. Giriş

01.04.2021 tarihli Resmî Gazete'de yayımlanan ve 01.05.2021 tarihinde yürürlüğe giren Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik ("**Yönetmelik**") amaç ve kapsamı, birinci maddesinde düzenlendiği üzere *bankalar tarafından **yeni müşteri kazanımında** kullanılabilecek uzaktan kimlik tespiti yöntemlerine ve müşteri kimliğinin tespit edilmesini müteakip sunulacak bankacılık hizmetlerine yönelik olarak mesafeli olsun olmasın **bir bilişim veya elektronik haberleşme cihazı üzerinden yazılı şeklin yerine geçecek şekilde** ya da mesafeli olarak sözleşme ilişkisinin kurulmasına yönelik usul ve esasları düzenlemek* olarak belirlenmiştir. Bu kapsamda Yönetmelik kapsamında getirilmiş olan yeniliğin yeni müşterilere yönelik olduğu anlaşılmaktadır.

Uzaktan Kimlik Tespiti yönteminin Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile Kişisel Verilerin Korunması Kanunu ("**KVKK**") öncelikli olmak üzere mevzuatta yer alan hükümler saklı kalmak kaydıyla uygulanacağını düzenlemiştir.

2. Uzaktan Kimlik Tespiti Süreci Kurgusu

Yönetmelik m.4 kapsamında uzaktan kimlik tespitinin tanımı yapılmış, yöntemin **asgari seviyede risk içerecek şekilde tasarlanması gerekliliği** vurgulanmış ve görüntülü görüşme yöntemindeki güvenlik önlemlerinin alınmasından söz edilmiştir.

Buna göre **süreç tek kişi tarafından yönetilemeyecek**, süreç başlatıldıktan sonra birtakım kontrollere tabi tutulup onay ve ek kontroller doğrultusunda tamamlanacak **üç aşamalı bir sistem** kurgusu öngörülmüştür. Buna göre süreç*; (i) Kişi tarafından sürecin başlatılması, (ii) bilgi teknolojileri tarafından uygulanan kontroller ile devam ettirilmesi, (iii) müşteri temsilcisi tarafından yapılacak onaylama ve ek kontroller ile tamamlanması,* şeklinde özetlenmiş, **müşteri temsilcisi tarafından yapılan kontrollerde işlemin riskli bulunması halinde ikinci bir onaya gönderileceği veya sonlandırılacağı düzenlenmiştir.**

*Uzaktan Kimlik Tespitine ilişkin süreçler yürütülürken "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ("**BSEBY**") oluşabilecek herhangi bir risk faktörü veya güvenlik açığı konusunda hali hazırda mevcut bulunduğundan işbu Yönetmelik'te aynı konuyla ilgili ayrıca bir düzenlemeye gerek duyulmamıştır. BSEBY'nin "uzaktan kimlik tespiti ve üçüncü tarafa güven" başlıklı 43.maddesi bağlamında finansal hizmetlerde (bankacılık işlemleri, kredi kartı vd.) uzaktan iletişim araçlarıyla mesafeli sözleşmelerin kurulması, **uzaktan kimlik tespiti** ve üçüncü tarafa güven kapsamındaki uygulamaların gereklerine yönelik BDDK'nın ikincil mevzuatı ve Mali Suçları Araştırma Kurulu Başkanlığı (MASAK) düzenlemeleri ile 01.01.2021 tarihinden itibaren gündelik hayatımıza girmişti. Dolayısıyla bu Yönetmelik kapsamında getirilen yenilik yeni kazanılacak müşteriler açısından önem arz etmekte olup söz konusu güvenlik tedbirleri halihazırda alınmış ve uygulanmaktaydı.*

Uzaktan kimlik tespitini yapacak müşteri temsilcisi ve çalışma ortamı başlıklı m.5 uyarınca görüntülü görüşme aşaması bu konuda **eğitim almış müşteri temsilcileri** tarafından gerçekleştirilecek ve eğitim sonucunda temsilcilerin herhangi bir güvenlik ihlali ihtimali söz konusu olduğunda ilgili eylemlere karşı **yönetmelik ve mevzuat kapsamında bilgi sahibi olması beklenecektir.** Bu eğitimler **yılda en az bir defa**, konu ile ilgili herhangi bir güncelleme ve değişiklik olması durumunda da harici olarak yapılacaktır. Madde kapsamında verilmesi gereken eğitimler ayrıntılı olarak düzenlenmiştir ancak eğitim kalemleri **sınırlı sayı prensibiyle sayılmamış** olup özellikle verilmesi gerekli olan eğitimler (*bkz. 7. Fıkra: engelli kişilere hizmet verebilmek amacıyla gerekli eğitimlerin verilmesi sağlanır)* vurgulanmıştır.

Sürecin başlatılması ile uyulması gereken genel ilkeler başlıklı m.6 uyarınca bir ön-başvuru düzenlenmiştir. Görüntülü görüşme öncesi **elektronik ortamda doldurulan bir form** aracılığıyla başvuran hakkında bir risk değerlendirilmesi gerçekleştirilecek, değerlendirme sonucunda gerekiyorsa görüntülü görüşme başlatılmadan süreç sonlandırılacaktır. Yine bu madde uyarınca kişinin **"özel nitelikli kişisel veriler"** kategorisinde yalnızca **biyometrik veri kategorisine ait kişisel verilerinin** kullanılabileceği ve buna dair açık rızasının kayıt altına alınacağı düzenlenmiştir. **Hüküm özel nitelikli kişisel verilerin açık rıza olmaksızın işlenemeyeceğini ve biyometrik verinin bunlardan biri olduğunu düzenleyen KVKK m.6 ile de desteklenmektedir.**

Aynı maddenin beşinci fıkrası uyarınca görüntülü konuşmanın niteliği "*… gerçek zamanlı ve kesintisiz şekilde yapılır. Müşteri temsilcisi ile kişi arasındaki görsel-işitsel iletişimin bütünlüğünün ve gizliliğinin yeterli seviyede olması sağlanır. Bu amaçla, yapılan görüntülü görüşme uçtan uca güvenli iletişim ile gerçekleştirilir.*" şeklinde şarta tabi tutulmuştur. Devamla görüntü ve ses kalitesi, beyaz ışık şartı, cep telefonu numarası doğrulama ve belgenin durumu da ayrıntılı olarak düzenlenmiştir.

"Kullanılabilecek kimlik belgesi ve doğrulanması" başlıklı m.7 kapsamında özetle; kullanılacak kimlik belgesinin niteliğinin **"temassız yonga"** olarak bahsedilen terimin daha yaygın kullanımı olan **"çip"** terimini ifade ettiği, bu kapsamda **yakın alan iletişimi**nin kullanıldığı, kimlik belgesinin doğrulanırken izlenecek yol haritası ve bu sırada müşteri temsilcisinin izlemesi gereken adımların oldukça detaylı şekilde düzenlendiği söylenebilecektir. Bu maddeye göre **eski kimlik belgesiyle uzaktan kimlik tespiti yapılamayacak** olup, yeni kimlik belgelerinde bulunan birtakım teknolojik gelişmelerden yararlanılacağı açıktır. Optik karakter okuma yöntemleri kullanılarak ulaşılan **MRZ (Machine Readable Zone – Makine Tarafından Okunabilir Bölge)** bu gelişmelere örnek teşkil etmektedir.

Kimliği tespit edilecek kişinin doğrulanması başlıklı m.8/1 uyarınca **sahte yüz teknolojisine** dair riskleri önlemeye yönelik ilave tedbirler alınacağı düzenlenmiştir. **Madde incelendiğinde alınacak tedbirlerin kişinin yalnızca "canlılık" açısından mı tespit edileceği çok anlaşılmamaktır.** Görüşme sırasında karşıdaki kişinin canlı olarak orda bulunması veya bir video gibi görsel iletişim mekanizmalarının mı kullanıldığının ayırt edilmesi için önlem alınacağı açıktır. Ancak bugünün teknolojisinde "sahte yüz" yalnızca bu yolla yapılmamaktadır.

> ***Deepfake teknolojisi*** *ile yapay zekanın kişinin dudak hareketleri ve mimiklerine kadar öğrenip algoritma oluşturarak aslında var olmayan yepyeni videolar ortaya çıkarması geçmişte çok olanaksız görünse de bugünün gerçeğini teşkil etmektedir. Global basında sayısız makalenin yayınlandığı deepfake konusu modern dünyanın en büyük tehditlerinden biri olarak görülmektedir. Ucuz bir teknoloji olmasının yanı sıra deepfake'i özel olarak belirleyen bir hard-data (somut veri) bulunmadığından tespiti oldukça zordur. Öyle ki; deepfake fenomeni, inanç yaratmak için imgelerin, seslerin ve videonun psikolojik gücü nedeniyle çok tehlikelidir. Deepfakelerin yüz biyometrisi sahtekarlığı yapılarak birtakım ihlallerin yapılması mümkündür ancak önlenebilirdir.* ***Deepfake, bir kimlik doğrulama sistemi tarafından bir video olarak ele alınacağından, kimlik doğrulama sistemi video tabanlı saldırılara karşı yeteri kadar korunaklı ise, kameranın gördüklerinin yasal veya doğru olmadığını belirlemelidir.*** *Bunu başarmak için sistemin üç özelliğe sahip olması gerekir:* ***(i) iki veya üç boyutlu nesneleri ayırt edebilme, (ii) sertifikalı, üçüncü taraflarca test edilmiş insan canlılığı tespiti kullanarak sensörün gördüklerinin canlı olduğunu doğrulayabilme, (iii) canlı üç boyutlu görüntüyü, üç boyutlu bir görüntünün doğru dijital temsilini sağlayan önceden kaydedilmiş bir üç boyutlu "yüz haritası" ile eşleştirebilme.*** [1]

Bankaların şu aşamada bu tarz bilgisayar yazılımlarına karşı da önlem alıp alamayacağı tartışmaya açık olmakla birlikte, düzenlemenin lafzı ve ruhu kanaatimizce bu ihtimali de kapsar niteliktedir. Ancak teknolojinin Pandemi koşulları sebebiyle gittikçe artan gelişim ivmesi bu tarz teknolojilerin kullanım alanlarını ve dolayısıyla ihlal ihtimallerini arttıracağından yasal düzenlemelerin de bunlara ayak uyduracak hızda düzenlenmesi önem arz etmektedir.

---

[1] *The deepfake threat to face biometrics – JohnWojewidka – Biometric Technology Today Volume 2020, Issue 2, February 2020, Pages 5-7*

Yönetmelikte bahsi geçen bir diğer önemli husus da "**yakın alan iletişimi**" kavramıdır. **Near Field Communication (NFC)** kavramından çevrilen yakın alan iletişimi kısa menzilli ve kablosuz kişisel iletişim alanı teknolojisidir. En basit anlatımıyla kredi kartı-pos makinesi arasında iletişim kurulmasını sağlayan teknolojidir. Yönetmelik uyarınca yakın alan iletişimi kullanılarak **temassız yongadaki fotoğraf ile kişinin yüzünün biyometrik karşılaştırılması yapılacağı** düzenlenmiştir.

Devamla "… *Bu kapsamda kimlik avına, sosyal mühendisliğe, başka bir tarafın zorlamasıyla baskı altında gerçekleşen hareketlere ve benzeri dolandırıcılık yöntemlerine ilişkin riskler göz önünde bulundurulur.*" şeklinde düzenlenen hüküm işlemi yapacak müşteri temsilcisinin görüntülü görüşme sırasında "baskı" gibi çeşitli dolandırıcılık unsurlarını da tespit edebileceğinden bahsetmektedir. **Bu durumda müşteri temsilcilerinin alması gereken eğitimlerden birinin de m.5 kapsamında sayılmamış olsa da psikolojik eğitimler olması gerektiği yorumu yanlış bir değerlendirme olmayacaktır.**

Görüntülü görüşmede sürecin sonlandırılması başlıklı m.9 uyarınca süreç tamamlanmadan görüşmenin sona erdirilmesi düzenlenmiştir. Bağlantı, görüntü kalitesi, süreçte herhangi bir tutarsızlık veya belirsizlik, belge geçerliliği, dolandırıcılık veya sahtecilik gibi konularda herhangi bir sorun veya şüphe meydana geldiğinde süreç direkt olarak sonlandırılabilecektir. **Güvenlik önlemlerini alma konusunda bankaların sorumluluğu yüksek olduğundan sürecin sonlandırılması da doğru orantılı olarak ağır şartlara tabi tutulmamıştır.**

Verilerin kaydedilmesi ve saklanması başlıklı m.10 sürecin tamamının kayıt altına alınacağından ve saklanacağından bahsetmektedir. Bilgi ve belge saklama gerekliliklerine ilişkin ilgili mevzuat hükümleri saklı tutulmuştur. Kanaatimizce, söz konusu maddenin daha ayrıntılı düzenlenmesi gerekmektedir. Özel nitelikli kişisel veri kapsamında olan **"biyometrik veri"** saklanıp depolanacağından, sürecin müşteri tarafından tek taraflı olarak iptal edilmesi durumunda verilerin akıbetinin ne olacağı ve ne kadar saklanacağı konusunda açıklık getirilmesi Kişisel Verilerin Korunması Hukuku açısından önem arz etmektedir. BDDK tarafından yurtdışına veri aktarımı yapılması yasaklandığından bu **verilerin nasıl depolanacağı veya hangi bulut sistemi kullanılacağı** ile ilgili detaylı olmasa da genel hükümler getirilmesi uzun zamandır beklenen bir yönetmelikte aranması gereken unsurlardandır. Ancak kanun koyucunun yürürlükteki mevzuatın yeterli olduğunu ve ekstra bir düzenleme olarak bir ayrım yapılmasına gerek olmadığını düşündüğü şeklinde tahmin yürütülebilecektir.

Özel nitelikli kişisel veri kategorisinde yer alan **biyometrik veri** tanımına KVKK'da yer verilmemekle birlikte, 25.05.2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğünde ("**GDPR**") biyometrik verinin; "*yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler*" olarak tanımlandığı; Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararında biyometrik yöntemlerin, *ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini* ifade ettiği belirtilerek, bu yöntemler *arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma,* ***yüz tanıma,*** *retina tanıma, DNA tanıma gibi* yöntemlerin bulunduğunun ifade edildiği dikkate alındığında **uzaktan kimlik tespiti yöntemlerinin bu kapsamda olduğu** tartışmasızdır.

KVKK m. 4 genel ilkelerinden; **işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma** ilkesi çerçevesinde işlenen verilerin faaliyet konusu uzaktan kimlik tespitine paralel olarak düşünüldüğünde işleme faaliyetinin meşru bir temele dayandırıldığı iddia edilebilecektir. Ancak bankaların ve denetçilerinin bu faaliyet kapsamında işlenen verilerin biyometrik nitelikli olması **sebebiyle amaçla bağlantılı, sınırlı ve ölçülü olma konusunda sorumluluğun ve yaptırımların ağır olduğunun bilincinde hareket etmesi elzemdir.**

Kişisel Verileri Koruma Kurulunun "biyometrik veri" hususuna hassas yaklaşımı dolayısıyla **özellikle depolama ve muhafaze tedbirleri açısından** ayrıntılı düzenleme yapılmamış olması bankalar açısından önemli ihlallere yol açabilecektir. Uzaktan kimlik tespitinde sorumluluk bankaya

yüklenmiştir. İtiraz halinde ispat yükümlülüğü de bankada olacaktır. Bankanın uzaktan kimlik tespiti faaliyetlerini şikâyet üzerine kısıtlama ve durdurma yetkisi BDDK'ya aittir.

3. Elektronik Ortamda Sözleşme İlişkisinin Kurulması

Kimlik tespitini müteakip sözleşme ilişkisinin kurulması için **sözleşmeyi kuran irade beyanının alınması** şart koşulmuştur. Kişinin uzaktan kimlik tespiti sonrasında gerekli işlemleri yapabilmesi için şubeye gittiğinde ıslak imzası ile alınan ilgili sözleşmeyi kurmaya yönelik irade beyanının ne şekilde kurulacağı bu madde içinde düzenlenmekle birlikte getirdiği en önemli yenilik **ıslak imza şartının kalkmasıdır**. Yazılı şeklin yerine geçecek nitelikte sözleşme kurulabilmesi için aranan şartlar sayılırken BSEBY madde 38/3 ve 39/1'de belirtilen **müşteriye özgü şifreleme gizli anahtarı** kavramına atıf yapılmıştır. Tek kullanımlık bir doğrulama kodu üretilmesi sonrası taklit edilemeyen ve türetilemeyen bu kodların işlemi gerçekleştirdikten sonra geçersiz hale getirilmesi sağlanmaktadır.

4. Sonuç

Bu bilgiler ışığında Yönetmelik ile getirilen en önemli yenilikler;

- Uygulaması kendi müşterileri açısından belli işlemler için zaten başlamış olan uzaktan kimlik tespiti yöntemlerinin yeni müşteriler açısından da uygulanması,
- Uzaktan kimlik tespiti süreçlerinin detaylandırılması ve ek şartlar getirilmesi,
- Sahte yüz teknolojilerine karşı alınacak önlemlerde yetersiz ancak önemli bir ilk giriş düzenlemesi ve
- Islak imza şartının kalkması, şeklinde özetlenebilecektir.

Sahte yüz teknolojilerine karşı önlem alınmasını düzenleyen Yönetmelik maddesi teknolojinin gelişim hızı hesaba katılarak geniş söylemlere yer verilerek düzenlenmiş olmakla birlikte somut ihtiyacı yakın gelecekte oldukça mümkün olan bir konunun da ivedilikle spesifikleştirilmesi gerektiği kanaatindeyiz.

Aynı şekilde özel nitelikli kişisel veri kategorisinde yer alan biyometrik verilerin depolanması hususunun ayrıntılı düzenlenmemiş olması ciddi hukuki yaptırımlara gebe olabilecektir.

Yönetmelik kapsamında özellikle görüntülü görüşme ile ilgili usul ve esaslar düzenlenirken detaylı hükümlere yer verilmiş olması sürecin ciddiye alındığının göstergesidir. Eksik kalan alanlar ise halihazırda mevzuat uygulaması olan ve bir şekilde mutlaka ilgili mevzuatın uygulama alanlarıyla kesişir niteliktedir.

Dolayısıyla Yönetmelik kapsama alanının görece geniş ve düzenleme ihtiyacına cevap verecek yeterlilikte olduğunu söylemek en azından şu an için yanlış bir yorum olmayacaktır.

Saygılarımızla,

GRC | LEGAL