BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI
ÖZEL HUKUK TEZLİ YÜKSEK LİSANS PROGRAMI

RİSK MERKEZİ FAALİYETLERİ ÇERÇEVESİNDE MÜŞTERİ SIRRI VE BU SIRRIN KORUNMASI

HAZIRLAYAN

SEDEF ÖZTEK

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

AHMET CEMİL ÜNAL

ANKARA-2025

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 29 / 08 / 2025

Öğrencinin Adı, Soyadı	: Sedef ÖZTEK
Öğrencinin Numarası	: 22220293
Anabilim Dalı	: Özel Hukuk Anabilim Dalı
Programı	: Özel Hukuk Tezli Yüksek Lisans Programı
Danışmanın Unvanı/Adı, Soyadı	: Dr. Ahmet Cemil ÜNAL
Tez Başlığı	: Risk Merkezi Faaliyetleri Çerçevesinde Müşteri Sırrı ve Bu Sırrın Korunması

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 124 sayfalık kısmına ilişkin, 19/08/2025 tarihinde şahsım/tez danışmanım tarafından turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 4 tür. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:…….

ONAY

Tarih 29 / 08 / 2025

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Dr. Ahmet Cemil ÜNAL

TEŞEKKÜR

Bu tezin hazırlanma sürecinde desteklerini esirgemeyen, bilgi birikimi ve kıymetli görüşleriyle çalışmama yön veren değerli hocam Prof. Dr. Rıza AYHAN'a; tez çalışmamı inceleyerek görüşleri ve yapıcı eleştirileriyle çalışmamın gelişimine katkıda bulunan, tez savunmamı dinlemek için değerli vaktini ayıran ve tez jürimde yer almasından onur duyduğum değerli hocam Prof. Dr. Hayrettin ÇAĞLAR'a teşekkürlerimi sunarım.

Tez çalışmam sırasında olduğu gibi yaşamımın her anında yanımda olup bugünlere gelmeme vesile olan, sevincimin ve başarılarımın mimarı aileme ve her zaman destekleriyle bana güç veren dostlarıma teşekkür ederim.

ÖZET

ÖZTEK, Sedef, Risk Merkezi Faaliyetleri Çerçevesinde Müşteri Sırrı Kavramı ve Bu Sırrın Korunması, Başkent Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Tezli Yüksek Lisans Programı, 2025.

Banka müşterilerine ait kişisel veriler Bankacılık Kanunu uyarınca gizli tutulmalı ve bu veriler yalnızca müşterilerinin açık rızası veya kanunun öngördüğü istisnai hallerde paylaşılmalıdır. BankK. m. 73, bu yükümlülüklerin ihlali durumunda cezaî yaptırımlar öngörürken, anayasal düzeyde bakıldığı taktirde özel hayatın korunması temel bir hak olarak güvence altına alınmıştır. KVKK da müşteri verilerini özel veri kabul ederek veri işleme ve paylaşmada rıza, ölçülülük, amaçla sınırlı olma gibi ilkelerini düzenlemiştir. Bu çerçevede TBB bünyesinde faaliyet gösteren Risk Merkezi, kredi ve borç bilgilerinin toplandığı, bankaların yanı sıra faktöring, finansman ve leasing şirketlerini de kapsayan bir kredi bilgi sistemi olarak faaliyet göstermektedir. Risk Merkezi, mikro düzeyde bireysel kredi riskinin ölçülmesinde, makro düzeyde ise finansal sistem istikrarının gözetilmesinde önemli bir rol üstlenmektedir.

Çalışmanın ilk bölümünde müşteri sırrı ve Risk Merkezi kavramları incelenmiş, ikinci bölümünde ise Risk Merkezi'nin işleyişinde karşılaşılan sorunlar ele alınmıştır. İlgili hükümler ve ulusal mevzuat çerçevesinde hukuka uygunluk durumu incelenmiş, ayrıca uluslararası kredi bilgi sistemleriyle karşılaştırılmalı analizler yapılmıştır. Son olarak eksikliklere ilişkin hukukî, teknolojik denetim mekanizmaları ve gelişmelere yönelik iyileştirme önerileri sunularak çalışma sonlandırılmıştır.

Anahtar Kelimeler: Risk Merkezi, müşteri sırrı, kişisel veriler, banka sırrı, veri koruma.

ABSTRACT

ÖZTEK, Sedef, The Concept of Customer Secret and the Protection of This Secret within the Framework of the Risk Center's Activities, Başkent University Institute of Social Sciences, Master's in Private Law with Thesis, 2025.

Pursuant to the Banking Law, personal data of bank customers must be kept confidential, and such data may only be disclosed with the explicit consent of the customer or under exceptional circumstances expressly provided by law. Article 73 of the Banking Law prescribes criminal sanctions in cases of breach, while at the constitutional level, the protection of private life is safeguarded as a fundamental right. The Law on the Protection of Personal Data similarly treats customer information as sensitive data, regulating its processing and disclosure through the principles of consent, proportionality, and purpose limitation. In this context, the Risk Center, operating under the auspices of the Banks Association of Turkey, serves as a credit information system that consolidates credit and debt data, encompassing not only banks but also factoring, financing, and leasing companies. The Risk Center plays an important role, from evaluating personal creditworthiness to ensuring the resilience of the financial system.

The first part of the study examines the concepts of client confidentiality and the Risk Center, while the second part addresses the operational issues encountered in the functioning of the Risk Center. The analysis further evaluates the legality of its practices within the framework of relevant provisions and national legislation, accompanied by an analysis of international credit information systems. Finally, the final section puts forward suggestions for legal and technological oversight mechanisms, as well as improvement strategies to address identified shortcomings and future developments.

Key Words: Risk management, customer secret, personal data, banking law, data protection.

İÇİNDEKİLER

2. BÖLÜM

RİSK MERKEZİNİN İŞLEYİŞİ VE UYGULAMADA KARŞILAŞILAN SORUNLAR

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AY	Anayasa
AYM	Anayasa Mahkemesi
bkz.	bakınız
BankK.	Bankacılık Kanunu
BCBS	Basel Committee on Banking Supervision
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BIS	Bank for International Settlements
BK	Borçlar Kanunu
C.	Cilt
CBES	Climate Biennial Exploratory Scenario– CBES
CRS	Common Reporting Standard
EBRD	European Bank for Reconstruction and Development
ECB	European Central Bank
E.T.	Erişim Tarihi
EVE	Economic Value of Equity
FATF	Financial Action Task Force
FCRA	Fair Credit Reporting Act
FINRA	Financial Industry Regulatory Authority
FSAP	Financial Sector Assessment Program
GDPR	General Data Protection Regulation
IRB	Internal Ratings-Based

IRRBB	Interest Rate Risk in the Banking Book
ISO	International Organization for Standardization
KKB	Kredi Kayıt Bürosu
KVKK	Kişisel Verileri Korunması Kanunu
KYC	Know Your Customer
LCR	Liquidity Coverage Ratio
m.	Madde
MASAK	Malî Suçları Araştırma Kurulu
NSFR	Net Stable Funding Ratio
NGFS	Greening the Financial System
NII	Net Interest Income
OECD	Organisation for Economic Co-operation and Development
PDCA	Plan-Do-Check-Act
RFPA	Right to Financial Privacy Act
s.	sayfa
S.	sayı.
SMA	Standardised Measurement Approach
TBB	Türkiye Bankalar Birliği
TBK	Türk Borçlar Kanunu
T.C.	Türkiye Cumhuriyeti
TCK	Türk Ceza Kanunu
TCMB	Türkiye Cumhuriyeti Merkez Bankası
TCFD	Task Force on Climate-related Financial Disclosures
TTK	Türk Ticaret Kanunu
VaR	Value at Risk
www	World Wide Web
YHGK	Yargıtay Hukuk Genel Kurulu

GİRİŞ

Bankacılık sektörü günümüzde, finansal sistemlerin vazgeçilmez bir parçası olarak müşterinin güveninin sağlanması ve korunmasıyla yakından ilişkilidir. Sektörün işleyişinde müşteri bilgileri ve bu bilgilerin korunması yalnızca bankaların itibarı açısından değil, aynı zamanda finansal sistemin güvenilirliğinin sağlanması bakımından da önem arz etmektedir. Bankalar, müşterilerini korumak amacıyla elde ettikleri bilgileri yalnızca yasal çerçevede ve belirli sınırlar içinde işleyebilmektedirler. Ancak, dijitalleşmenin hızla yayılması ve bilgi paylaşımına dayalı iş yapısının artması, müşteri sırlarının korunması konusundaki tartışmaları derinleştirmiştir. Bu noktada, finansal kuruluşlar arasında bilgi paylaşımı ve kredi risklerinin değerlendirilmesi amacıyla Türkiye Bankalar Birliği bünyesinde faaliyet gösteren Risk Merkezi, ekonomik güvenliği artırarak finansal istikrarın sağlanmasında kritik bir görev üstlenmektedir. Özellikle kişisel veri olarak nitelendirilen müşteri bilgilerinin toplanması ve paylaşılması esnasında, hukukî düzenlemelerle tanımlanmış sınırların ihlali söz konusu olduğu takdirde ciddi hukukî ve cezaî sonuçlar ortaya çıkabilmektedir. Bu çalışma Türkiye'de sınırlı şekilde ele alınan Risk Merkezi'nin işleyişini ulusal ve uluslararası standartlar çerçevesinde değerlendirmeyi amaçlamaktadır. Çalışmada, müşteri sırlarının korunmasına ilişkin Türkiye'deki hukukî düzenlemeler ve uygulamalar ile uluslararası standartlar incelenerek bu alandaki sorunlar ve çözüm önerileri ortaya konulacaktır. Bu tez kapsamında şu sorulara yanıt aranacaktır: Risk Merkezi'nin işleyişinde müşteri sırlarının korunması ne ölçüde etkin bir şekilde sağlanmaktadır? Türkiye'deki hukukî düzenlemeler ve uluslararası standartlar nelerdir ve hangi noktalarda örtüşmekte veya farklılaşmaktadır? Müşteri sırlarının ifşâsı durumunda ortaya çıkabilecek hukukî ve cezâi sorumluluklar nelerdir? Risk Merkezi'nin işleyişinde şeffaflık ve müşteri sırrının korunması arasındaki dengeyi güçlendirmek için neler yapılmalıdır? Çalışmanın ilk bölümünde, müşteri sırrı kavramı ve bu kavramın bankacılık hukukundaki yeri ele alınacaktır. İkinci bölümde ise Risk Merkezi'nin faaliyetleri incelenerek, müşteri bilgilerine ilişkin mevcut hukukî düzenlemeler, uygulamada karşılaşılan sorunlar ve çözüm önerileri sunularak bankacılık sektöründe müşteri sırlarının korunması ile şeffaflık arasında bir denge kurulabileceği ortaya konulacaktır.

1. BÖLÜM

SIR, MÜŞTERİ SIRRI VE RİSK MERKEZİ KAVRAMLARI

I. SIR KAVRAMI

1. Sır Kavramının Tanımı ve Temel Unsurları

Sır, doktrinde genellikle yalnızca bir kimseye veya bir kitleye ait olan, kamunun bilgisine sunulmamış ve sahibinin açıklanmasını istemediği bilgi olarak tanımlanır[1]. Bu tanıma göre, bilginin gizli kalması bireyin kişilik hakları, itibarı gibi kişisel menfaatleri açısından önem arz etmektedir[2]. Ancak sır kavramı, bu tanımsal çerçeveyle sınırlı olmayıp aynı zamanda bireyin özel alanını ilgilendiren ve hukuk düzeni tarafından korunmakta olan bir değerdir.

Bir bilginin sır olarak nitelendirilebilmesi için, o bilginin herkese açık olmaması, ifşâ edilmesi durumunda sahibinin meşru menfaatlerinin zedelenme ihtimalinin bulunması ve sır sahibinin bilginin gizli kalmasını istemesi gerekmektedir[3]. Bu üçlü yapı sır kavramını, yalnızca toplumsal güven ilişkileriyle açıklanan bir olgu olmaktan çıkararak hukuken tanımlanabilir ve korunabilir bir hak hâline getirmektedir. Sır kavramı yalnızca bireyin ekonomik menfaatlerine değil, aynı zamanda özel hayatı, itibarı ve kişilik hakları gibi manevi değerlerinin de korunmasına hizmet etmektedir. Bu yönüyle sır kavramı, bireylerin sübjektif değer yüklediği bir nitelikten öte, hukuk düzeni tarafından objektif kriterlerle belirlenip koruma altına alınan bir hukukî statü kazanmaktadır[4].

Sırrın hukuken korunması, dijitalleşmenin hız kazandığı bilgi çağında daha da önem kazanmıştır. Sır saklama yükümlülüğü bireysel ve ticarî menfaatlerin ötesine geçerek finansal güvenlik, ticarî rekabet, meslek etiği, kurumsal güvenlik gibi pek çok alana temas etmekte ve bu bağlamda farklı hukuk dallarında düzenlenmektedir[5]. Özellikle özel hukuk

---

[1] Faruk Erem, Akın Altınok ve Haluk Tandoğan, *Bankalar Kanunu Şerhi*, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, 1989, s.328.
[2] Servet Taşdelen, *Bankacılık Kanunu Şerhi*, Ankara, Adalet Yayınevi, Cilt 2, 2. Baskı, 2015, s. 850.
[3] Yaşar Alıcı, *Bankacılık Kanunu Şerhi*, İstanbul, On İki Levha Yayıncılık, 2. Baskı, 2017, s. 1288.
[4] Daniel J. Solove, "Bir Mahremiyet Sınıflandırması (A Taxonomy of Privacy)", *University of Pennsylvania Law Review*, Cilt 154, Sayı 3, 2006, s. 479.
[5] İlknur Kaya, *Banka Hukukunda Müşteri Sırrını Saklama Yükümlülüğü (Fransa, İsviçre ve Türk Hukukunda)*, Ankara, Seçkin Yayıncılık, 2024, s. 30.

alanında sır kavramı, kişisel verilerin korunması, müşteri sırrı, ticarî sır ve meslek sırrı gibi farklı başlıklar altında somutlaşmakta ve koruma altına alınmaktadır.

Ceza hukuku ve medenî hukuk alanlarında sır kavramı farklı şekillerde ele alınsa da, ortak payda bilginin yetkisiz kişilerce ifşâ edilmesi durumunda hukukî sorumluluğun doğmasıdır. Nitekim, Türk Ceza Kanunu'nun 239. maddesi ticarî sırların, bankacılık sırrının ve müşteri sırrının hukuka aykırı olarak ifşâ edilmesini suç sayarak hapis cezası öngörmüştür; böylece bilgilerin korunması kamu güvencesi kapsamına alınmıştır. Bu düzenleme ile sır saklama yükümlülüğüne, kamu düzenine ilişkin bir hukukî değer atfedilmektedir.

Güvene dayalı kurulan hekim ve hasta, avukat ve müvekkil ile banka ve müşteri ilişkisi gibi ilişkilerde taraflar arasında paylaşılan bilgilerin gizliliği bu ilişkilerin temelini oluşturmaktadır[6]. Bu nedenle sır kavramı güven ilişkisinin ayrılmaz bir parçası olmaktadır. Bu tür ilişkilerde, sır saklama yükümlülüğünün ihlali kişisel mahremiyetin sınırlarını aşmakla beraber, bu meslek gruplarına ve kurumlara duyulan sistemsel güvenin zedelenmesine sebep olabilmektedir. Bu sebeple sır kavramı, yalnızca bireysel mahremiyetin değil, aynı zamanda ticarî güvenirliğin, meslekî etiğin ve nihayetinde finansal sistemin sürdürülebilirliğinin temel dayanaklarından biri olarak da karşımıza çıkmaktadır.

Özellikle banka ile müşteri arasındaki ilişki özelinde sır kavramı, yalnızca sözleşmesel bir yükümlülük olarak değerlendirilmemekte aynı zamanda yasal düzenlemeler tarafından koruma altına alınmakta ve doktrinde de bu yükümlülüğün önemi vurgulanmaktadır. Böylelikle sır saklama yükümlülüğü, güvenin kurumsallaşmış bir biçimi olarak hukuk düzeninde yerini bulmaktadır.

Bu yaklaşım yalnızca ulusal hukukla sınırlı kalmamakta, uluslararası düzeyde de karşılığını bulmaktadır. Nitekim uluslararası hukukta sır kavramı, kişisel verilerin korunmasına ilişkin düzenlemelerle paralellik göstermekte ve geniş bir hukukî koruma alanı içinde değerlendirilmektedir. Örneğin, Avrupa Birliği Genel Veri Koruma Yönetmeliği (General Data Protection Regulation– GDPR), kişinin özel alanına ilişkin bilgilerin rızası dışında açıklanmasını hukuka aykırı kabul etmekte ve kişisel verileri koruma altına alarak

[6] Lee Andrew Bygrave, *Uluslararası Perspektifle Veri Koruma Hukuku* (*Data Privacy Law: An International Perspective),* Oxford University Press, 2014, s. 4.

sır kavramına normatif bir içerik kazandırmaktadır[7]. Benzer şekilde Ekonomik İş birliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development– OECD), veri gizliliğini sır saklama yükümlülüğünün ayrılmaz bir parçası olarak değerlendirmektedir[8]. OECD'nin Ortak Raporlama Standardı (Common Reporting Standard– CRS) kapsamında sınır ötesi finansal bilgi paylaşımlarının, gizlilik ilkesine aykırı düşmeyecek şekilde yürütülmesi gerektiği vurgulanır[9]. Yine benzer olarak Malî Eylem Görev Gücü (Financial Action Task Force– FATF), finansal kuruluşların veri paylaşım süreçlerinde yalnızca risk temelli ve meşru gerekçelerle hareket etmesi gerektiğini belirtmektedir[10]. Özellikle, FATF'ın 2024 yılında yayımladığı rehberinde, veri paylaşımının yalnızca ölçülü, meşru amaçlara dayalı olarak hukukî sınırlar içinde gerçekleşmesi gerektiği ifade edilmiştir[11].

2. Sır Kavramının Tarihsel Gelişimi ve Günümüz Dijital Dünyasında Sır Kavramının Evrimi

Sır kavramı, insanlık tarihi boyunca farklı toplum ve kültürlerde çeşitli şekillerde ele alınmıştır. Örneğin, Mezopotamya'da gökyüzü hareketlerine dayalı kehanetler tanrısal kabul edilip sadece tapınak rahipleri tarafından bilinirdi ve halka açıklanmazdı[12]. Sırların korunmasına yönelik ilk kanunlaşma hareketi ise Hammurabi Kanunlarına dayanmaktadır. O dönem sırların açıklanması yasaklanmış ve gizli kalması gereken bu sırları açıklayan

[7] Avrupa Birliği, Gerçek Kişilerin Kişisel Verilerinin İşlenmesine ve Bu Verilerin Serbest Dolaşımına İlişkin Koruma Hakkında Avrupa Parlamentosu ve Konsey Tüzüğü (AB) 2016/679 (Genel Veri Koruma Tüzüğü– GDPR), 27 Nisan 2016, Avrupa Birliği Resmî Gazetesi, L119, 4 Mayıs 2016, m. 6 ve 9. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (E.T.: 01.08.2025)

[8] OECD, "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımı Hakkında Rehber İlkeler (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)", 1980, s. 3. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf (E.T.: 01.08.2025)

[9] OECD, *Gizlilik ve Bilgi Güvenliği Yönetimi Araç Seti (Confidentiality and Information Security Management Toolkit)*, Küresel Şeffaflık ve Vergi Konularında Bilgi Değişimi Forumu, 2020, s. 3. https://www.oecd.org/content/dam/oecd/en/networks/global-forum-tax-transparency/confidentiality-ism-toolkit-en.pdf (E.T.: 01.08.2025)

[10] FATF, Özel Sektörde Bilgi Paylaşımına İlişkin Rehber (Guidance on Private Sector Information Sharing), 2017, s. 10. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf (E.T.: 01.08.2025)

[11] FATF, *2023–2024 Yılı Faaliyet Raporu (Annual Report 2023–2024)*, Paris, 2024, s. 24. https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html (E.T.: 01.08.2025)

[12] Francesca Rochberg, *Göksel Yazı: Mezopotamya Kültüründe Kehanet, Horoskopi ve Astronomi* (*The Heavenly Writing: Divination, Horoscopy, and Astronomy in Mesopotamian Culture)*, Cambridge, Cambridge University Press, 2004, s. 216.

kişinin yasak bir davranışta bulunduğu kabul edilerek gözlerinden bir tanesinin çıkarılacağı eklenmiştir[13].

İlk çağlarda sır korunmasına ilişkin özel bir düzenleme bulunmamakla beraber bazı meslek gruplarının mesleklerini icra ederken öğrenmiş oldukları sırları saklamakla yükümlü oldukları kabul edilmiştir. Örneğin, "*Hipokrat Yemini*" hekimlerin görevleri esnasında öğrendikleri sırları saklamakla yükümlü olduklarını belirten bir metindir[14].

Bu tarihsel arka plan sır kavramının toplumsal ve hukukî düzenlemelerde de belirli bir statü kazanmasına zemin hazırlamıştır. Örneğin, Roma hukukunda da *fides* (güven) ilkesi çerçevesinde, taraflar arasında kurulan güven ilişkileri, bazı bilgilerin gizli kalmasını zorunlu kılarak sır saklama yükümlülüğüne örnek teşkil etmiştir. Özellikle *mandatum* (vekâlet), *depositum* (emanet) ve *societas* (ortaklık) sözleşmelerinde, taraflardan birinin diğerine aktardığı bilgi ya da malvarlığı unsurlarının çoğunlukla güven temelinde korunmuştur. Bu kapsamda vekil, vekâlet verenin açıkladığı gizli bilgileri üçüncü kişilere açıklamamakla yükümlüydü. Benzer şekilde, emanet alan kişi de kendisine emanet edilen malın içeriğini veya niteliğini başkasına açıklaması hâlinde *fides* ilkesine aykırı davranmış sayılmaktaydı ve sorumluluğu doğmaktaydı[15].

Orta Çağ'da ise sır kavramı ağırlıklı olarak lonca sistemleri ve belli zanaat grupları çerçevesinde şekillenmiştir. Bu dönemde bilgi yalnızca bireysel yetenek olarak değil, aynı zamanda ekonomik güç ve sosyal statünün kaynağı olarak görülmüştür. Bu nedenle, belirli meslek grupları sahip oldukları bilgileri, üretim tekniklerini ve ticarî bilgilerini gizli tutarak mesleklerinin kalitesini ve itibarını koruyup rekabet avantajları sağlamışlardır. Usta çırak ilişkisi içerisinde aktarılan bir deri işleyicisinin kullandığı özel yöntem ya da bir silah ustasının döküm tekniği gibi bilgiler, o loncanın iç kurallarına ve etik ilkelerine sıkı sıkıya bağlı olarak yalnızca ilgili meslek grupları arasında saklı tutulmuştur. Bu sayede meslek erbapları teknik bilgi birikimini dışa kapalı tutarak hem meslekî kalitesini korumuş hem de diğer gruplar karşısında ekonomik bir rekabet avantajı elde etmiştir[16].

---

[13] "Hammurabi Kanunları", çeviri: L.W. King, *The Avalon Project*, Yale Law School. https://avalon.law.yale.edu/ancient/hamframe.asp (E.T.: 01.08.2025)

[14] "Hipokrat Yemini", çeviri: W.H.S. Jones. *Loeb Classical Library*, Harvard University Press, 1923. https://www.loebclassics.com/view/hippocrates_cos-oath/1923/pb_LCL147.295.xml (E.T.: 01.08.2025)

[15] Schulz Fritz, *Klasik Roma Hukuk (Classical Roman Law)*, Oxford, Clarendon Press, 1951, s. 134.

[16] William Eamon, *Bilim ve Doğanın Gizleri: Orta çağ ve Erken Modern Kültürde Sır Kitapları (Science and the Secrets of Nature: Books of Secrets in Medieval and Early Modern Culture)*, Princeton, Princeton University Press, 1994, s. 82.

Nitekim bu dönemde sır kavramı yalnızca bireysel değil, aynı zamanda kolektif bir aidiyet anlamı taşımaktaydı. Meslekî bilginin paylaşımı, topluluğun onayını almadan mümkün değildi ve ihlaller meslek sırlarının ifşâsına yönelik cezaî bir sorumluluk bulunmamasına rağmen ağır yaptırımlarla karşılık bulmaktaydı[17]. Örneğin, 13. yüzyılda Venedik'te cam ustalarının üretim tekniklerini ihlal edenlerin şehir dışına çıkmaları yasaklanmış, Floransa'da ise kuyumcu loncalarındaki teknik sırları dışarı sızdıranlar loncadan ihraç edilmişti[18].

Benzer bir durum Osmanlı İmparatorluğundaki esnaf teşkilatlarının da farklı bir tarihsel dönemde, benzer bir sır koruma anlayışını sürdürdüğü görülmüştür. Osmanlı'da loncaların bağlı bulunduğu ahîlik geleneği çerçevesinde, zanaat ve meslek bilgileri yalnızca usta-çırak hiyerarşisi içinde aktarılmış ve ehl-i hıref olarak bilinen saray zanaatkârlarının dahi üretim tekniklerini dışarı sızdırması hâlinde meslekten ihraç ve kamu önünde itibar kaybı gibi ciddi sonuçlarla karşı karşıya kaldığı görülmüştür[19].

Bu tarihsel arka plan, modern dönemde ticarî sır, meslek sırrı, müşteri sırrı gibi kavramların temelini oluşturarak sır kavramının kurumsallaşmasına zemin hazırlayıp hukukî düzenlemelere ilham olmuştur. Sır kavramı, zamanla yalnızca zanaatkâr çevrelerle sınırlı kalmayıp kişisel verilerin korunmasından ulusal güvenliğe kadar uzanan geniş bir yelpazede hem özel hukukun hem de kamu hukukunun ortak koruma alanına girmiştir.

Sır kavramı artık yalnızca ahlaki bir yükümlülük olarak değil, hukuken tanımlanmış, sınırları belirlenmiş ve ihlali hâlinde yaptırımla karşılanan bir hak olarak düzenlenmektedir. Bu kapsamda ticarî sır, meslek sırrı ve devlet sırrı gibi alt kategorilerde ele alınmakta ve her biri farklı düzenlemelere tâbi tutulmaktadır. Örneğin, Türkiye'de 4857 sayılı İş Kanunu'nun 25/II-e maddesi uyarınca, çalışanların işverene ait ticarî sırları açıklaması, iş sözleşmesinin haklı nedenle feshi için yeterli kabul edilmekte ve işverenin tazminatsız fesih hakkı doğmaktadır.

Benzer şekilde devlet sırrı niteliği taşıyan bilgilerin kamu güvenliği, diplomatik ilişkiler ve ulusal savunma gibi alanlardaki önemi sebebiyle bu kapsamdaki bilgilerin yetkisiz olarak ifşâsı hem iç hukukta hem de uluslararası hukukta ciddi yaptırımlarla karşılık

[17] Süheyl Donay, *Meslek Sırrının Açıklanması Suçu*, İÜHF Yayınları, 1978, s.26.
[18] Eamon, s. 82.
[19] Yusuf Ibish, "Çarşıların Loncaları (Brotherhoods of the Bazaars)", *The UNESCO Courier*, Cilt 30, Sayı 12, 1977, s. 15. https://unesdoc.unesco.org/ark:/48223/pf0000074817 (E.T.: 01.08.2025)

bulmaktadır. Örneğin, Türkiye Cumhuriyet Anayasası'nın 28. maddesinin 2. fıkrasında basın özgürlüğünün devlet sırlarını ifşâ etme amacıyla kullanılamayacağı belirtilmiş ve bu bilgilerin kamuya açıklanması engellenmiştir. Bu sayede devlet sırrı niteliğindeki bilgilerin açıklanmasının toplumsal güvenliğe zarar vermesinin önüne geçilmiştir.

Bilgi ve iletişim teknolojilerinin yaygınlaşması, kişisel ve ticarî bilgilerin dijital ortamlarda saklanmasını ve paylaşılmasını kolaylaştırmıştır. Bu sebeple, Avrupa Birliği'nin 2016 yılında kabul ettiği ve 2018 yılında yürürlüğe giren Genel Veri Koruma Yönetmeliği, kişisel verilerin işlenmesi ve paylaşılması konusunda sır kavramının önemini vurgulayarak katı kurallar getirmiştir[20].

Aynı yıl Türkiye'de de benzer gelişmeler yaşanmıştır. 2016 yılında yürürlüğe girmiş olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin korunmasını somutlaştırarak bu alanda önemli düzenlemeler getirmiştir. Bu düzenlemeler arasında açık rıza ilkesinin zorunlu hâle gelmesi, veri sorumlusunun aydınlatılma yükümlülüğü, kişisel verilerin yurt dışına aktarımında Kişisel Verileri Koruma Kurulu'nun izninin aranması ve ilgilinin verilerine erişim, düzeltme, silinme ve itiraz hakkına sahip olması gibi ilkeler öne çıkmıştır. Özellikle KVKK madde 5 ve 6'da kişisel verilerin ancak kanunun uygun gördüğü hukukî sebeplerle işlenebileceğini belirtilerek bilgilerin kullanılması ve paylaşılmasında keyfiliğin önüne geçilmiştir.

Dijitalleşme ile beraber sır kavramı yalnızca hukukî değil, aynı zamanda etik ve sosyal boyutlarda da dönüşüm geçirmiştir. Etiksel açıdan bakıldığında, bireylerin mahremiyet haklarına saygı gösterilmesi ve rızaya dayalı veri paylaşımı ilkesi önem kazanmıştır[21]. Sosyal boyutta değerlendirildiğinde ise, dijital ortamdaki görünürlük kişiler arası güven, sosyal itibar ve dijital kimlik gibi kavramlar üzerinde doğrudan etkide bulunarak birey ve toplum ilişkisini etkilemektedir. Nitekim 2021 yılında Facebook üzerinden yaşanan bir veri ihlali sonucunda, 533 milyondan fazla kullanıcının e-posta adresi, doğum tarihi, telefon numarası, konum bilgisi gibi kişisel verileri üçüncü tarafların erişimine açılmıştır. Bu durum platform kullanıcılarının özel hayatına ilişkin bilgilerin ifşâsına yol açmakla kalmamış, bireylerin dijital kimliklerine ve toplumsal itibarlarına da zarar vermiştir[22]. Sosyal medya

[20] GDPR, m. 5 ve m. 32.
[21] Lee Andrew Bygrave, s. 120.
[22] Andrew James Dellinger, "533 Milyon Facebook Kullanıcısının Kişisel Verisi Çevrimiçi Sızdırıldı (Personal Data of 533 Million Facebook Users Leaks Online)", *Forbes*, 2021. https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/ (E.T.: 01.08.2025)

platformlarında kişisel bilgilerin paylaşılması ve dijital platformların kullanım politikaları, bu ve benzeri olaylar etkisiyle, sır kavramının sınırlarını belirsizleştirmektedir. Dolayısıyla dijital çağda sır kavramı bireyin özel alanıyla sınırlı kalmayarak, dijital özerkliğiyle ve sosyal ilişkileriyle doğrudan bağlantılı hâle gelmiştir.

3. Sır ile İlişkili Kavramların Karşılaştırılması

A. Gizlilik

Gizlilik, sır kavramının temel yapıtaşlarından biri olmakla beraber, sır kavramından daha geniş ve kapsamlı bir anlam taşımaktadır. Gizlilik, kişinin özel hayatına ilişkin bilgilerin ifşâsını engelleme hakkını içerirken, sır bu gizliliğin belirli bir çıkarı korumak amacıyla hukukî koruma altına alınan hâlidir. Örneğin, bir şirketin organizasyon yapısı gizlilik kapsamında olabilirken üretim formülü sır olarak nitelendirilmektedir[23].

B. Mahremiyet

Mahremiyet kişinin kendi özel yaşam alanı üzerindeki denetim hakkını ifade eden bir kavramdır. Sırdan daha sübjektif bir boyut taşımaktadır. *Westin*'e göre mahremiyet, bireylerin kendi bilgilerinin ne zaman ve ne ölçüde paylaşılacağına karar verebilme imkânına sahip olmasıdır ve çoğunlukla kültürel, dinî ve ahlâki değerlere göre şekillenir[24]. Oysa sır, daha çok üçüncü kişilere karşı korunması gereken ve belirli bir tarafça edinilen özel bilgiyle ilgilidir. Örneğin, bir müşteriye ait finansal veriler hem mahremiyet hem sır kapsamında değerlendirilebilir ancak bu bilgilere banka çalışanının görevi gereği erişmesi durumunda banka sırrı ve meslek sırrı boyutu da devreye girecektir.

C. Kişisel Veri

Kişisel veri kavramı, 6698 sayılı KVKK'ye göre, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Bilginin gizli olması ya da olmaması kişisel veri olarak tanımlanması bakımından önem arz etmemektedir[25]. Sır ise gizli kalması beklenen, ekonomik ya da stratejik değeri bulunan daha dar kapsamlı bir bilgi grubunu ifade eder. Her

[23] Burak Başel, *Banka Sırrının Açıklanması Suçu (BankK m. 159)*, Ankara, Seçkin Yayıncılık, 2021, s. 62.
[24] Alan Furman Westin, Mahremiyet ve Özgürlük (*Privacy and Freedom)*, New York, Atheneum, 1967, s. 7.
[25] Hüseyin Can Aksoy, *Medenî Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak, Ankara 2010, s. 14.

sır bir kişisel veri olabilir ancak her kişisel veri bir sır değildir. Örneğin, kişinin adı ve soyadı kişisel veri iken, bankadaki varlık dağılımı hem kişisel veri hem de müşteri sırrıdır.

D. Ticarî Sır

Ticarî sır, işletmeye rekabet avantajı sağlayan ve açıklanması durumunda zarar doğurabilecek gizli bilgilerden oluşur[26]. Sır, daha geniş bir kavram iken, ticarî sır bu kavramın bir alt türünü oluşturmaktadır. Örneğin, Coca Cola'nın formülü bir ticarî sırdır ancak bu formüle dair bilgiye sahip olan çalışan için bu aynı zamanda meslek sırrı da olabilir. Nitekim Yargıtay da işletmeye ait gizli bilginin çalışan tarafından ifşâsını hem ticarî sırrın hem de meslekî gizlilik yükümlülüğünün ihlali olarak değerlendirmektedir[27].

E. Meslek Sırrı

Meslek sırrı, belirli bir meslek mensubunun görevi sırasında edindiği ve saklamakla yükümlü olduğu gizli bilgilerdir[28]. Noter ile taraflar, psikolog ile danışan, muhasebeci ile müşteri veya bankacı ile müşteri arasındaki güven ilişkisi meslek sırrını ortaya çıkaran ilişkilere örnek teşkil etmektedir. Meslek sırrı her ne kadar sır kavramı kapsamında değerlendirilse de bu bilgilerin korunmasına yönelik yükümlülükler daha sıkı düzenlemelere tâbi tutulmuş ve cezaî yaptırımlarla desteklenmiştir. Nitekim Yargıtayın 31/01/2013 kararından da anlaşılacağı üzere, ticari sır veya müşteri sırrı niteliğindeki bilgilerin üçüncü kişilere aktarılması, TCK m. 239 kapsamında suç teşkil etmekte ve ilgililerin sorumluluğunu doğurmaktadır[29].

F. Devlet Sırrı

Devlet Sırrı Kanunu Tasarısı'nın 3. maddesine göre devlet sırrı, açıklanması veya öğrenilmesi durumunda devletin dış ilişkilerine, millî savunmasına ve millî güvenliğine zarar verme potansiyeli sebebiyle gizli kalması gereken bilgi ve belgelerdir[30]. Örneğin, bir devletin olası savaş, büyük afet, ekonomik çöküş gibi krizler için hazırladığı müdahale ve yönetim planları, yapmayı planladığı askerî harekâtın tarihleri, hedef bölgeleri ve kuvvet

---

[26] Mehmet Emin Bilge, *Ticarî Sırrın Korunması*, Ankara, Seçkin Yayıncılık, 2. Baskı, 2005, s. 5.
[27] Bkz. Yargıtay 15. CD 14.05.2018 Tarih ve E. 2018/1699, K., 2018/3379 sayılı kararı. (www.yargitay.gov.tr, E.T.: 01.08.2025)
[28] Faruk Erem, *Ceza Hukuku Genel Hükümler*, Ankara, Sevinç Matbaası, 1997, s. 588.
[29] Bkz. Yargıtay 4.CD 31/01/2013 Tarih ve E.2011/10653, K.2013/2381 sayılı karar. (www.yargitay.gov.tr, E.T.: 01.08.2025)
[30] https://www.bilgiedinmehakki.org/blog/2006/10/12/devlet-sirlari-kanunu-tasarisi/ (E.T.: 01.08.2025)

dağılımı gibi açıklanması durumunda millî güvenlik veya milletlerarası ilişkiler bakımından zarar ve tehlike arz eden bilgiler devlet sırrı kabul edilebilir. Bu tür bilgiler özel yasal düzenlemelerle korunur ve ifşâsı durumunda Türk Ceza Kanunu (TCK) m. 327 ve devamı maddelerine göre ağır cezaî yaptırımlar uygulanır. Nitekim Yargıtay 16. Ceza Dairesi de MİT tırlarına ilişkin operasyon bilgilerini içeren görüntülerin medya yoluyla paylaşılmasını, devletin güvenliğine yönelik gizli bilgilerin ifşâsı olarak değerlendirerek TCK m. 327 ve devamı maddelerindeki düzenlemeler çerçevesinde cezalandırılabileceğini vurgulamaktadır[31].

G. Banka Sırrı

Banka sırrı, Ticarî Sır, Banka Sırrı ve Müşteri Sırrı Hakkındaki Kanun Tasarısı'nın 2/1-b maddesinde "Bankanın yönetim ve denetim organlarının üyeleri, mensupları ve diğer görevlileri tarafından bilinen malî, iktisadî, kredi ve nakit durumu ile ilgili bilgilerle bankanın müşteri potansiyeli, kredi verme, mevduat toplama, yönetim esasları, diğer bankacılık faaliyetleri, risk pozisyonlarına ilişkin her türlü bilgi, belge" olarak tanımlanmıştır[32].

Öğretide bankalara ve onların iştiraklerine, birlikte kontrol edilen ve bağlı olan ortaklıklarına ve bankaların müşterilerine ait olan sır[33] olarak da tanımlanan banka sırrı kavramı, müşteri sırrı kavramı ile iç içe geçmiş olsa da bu kavramları ayrı değerlendirmek gerekmektedir. Yapılmış olan bu tanımlardan hareketle bankacılık sırrı kavramı, banka müşterilerine ait müşteri sırrı dışında kalan bilgilerin tamamı olarak nitelendirilebilir[34].

4. Sır Kavramının Hukukî Dayanakları

A. Türkiye Cumhuriyeti Anayasası

Türkiye Cumhuriyeti Anayasası'nın 20. maddesi, özel hayatın gizliliğini ve kişisel verilerin korunmasını isteme hakkını güvence altına almaktadır. Maddenin 1. fıkrası bireylerin mahrem alanlarının devlet ve 3. kişilerce ihlal edilmemesini teminat altına

[31] Bkz. Yargıtay 16. CD 20/09/2018 Tarih ve E.2018/2088, K.2018/2728 sayılı kararı. (www.yargitay.gov.tr, E.T.: 01.08.2025)
[32] https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=706 s. 9. (E.T.: 01.08.2025)
[33] Ünal Tekinalp, *Banka Hukukunun Esasları,* İstanbul, Vedat Kitapçılık, 2009, 2. Baskı, s. 411.
[34] Cengiz Topel Çiftçioğlu, *Sırrın Korunması Boyutuyla Ticarî Sır, Bankacılık Sırrı veya Müşteri Sırrının Açıklanması Suçu,* Ankara, Seçkin Yayıncılık, 2017, s. 171.

almaktadır. Özel hayatın gizliliği kapsamında bireylerin sırlarının korunması da mündemiçtir. Nitekim bireylerin "kendilerine ait bilgi ve sırları başkalarına açıklamama ve açıklanmasını engelleme hakkı" özel hayatın gizliliğinin doğal bir sonucudur. Yargıtay Hukuk Genel Kurulu'nun da 06.11.2018 tarihli kararında vurgulandığı üzere, kişisel verilerin korunması hakkı ve bireylerin kendileriyle ilgili bilgileri kontrol edebilme yetkisi Anayasa m. 20 ile güvence altına alınmıştır[35]. Bu bağlamda, bireylerin sağlık bilgileri, finansal durumu, haberleşme içerikleri gibi sır niteliğindeki bilgilerin korunması, anayasal bir korumaya sahiptir.

2010 yılında Anayasa m. 20'ye eklenen 3. fıkra ile kişisel verilerin korunması talebi anayasal bir hak olarak somutlaştırılmıştır. Bu fıkraya göre herkes, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme ve bu verilere erişme, düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahiptir. Ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya ilgili kişinin açık rızasıyla işlenebileceği belirtilmiştir. Bu düzenleme, bireylerin kendilerine ait veriler üzerindeki tasarruf hakkını güçlendirirken devletin de bu verilerin gizliliğini korumak üzere gerekli olan hukukî ve idarî tedbirleri alması yükümlülüğünü doğurmaktadır. Anayasa m. 20/3 aynı zamanda özel hayatın gizliliğinin dijital çağda genişleyen boyutunu da kapsayarak kişisel dijital verilerin mahremiyetini de güvence altına almıştır.

Özel hayatın gizliliği hakkı, sır saklama ile yakından ilgilidir. Anayasada açıkça "sırların korunması" ifadesi yer almasa da m. 20 kapsamında mahremiyet hakkı, bireyin istemediği verilerinin ifşâ edilmemesi hakkı korunur. Örneğin, banka müşterisinin finansal bilgilerinin gizliliği, haberleşmenin gizliliği gibi hususlar özel hayatın gizliliği kapsamında değerlendirilir.

Anayasa m. 13 gereğince, özel hayatın gizliliğine yapılacak herhangi bir müdahale ancak kanunla öngörülmeli, meşru bir amacı olmalı ve demokratik toplum düzeninin gereklerine uygun, ölçülü bir şekilde uygulanmalıdır. Bu ilke, verilere kamusal müdahalelerin de sınırını çizmektedir. AYM'nin bireysel başvuru kararlarında kişisel verilerin hukuka aykırı ifşâsı veya özel hayatın ihlali iddialarını bu çerçevede incelemesi anayasal düzeyde sırların korunmasının ne denli önemsendiğini ortaya koymaktadır.

[35] Bkz. YHGK 06.11.2018 Tarih ve E.2017/1340, K.2018/1622 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

B. Borçlar Kanunu

6098 sayılı Türk Borçlar Kanunu'nun m. 49 uyarınca, hukuka aykırı bir fiille başkasına zarar veren kişi zararı tazmin etmekle yükümlüdür. Müşteri sırlarının ifşâ edilmesi açıkça hukuka aykırı bir fiildir. Nitekim böyle bir fiil hem sözleşmesel gizlilik yükümlülüğünü hem de kişilerin mahremiyet hakkını ihlal eder. Dolayısıyla, müşteriye ait gizli bilgileri izinsiz açıklayan kişi veya kuruluş, TBK m. 49 uyarınca doğan maddi zararları gidermekle sorumlu olacaktır. Örneğin, bir bankanın müşteri verisini ifşâ etmesi üzerine, müşteri iş fırsatını kaybetmiş veya maddi bir zararı söz konusu olmuşsa uğradığı zararının tazminini bankadan talep edebilecektir. İhlal hâlinde maddi zararın hesaplanması ise elde edilemeyen kar, zamanından önce bozulan mevduat faizi geliri veya ifşâ sebebiyle ödenmek zorunda kalınan ödenen fazladan vergi veya ceza gibi giderler göz önünde bulundurularak somut olaya göre yapılır.

TBK m. 49 kapsamında tazmin edilecek zarar yalnızca maddi kayıplarla sınırlı olmamaktadır. Müşteri sırrının ihlali çoğu kez kişinin özel hayatının gizliliğinin ihlali anlamına geldiğinden bir kişilik hakkının ihlali sayılmaktadır. Bu sebeple, kişi maruz bırakıldığı manevi üzüntü ve sıkıntı nedeniyle manevi tazminat talebinde bulunabilecektir. TBK m. 58 kişilik hakkının ihlali hâlinde manevi tazminata hükmedilebileceğini öngörmektedir. Mahkeme manevi tazminat miktarının takdirini yaparken ihlalin ağırlığı, müşterinin itibarına etkisi gibi unsurları göz önünde bulundurur. Örneğin, bankanın müşterisinin yüklü borç bilgilerinin basına sızdırılması durumunda daha yüksek manevi tazminata hükmedilebilirken, daha hafif ihlal için sembolik bir tazminat verilmesi mümkün olabilir. Ayrıca TBK m. 58 manevi tazminat yerine veya manevi tazminata ek olarak diğer tatmin yollarına da imkân tanımaktadır. Örneğin, hâkim, bankanın müşteri sırrı ihlalini kınayan bir karar verip, bu kararı bankanın yanlışını kabul eden özür mahiyetindeki bir şekilde gazete yayımlanması şeklinde ilanına karar verebilir[36].

Öte yandan sır saklama yükümlülüğü işveren-işçi ilişkisi gibi alanlarda da karşımıza çıkmaktadır. TBK 396. maddesi, işçinin işverenine ait sırları saklama yükümlülüğünü özel hukuk ilişkisine dayalı bir borç olarak çeşitli yaptırımlara bağlar. Bu maddeye göre, işçi, işverenin üretim ve iş sırlarını hizmet ilişkisi süresince ve sonrasında korumakla yükümlüdür. İş sözleşmesinden doğan bu yükümlülük, işçinin işverene karşı sadakat

[36] Fikret Eren, İpek Yücer, *Borçlar Hukuku Özel Hükümler,* Ankara, Legem Yayınevi, 12. Baskı, 2024, s. 906.

borcunun bir parçasıdır. Çalışan, işi gereği öğrendiği ticarî veya teknik bilgileri, müşteri bilgilerini ve işverene ait diğer gizli hususları izinsiz olarak üçüncü kişilerle paylaşamaz[37].

Sır saklama yükümlülüğü iş akdi sona erdikten sonra bile devam etmektedir. Çalışan işten ayrıldıktan sonra dahi önceki işverenin sırlarını ifşâ ederse sorumluluğu doğacaktır. Bu yükümlülüğe aykırı davranış hem borçlar hukuku hem de iş hukukuna aykırılık teşkil etmektedir. İşveren, gizliliği ihlal eden işçisi hakkında uğramış olduğu zarara göre TBK m. 49 uyarınca tazminat talep edebileceği gibi, İş Kanunu m. 25 uyarınca haklı nedenle derhâl fesih hakkını da kullanabilecektir. Nitekim Yargıtay 05/07/2022 tarihli bir kararında, işverenin satış ve pazarlama bilgilerini e-posta ile dışarı sızdıran çalışanının eylemi sır saklama yükümlülüğüne aykırılık sayarak işverene haklı fesih imkânı verdiğini ve ayrıca manevi tazminat sorumluluğunu da doğurduğunu açıkça belirtmiştir[38].

C. Ticaret Hukuku

6102 sayılı Türk Ticaret Kanunu (TTK), ticarî sırların korunmasını haksız rekabet hükümleri çerçevesinde ele alır. Türk hukukunda ticarî sırlara özel bir kanun bulunmamakla beraber, TTK dışında bankacılık, elektronik haberleşme gibi sektörlere özgü kanunlarda da gizlilik hükümleri yer almaktadır. Genel olarak ticarî sır bir işletmenin rakiplerine karşı ekonomik değer taşıyan ve kamuya açık olmayan, gizli kalmasında sahibinin menfaati bulunan her türlü bilgi olarak tanımlanabilir. Örneğin, bir şirketin üretim yöntemleri, formülleri, fiyatlandırma politikaları, pazarlama stratejileri veya müşteri verileri ticarî sır kapsamında değerlendirilir. İşletmeye rekabet avantajı sağlayan bu bilgilerin izinsiz ifşâsı haksız rekabet olarak değerlendirilir ve hukukî yaptırımlara tâbidir.

TTK m. 54 ve devamı maddelerinde düzenlenen haksız rekabet hükümleri ticarî sırların izinsiz ifşâsını dürüstlük kuralına aykırı bir rekabet avantajı olarak görerek yasaklamaktadır. TTK m. 55/1-c hükmü uyarınca, üretim ve iş sırlarını hukuka aykırı olarak ifşâ etmek bir haksız rekabet fiilidir. Bu hüküm bir tacirin ticarî faaliyetlerine ilişkin gizli bilgileri hukuka aykırı şekilde ele geçirip kullanmasını veya meşru yollardan öğrenilmiş olsa bile izinsiz olarak açıklamasını dürüstlük kuralına aykırı davranış olarak kabul etmektedir. Dolayısıyla, rakip olan bir şirketin gizlice elde ettiği bir üretim formülünü kendi çıkarına kullanması da şirket çalışanının öğrendiği iş sırlarını izinsiz bir şekilde üçüncü şahıslara ifşâ

[37] Fikret Eren, İpek Yücer, s. 547.
[38] Bkz. Yargıtay 9.HD 05/07/2022 Tarih ve E.2022/6929, K.2022/8687 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

etmesi de TTK m. 55 anlamında haksız rekabeti oluşturmaktadır. Failin bu eylemlerden maddi bir kazanç sağlamaması, fiil neticesinde zarar doğmaması, karşı tarafın zarar görmemesi veya failin kazanç elde etmemesi önemli olmamaktadır. Fiilin dürüst rekabet ortamını bozucu nitelikte olması hukuka aykırılık için yeterli olmaktadır.

TTK m. 55'e uyarınca, çalışanlar veya yardımcılar üzerinden gerçekleştirilen sır ihlalleri de haksız rekabet kapsamında özel olarak düzenlenmiştir. Örneğin, işçileri işverenlerinin üretim ve iş sırlarını ifşâ etmeye veya ele geçirmeye yönlendirmek haksız rekabet teşkil eder. Üçüncü bir kişinin, rakip işletmenin çalışanını para veya menfaat karşılığında işvereninin gizli bilgilerini vermeye teşvik etmesi de örnek gösterilebilir. Keza bir şirketin eski çalışanının, önceki işverenine ait müşteri listesi gibi gizli bilgileri yeni işverenine vermesi durumunda, yeni işveren hem bu bende göre haksız rekabet suçu işlemiş olur hem de TBK m. 396'daki sadakat borcuna aykırılığa iştirak etmiş olur.

Haksız rekabet fiilleri nedeniyle açılacak davalar TTK m. 60 uyarınca ihlalin ve failin öğrenilmesinden itibaren 1 yıl, her hâlde fiilin gerçekleşmesinden itibaren 3 yıl içinde ileri sürülmelidir. Mahkeme, durumun gereğine göre, hukukî koruma yollarından birine veya birkaçına birlikte hükmederek hem ihlali durdurabilir hem de geçmiş zararları giderebilir. Ayrıca hükmün gazetede ilanı gibi sonuçlar da uygulanabilir. Bu durum özellikle şirket itibarının zedelenmesi söz konusu ise önem taşımaktadır.

TTK, ticarî sırların ihlaline karşı cezaî yaptırımlar öngörmeyi de ihmal etmemiştir. TTK m. 62 haksız rekabet fiillerini kasten işleyenlerin, şikâyet üzerine iki yıla kadar hapis veya adlî para cezasıyla cezalandırılabileceğini de hükme bağlamıştır. Bunun yanı sıra TCK m. 239'da ticarî sır, banka sırrı veya müşteri sırrı niteliğindeki bilgilerin yetkisiz ifşâsını ayrı bir suç olarak düzenlemektedir. Örneğin, bankanın kredi değerlendirme biriminde çalışan görevlinin müşterilere ait finansal raporları çıkar amaçlı üçüncü kişilere sızdırması hem TTK anlamında haksız rekabet teşkil edecek hem de TCK m. 239 kapsamında cezaî sorumluluğa yol açacaktır.

D. Ceza Hukuku

Sır kavramının ceza hukuku boyutu, 5237 sayılı Türk Ceza Kanunu ile çizilmiştir. TCK m. 136 kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması veya ele geçirilmesi suçunu tanımlayarak kişisel veri mahremiyetini koruma altına almaktadır. Bu madde kişinin rızası veya kanuni dayanak olmaksızın kişisel verilerinin ele geçirilmesini

veya ifşâ edilmesini içermektedir. Örneğin, bir banka çalışanının müşterilerin kimlik veya hesap bilgilerini üçüncü kişilere satması hem kişisel verilerin hukuka aykırı aktarılması suçunu oluşturmaktadır hem de müşteri sırrı ihlali niteliğini taşımaktadır. Bu madde kişisel verilerin gizliliğini ihlal eden fiileri kapsar ve re'sen soruşturulur, böylece özel hayatın gizliliği kamu otoritesince cezaî yaptırımlara konu olur.

TCK m. 239, ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgilerin yetkisiz kişilere açıklanmasını suç olarak tanımlamakta ve bu fiillere cezaî yaptırımlar öngörmektedir. Bu düzenleme özellikle iş dünyasında ve bankacılık alanındaki gizli bilgilerin korunmasına hizmet etmektedir. Suçun basit hâli şikâyete tâbidir. Dolayısıyla, soruşturma sır sahibi kişinin şikâyeti üzerine başlatılabilmektedir. Bu durum, ticarî sırlar ve müşteri sırlarının çoğu zaman özel hukuk kişisine bağlı olduğunu ve soruşturmanın kişisel talebe bırakıldığını göstermektedir. Öte yandan, bu suç aynı zamanda bireylerin özel hayatının gizliliğini de ihlal edebileceğinden, korunan hukukî değer sadece şirketin veya bankanın menfaati değil, aynı zamanda ilgili kişinin temel haklarıdır. Örneğin, banka müşterisinin bilgilerinin ifşâsı TCK m. 239 kapsamında cezalandırılırken, dolaylı olarak müşterinin mahremiyet hakkı da korunmuş olur.

Uygulamada TCK m. 136 ve TCK m. 239 suçları birleşebilmektedir. Özellikle müşteri sırrı niteliğindeki verilerin aynı zamanda kişisel verileri içermesi durumunda failin eylemi her iki maddeye de uyabilmektedir. Örneğin, bankadan sızdırılan müşteri verilerinde hem ticarî sır hem de kişisel veri niteliği varsa, fail TCK m. 239 yanında TCK m. 136'dan da sorumlu tutulabilir. Böyle bir durumda fikri içtima hükümleri uygulanarak daha ağır cezayı öngören maddeden ceza verilmektedir[39].

TCK m. 239/1. fıkrası, "*görevi gereği sırra vakıf olma*" şartını vurgulayarak özellikle şirket çalışanları, bankacılar, memurlar gibi işi gereği sır niteliği taşıyan bilgilere erişimi olan kişilerin sır saklama yükümlülüğünü ihlal etmelerini suç olarak tanımlamıştır. Örneğin, bir bankanın kredi departmanı çalışanının, müşterilerin kredi skorlarını veya hesap ekstrelerini rakip olan bir finans kurumuna veya basına sızdırması bu suçu oluşturacaktır. Suçun oluşması için gerekli olan bilginin gerçekten sır niteliği taşıyıp taşımadığının takdiri hâkim tarafından, ilgili kanunlar ve somut durum gözetilerek belirlenmektedir. Yargıtay da 07/06/2023 tarihli kararında sanığın ifşâ ettiği bilgilerin ticarî veya müşteri sırrı niteliğinde

[39] Okan Özen, *Ticarî Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu*, Ankara, Seçkin Yayıncılık, 2024, s. 135.

olup olmadığının uzman bilirkişi raporuyla tespitinin gerekli olduğunu belirterek bu niteliğin belirlenmesinin önemini ortaya koymuştur[40].

TCK m. 239'un kapsamı geniş tutulmuş olup, sır niteliğindeki bilgileri dışarıdan hukuka aykırı yolla sırrı elde edip ifşâlayanları da kapsamaktadır. Örneğin, bir hackerın bankanın gizli bilgilerini çalıp yayması da aynı suç tipi içinde değerlendirilmesini gerektirmektedir. Böylece hem içeride sızdırmalar hem de dışarıdan yapılan fiiller ortak bir cezaî koruma alanına alınmıştır. Aynı maddenin 3. fıkrasında sırların yabancı bir ülkeye veya yabancı yetkililere açıklanması hâli ise ağırlaştırıcı bir neden olarak nitelendirilmiş ve cezanın üçte bir oranında artırılacağı, bu durumda şikâyet aranmayacağı belirtilmiştir. Bu düzenleme sırrın ifşâsının ülke dışına çıkması durumunda kamusal zararın daha büyük olabileceği düşüncesine dayanmaktadır. 4. fıkrada ise cebir veya tehdit kullanılarak bir kimseyi sırrını açıklamaya zorlamayı ayrı bir suç olarak düzenleyerek bu fiile 3 yıldan 7 yıla kadar hapis cezası öngörmüştür.

Bununla birlikte, ticarî sır ve kişisel verilerin korunmasına ilişkin suçların uygulanmasında kastın varlığı da belirleyici bir unsur olmaktadır. TCK m. 239'da düzenlenen '*ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçu'* kasten işlenebilen bir suçtur, bu sebeple failin sır niteliğini bilerek ve isteyerek ifşâ etmesi aranır. Bu çerçevede Yargıtay 04/04/2019 tarihli kararında, sanığın şirket verilerini kişisel bilgisayarına kopyalaması olayında söz konusu verilerin gerçekten sır niteliğinde olup olmadığının uzman raporuyla belirlenmesi gerektiğini ancak verilerin üçüncü kişilere aktarıldığına ifşâ edildiğine dair delil bulunmadığından mahkûmiyet hükmünün bozulması gerektiğini belirtmiştir. Bu karar, sır niteliği taşıyan verilerin ayırt edilmesinin ve failin kastının ispatının suçun oluşumu açısından önemli olduğunu ortaya koymaktadır[41].

Öte yandan, Yargıtay'ın 20/09/2021 tarihli bir diğer kararında, müşteri sırrının ifşâsında asıl korunan değerin finansal sistemin işleyişi ve taraflar arasındaki güven ilişkisi olduğu vurgulanmıştır. Bu nedenle fiilin maddi bir zarar doğurup doğurmadığına bakılmaksızın müşteri verilerinin yetkisiz bir şekilde sanığın kendi e-posta adresine

[40] Bkz. Yargıtay 5.CD 07/06/2023 Tarih ve E.2020/6015, K.2023/7213 sayılı kararı. (www.yargitay.gov.tr E.T.:01.08.2025)
[41] Bkz. Yargıtay 15. CD 04/04/2019 Tarih ve E.2017/6957, K.2019/3420 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

gönderilmesinin suçun oluşumu için yeterli sayıldığını ifade etmiştir[42]. Her iki karar birlikte değerlendirildiğinde, Yargıtay'ın somut olaya göre farklı kararlar verdiği görülmektedir. Kastın varlığının tartışmalı olduğu durumda sırrın ifşa edilip edilmediğinin tespitinin önem kazandığı, buna karşılık kastın açıkça ortada olduğu durumda fiilin bir zarar doğurup doğurmadığına bakılmaksızın sırların yetkisiz bir şekilde aktarılmasının suçun oluşumu için yeterli görüldüğü anlaşılmaktadır. Bu yaklaşım ceza hukukunun sırların korunmasında hem bireysel hem de kamusal menfaatleri gözeten caydırıcı bir görev üstlendiğini ve sır saklama yükümlülüğünün kamusal düzenin bir parçası olarak değerlendirildiğini göstermektedir.

E. Kişisel Verilerin Korunması Kanunu

6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesi ve korunmasına ilişkin hükümler içerir. Bu kanun, kişisel verilerin korunmasını isteme hakkını somutlaştırırken aynı zamanda sır kavramıyla da örtüşen hükümler içermektedir. Nitekim birçok kişisel veri niteliği itibarıyla sahibinin sırrı konumundadır. KVKK m. 5 kişisel verilerin işlenme şartlarını düzenlemektedir. Kural olarak kişisel veriler ilgili kişinin açık rızası olmaksızın işlenememektedir. Ancak aynı maddede sayılan hukuka uygunluk sebepleri açık rıza olmaksızın veri işlemenin mümkün olduğu istisnai hâlleri belirtmektedir. Bankalar bu istisnai durumlara dayanarak müşterilerin kredi bilgilerini açık rıza aranmaksızın Risk Merkezi'ne aktarabilmektedirler. Bu durum KVKK m. 5/2-a istisnasını kapsamaktadır. Örneğin, bir bankanın müşterinin adres bilgisini, kredi kartı gönderimi için kullanması sözleşmenin ifası ile ilgili olduğundan rızasız işlenebilecektir. Ancak bu durumlarda bile işleme faaliyetlerinin amaçla bağlantılı, sınırlı ve ölçülü olması KVKK m. 4'teki genel ilkelerdendir.

KVKK m. 6 ise özel nitelikli kişisel verileri düzenler ve kural olarak bu verilerin işlenmesi yasaklar. Özel nitelikli verilere sağlık verileri, biyometrik ve genetik veriler, dini inanç, siyasî düşünce, dernek ve vakıf üyelikleri, ceza mahkûmiyeti gibi hassas veriler girmektedir. Bankacılık sektöründe müşterinin bu özel nitelikli verileri ödeme kayıtları üzerinden dolaylı olarak da olsa işlenebilmektedir. Müşteri sırrı kavramıyla direkt olarak ilgili olmasa da özel nitelikli veriler de yüksek gizlilik gerektirdiğinden, bankaların bu tür

[42] Bkz. Yargıtay 7. CD 20/09/2021 Tarih ve E.2021/14580, K.2021/10255 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

verileri işlerken hem KVKK hem de Bankacılık Kanunu'nun gizlilik hükümlerine uyması gerekmektedir.

KVKK m. 8 ise kişisel verilerin üçüncü kişilere aktarılmasını düzenlemektedir. Maddeye göre kişisel verilerin yurt içinde üçüncü bir kişiye aktarımı tıpkı m. 5'teki gibi işleme şartına tâbidir. Yani ilgili kişinin rızası mevcut değilse, ancak kanundaki istisna hâller mevcut olduğu takdirde aktarım yapılabilecektir. Yurt dışına aktarımlarda ise m. 9'da ayrıca düzenlenerek ilgili ülkenin yeterli koruması veya Türkiye'deki gerekli otoriteden izin gibi şartlar aranır. Bankaların müşteri bilgilerini sigorta şirketine, pazarlama şirketine veya herhangi bir üçüncü tarafa aktarımı KVKK m. 8 kapsamında aktarım faaliyeti sayılır. Bu noktada KVKK ve Bankacılık Kanunu hükümleri, müşteri sırrı niteliğindeki kişisel verilerin kural olarak ilgilinin rızası olmaksızın verilmemesini önemseyerek aynı amacı paylaşır. KVKK m. 8'e göre bankaların müşterilerinin verilerini rıza olmaksızın paylaşımı yasaktır. Ancak kanuni yükümlülük veya meşru menfaat durumlarında, gerekli ölçüde üçüncü kişilere aktarılabileceği belirtilir. Örneğin, sahtecilik şüphesi nedeniyle bir müşterinin işlem detaylarını BDDK ve MASAK ile paylaşmak kanunen zorunludur ve KVKK m. 8 uyarınca bu aktarım hukuka uygundur. Buna karşılık, bir bankanın müşterinin iletişim bilgilerini rızası olmaksızın bir telekomünikasyon şirketine satması ne Bankacılık Kanunu m. 73 ne de KVKK m. 8 bakımından mümkündür.

KVKK yalnızca verilerin işlenme ve aktarım şartlarını düzenlemekle kalmaz, aynı zamanda verilerin güvenliği ve gizliliğine ilişkin yükümlülükler de öngörür. Özellikle KVKK m. 12/4 uyarınca, banka gibi veri sorumluları ile veri işleyenler ve bunların çalışanları, görevleri sırasında öğrendikleri müşteri verilerini kanuna aykırı olarak başkasına açıklayamaz ve amacı dışında kullanamaz. Görüldüğü üzere KVKK, veri sorumluları açısından adeta genel bir sır saklama zorunluluğu getirmektedir.

Nitekim KVKK Kurulu'nun 12/01/2021 tarihli bir kararında bir banka çalışanının müşteri verilerini boşanma davasında kullanmak üzere eşine vermesi olayı, veri güvenliğini sağlama yükümlülüğünün ihlali olarak değerlendirilmiştir[43]. Bu yaklaşım, veri sorumlularına adeta genel bir sır saklama yükümlülüğü yüklendiğini ve bu yükümlülüğün yalnızca teknik değil, aynı zamanda kurumsal farkındalık ve kontrol mekanizmalarını da içerdiğini göstermektedir. Bu yükümlülüklere aykırı davranılması hâlinde ise KVKK m. 18

[43] KVKK Kurulu 12/01/2021 Tarih ve 2021/32 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)

uyarınca idarî para cezası uygulanması söz konusu olabilmektedir. Dikkat çeken diğer bir karar ise Yargıtay'ın 24/03/2010 tarihli kararıdır. Bu karara göre sırrın ifşâsında hesap sahibinin rızasının bulunmasının dahi eylemi hukuka uygun kılmamaktadır[44]. Bu karar, sır saklama yükümlülüğünün sadece bireysel müşteri menfaatini değil, aynı zamanda finansal sistemin bütünlüğüne ve kamu güvenine hizmet eden kamusal bir nitelik taşıdığını ortaya koymaktadır.

KVKK ve Bankacılık Kanunu hükümleri beraber değerlendirildiği takdirde, bu iki düzenlemenin paralel ve bütüncül olduğu ortadadır. Bankacılık Kanunu, ihlal durumunda cezaî yaptırımlar öngörürken KVKK idarî yaptırımlar öngörmektedir. Bir bankanın müşteri sırrını ihlal eden çalışanı hem TCK 239 kapsamında ceza sorumluluğu hem de KVKK idarî para cezası ile hem de iş akdinin feshi gibi sonuçlarla karşılaşabilecektir. Bu çok katmanlı koruma müşteri sırrının işlenmesi ve aktarılmasında oldukça sıkı bir rejim doğurur. Bununla birlikte iki düzenlemenin de öngörmediği gri alanlar uygulamada sorun yaratabilmektedir. Örneğin, müşteri verilerinin ne kadar süreyle saklanacağı, verilerin anonimleştirilme yöntemlerinin ne derece uygulanacağı, açık rızanın geri alınması gibi konularda belirsizlikler mevcuttur. Bu açıklıklar, KVKK ilkeleri ve Bankacılık etiğinden hareketle yorum yapılarak ve KVKK Kurulu tarafından doldurulmaktadır.

F. Bankacılık Kanunu m. 73.

5411 sayılı Bankacılık Kanunu m. 73 Türkiye'de banka ve müşteri sırrının korunmasına ilişkin temel düzenlemedir. Bu hüküm bankacılık faaliyetleri sırasında edinilen sır niteliğindeki bilgilerin ifşâ edilmemesini esas almaktadır ve sır saklama yükümlülüğünü bankalara, bankaların yönetim organı üyeleri ve çalışanlarına, ayrıca ilgili kurum personeli dâhil, görevi gereği bu bilgilere erişebilen kişilere yüklemektedir. Aynı hükme göre, bankaların dışarıdan hizmet aldığı kişiler ve hizmeti sunan çalışanları da sır saklama yükümlülüğüne tâbidir. Bu şekilde bankacılık sisteminde sır kapsamındaki bilgilerin dolaşımı sadece belirli sınırlar içinde tutulmaya çalışılmış ve görevli olmayan kişilere sızmasının önüne geçilmesi amaçlanmıştır[45].

Müşteri sırrı kavramı BankK. m. 73'te açıkça tanımlanmasa da, uygulamada bankaların müşterileriyle olan ilişkileri kapsamında elde ettikleri her türlü bilgi ve belge

[44] Bkz. Yargıtay 7. CD 24/03/2010 Tarih ve E.2007/15770, K.2010/5483 sayılı kararı. (www.kazanci.com.tr E.T.: 01.08.2025)
[45] Adalet Hazar, Şenol Babuşçu, s. 143.

müşteri sırrı olarak kabul edilmektedir. BankK. m. 73'e göre bankalar, müşterilerine ait bilgileri yalnızca müşterilerinin açık rızasıyla veya kanunun açıkça izin verdiği hâllerde üçüncü kişilerle paylaşabilmektedirler. Kanun, bu yükümlülüğe ile müşterilerin bankaya duyduğu güvenin korunmasını amaçlamaktadır.

BankK. m. 73 sır saklama yükümlülüğünün istisnalarını da dolaylı olarak düzenlemektedir. Örneğin 4. fıkrasında müşterinin açık rızasıyla veya kanuni zorunluluk hâllerinde bilgilerin yetkili mercilere verilebileceği ifade edilmiştir. Ayrıca Kanun'un 159. maddesi denetim ve gözetimle görevli kamu kurum ve kuruluşlarının talebi hâlinde de bankaların her türlü bilgi ve belgeyi temin etmekle yükümlü olduğunu düzenlemiştir. Bu maddeye göre, BDDK, TCMB, MASAK gibi yasal olarak yetkilendirilmiş otoritelerin talebi hâlinde banka sırlarının bu mercilerle paylaşılması, sır saklamanın ihlali niteliği taşımayacaktır. Örneğin, MASAK kara para aklama incelemesi kapsamında bir bankadan şüpheli müşterinin hesap kayıtlarını istediğinde banka bu bilgileri vermek zorundadır. Bu durum kanundan kaynaklanan yükümlülüklerin banka sırlarına üstün tutulduğunu ve gereken hâllerde müşteri bilgisinin paylaşımının hukuka aykırı görülmediğini ortaya koymaktadır.

BankK. m. 73 ile BDDK'ya banka ve müşteri sırlarının paylaşım esaslarını belirleme yetkisi tanınmıştır. Bu kapsamda, BDDK 4 Haziran 2021 tarihinde Resmî Gazete'de yayımlanan "*Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik*" ile banka ve müşteri sırrı niteliği taşıyan bilgilerin hangi usûl ve esaslarla üçüncü kişilere aktarılabileceğini düzenlemiştir[46]. 2022 başında yürürlüğe giren bu yönetmelik, sır saklama yükümlülüğünü pekiştirirken bazı yeni ilkeler getirmiştir. Örneğin, bir gerçek veya tüzel kişinin bankanın müşterisi olduğuna dair bilginin dahi müşteri sırrı kapsamında olduğunu belirtilmiştir. Yönetmelik istisnai hâlleri de detaylandırarak kanunen yetkili mercilerle paylaşımlar dışında, diğer istisnai paylaşımlarda iki temel şart aramıştır: gizlilik sözleşmesi ve verinin sadece belirtilen amaçla sınırlı kullanımı. Örneğin, bir banka risk yönetimi amacıyla grup şirketine müşteri sırrını aktarmak isterse, bu şirketle kapsamlı bir gizlilik sözleşmesi imzalamalı ve veriyi sadece bu amaçla ve gerekli ölçüde paylaşmalıdır. Yönetmelik aynı zamanda grup içi paylaşımlarını mümkün kılmakla beraber her bir paylaşımın BDDK'ya raporlanması ve paylaşımın ölçülülük ilkesine uygun olarak

[46] Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik, Sayı: 31501, 4 Haziran 2021. https://www.resmigazete.gov.tr/eskiler/2021/06/20210604-6.htm (E.T.: 01.08.2025)

yapılması, verilerin mümkün olduğunca anonimleştirilmesi gibi şartlar öngörmektedir. Bu detaylar müşteri sırlarının korunmasında dinamik bir düzenleme anlayışının benimsendiğini ve uluslararası standartlara yaklaşılmaya çalışıldığını ortaya koymaktadır.

5. Sır Kavramının Uluslararası Düzenlemelerdeki Yeri

Dijitalleşen çağın etkisiyle, bireylerin özel hayatlarının gizliliği ve kişisel verilerinin korunması yalnızca ulusal hukuk sistemlerinin değil, aynı zamanda uluslararası hukuk düzeninin de temel konularından biri hâline gelmiştir. Modern uluslararası hukukta sır kavramı, yalnızca bireylerin özel yaşamına ilişkin bilgilerinin korunmasını değil, aynı zamanda ekonomik ve ticarî menfaatlerinin de güvence altına alınması amacıyla kapsamlı olarak ele alınmıştır.

Bu bağlamda, sır kavramına ilişkin uluslararası düzeyde olan en temel belgelerden biri, 1948 tarihli İnsan Hakları Evrensel Beyannamesidir[47]. Beyanname'nin 12. Maddesi sır kavramını, özel hayatın, konutun, ailenin ve haberleşmenin gizliliğini temel alan bir insan hakkı olarak tanımlamaktadır ve bu alanlara keyfi müdahaleyi yasaklamaktadır. Bu hüküm, uluslararası düzeyde mahremiyet hakkının ve sır kavramının korunmasına yönelik ilk sistematik adımı temsil etmektedir.

İnsan Hakları Evrensel Beyannamesi'nin devamı niteliğindeki 1966 tarihli Medenî ve Siyasî Haklara İlişkin Uluslararası Sözleşme (International Covenant on Civil and Political Rights– ICCPR), 17. maddesinde benzer bir yaklaşımla "*hiç kimsenin özel yaşamına, ailesine, konutuna veya yazışmalarına keyfi veya hukuka aykırı müdahaleye maruz bırakılamayacağını*" düzenlemiş ve devletlere bireylerin özel hayatlarına yönelik müdahaleleri önleme sorumluluğunu yüklemiştir[48]. Bu hükmün kapsamı, Birleşmiş Milletler İnsan Hakları Komitesi'nin 1994 tarihli "*Toonen v. Australia*" kararında genişletilmiştir [49]. Avustralya vatandaşı Nicholas Toonen'in başvurusu üzerine Komite, Tazmanya Eyaleti'nde yürürlükte olan eşcinsel bireyleri cezalandıran ceza normlarının bireyin özel yaşamına müdahale oluşturduğuna ve Medenî ve Siyasal Haklara İlişkin Uluslararası Sözleşme'nin

[47] BM, İnsan Hakları Evrensel Beyannamesi (Universal Declaration of Human Rights), 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights (E.T.: 01.08.2025)
[48] BM, Medenî ve Siyasal Haklara İlişkin Uluslararası Sözleşme (International Covenant on Civil and Political Rights (ICCPR)), 1966. https://www.ohchr.org/sites/default/files/ccpr.pdf (E.T.: 01.08.2025)
[49] İnsan Hakları Komitesi (Human Rights Committee), "Toonen v. Australia kararı", Başvuru No. 488/1992, 1994. http://hrlibrary.umn.edu/undocs/html/vws488.htm (E.T.: 01.08.2025)

17. maddesinin ihlal edildiğine karar vermiştir[50]. Kararda özel yaşamın yalnızca fiziksel mekânla sınırlı olmadığı, bireyin kendisine ilişkin bilgiler üzerindeki kontrolünün de özel hayatın bir parçası olduğu vurgulanmış ve kişisel verilerin korunması hakkı özel hayatın gizliliğinin ayrılmaz bir unsuru olarak yorumlanmıştır. Bu karar, sır kavramının geleneksel gizlilik anlayışıyla sınırlandırılmaması gerektiğini ve bireyin kendi verileri üzerindeki hakimiyetinin daha geniş bir çerçevede ele alınması gerektiğini göstermektedir.

Uluslararası alanda önemli diğer bir belge olan, OECD tarafından yayımlanan 1980 tarihli Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımı Hakkında Rehber İlkeler, veri koruma hukukunun temel ilkelerini ortaya koymuştur. Söz konusu belgede, veri kalitesi, veri sahibinin bilgilendirilmesi, veri güvenliği, amaca uygunluk, erişim ve düzeltme hakkı gibi ilkelerin yanı sıra, sınır ötesi veri aktarımında yeterli koruma yükümlülüğü gibi kritik düzenlemelere yer verilmiştir[51]. Bu ilkeler, yalnızca dönemsel bir çerçeve sunmakla kalmamış, özellikle Avrupa Birliği'nin 1995 tarihli Veri Koruma Yönergesi (Directive 95/46/EC) başta olmak üzere pek çok ülkenin ulusal mevzuatına doğrudan etki etmiş ve GDPR gibi modern düzenlemelere ilham kaynağı olmuştur[52].

Asya-Pasifik bölgesinde ise 2004 yılında kabul edilen ve 2005'te yayımlanan ve veri koruma standartlarının entegrasyonunu amaçlayan APEC Privacy Framework, sınır ötesi veri transferlerinde sır kavramının korunmasına yönelik GDPR'nin benimsediği katı ve merkezî denetim modeline kıyasla daha esnek, iş birliğine dayalı ve uygulamaya dönük bir yaklaşım getirmiştir. APEC sistemi veri koruma yükümlülüklerinin yalnızca kamu otoriteleriyle değil, özel sektörün katılımıyla da yerine getirilebileceği fikrine dayanır[53].

Bu çerçevenin uygulanabilirliğini artırmak amacıyla, APEC 2011 yılında Sınır Ötesi Gizlilik Kuralları (Cross-Border Privacy Rules– CBPR) sistemini geliştirmiştir. Bu sistemde şirketler "*Accountability Agent*" olarak adlandırılan yetkili ve bağımsız kuruluşlara başvurarak gizlilik politikalarının CBPR ilkelerine uygunluğunu denetletir. Uyum sağlandığında şirket, APEC ülkeleri arasında geçerli olan resmî bir gizlilik sertifikası elde

[50] Medenî ve Siyasal Haklara İlişkin Uluslararası Sözleşme, m. 17.
[51] OECD, "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımı Hakkında Rehber İlkeler", s. 3.
[52] Graham Greenleaf, "2013 Küresel Veri Mahremiyeti Yasaları (Global Data Privacy Laws 2013)", *Privacy Laws & Business International Report*, Sayı 122, 2014, s. 7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034 (E.T.: 01.08.2025)
[53] APEC, "APEC Gizlilik Çerçevesi (APEC Privacy Framework)", 2005, s. 32. https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1 (E.T.: 01.08.2025)

eder[54]. Bu mekanizma sayesinde hem veri sahiplerinin güveni artmakta hem de sınır ötesi ticarette yasal uyumluluk sorunları en aza inmektedir.

Avrupa'da sır kavramı, 1981 yılında kabul edilen 108 No'lu Avrupa Konseyi Sözleşmesi ile normatif bir çerçeveye oturtulmuştur. Bu sözleşme, kişisel verilerin otomatik işlenmesine ilişkin koruma standartları getirerek veri güvenliği ve gizliliği alanında uluslararası iş birliğini teşvik etmiştir[55]. Ayrıca, 2018 yılında yürürlüğe giren 108+ Protokolü ile bu sözleşmenin kapsamı genişletilmiş, algoritmaların ve yapay zekâ sistemlerinin veri işleme süreçlerindeki etkileri dikkate alınarak otomatik karar alma süreçlerinde şeffaflık, insan müdahalesi hakkı ve ayrımcılık yasağı gibi yeni koruma mekanizmaları öngörülmüştür[56].

Avrupa Birliği bünyesinde 2016 yılında kabul edilen ve 2018 yılında yürürlüğe giren GDPR, sır kavramını modern bir çerçevede yeniden tanımlamış ve kapsamlı düzenlemeler getirmiştir. GDPR sadece kişisel verilerin korunmasını değil, aynı zamanda bireylerin bu veriler üzerindeki aktif kontrol hakkını da güvence altına almıştır[57]. Bu bağlamda, açık rıza ilkesi, veri sahibinin erişim, düzeltme, silme gibi temel hakları ile veri işleyenlere şeffaflık ve hesap verebilirlik yükümlülükleri getirilmiştir. Ayrıca kişisel veri ihlallerinin bildirilmesi zorunluluğu, ağır idarî para cezaları gibi mekanizmalar sisteme dâhil edilmiştir. GDPR, yalnızca Avrupa Birliği sınırları içerisindeki veri işleyiciler için değil, AB vatandaşlarının verilerini işleyen tüm kurumlar için geçerlilik taşımaktadır. Bu geçerlilik Avrupa Adalet Divanı'nın 2019 tarihli Google v. CNIL kararında açıkça vurgulanarak veri sorumlularının yalnızca AB içinde değil, AB vatandaşlarının verilerinin işlendiği her yerde GDPR standartlarına uyum sağlamakla yükümlü oldukları belirtilmiştir[58].

Sır kavramı, bireysel hakların yanı sıra ticarî menfaatlerin korunması açısından da uluslararası düzeyde önem taşımaktadır. Dünya Fikri Mülkiyet Örgütü (World Intellectual

---

[54] APEC, "Sınır Ötesi Gizlilik Kuralları (CBPR) Sistemi: Politikalar, Kurallar ve Rehberler *(*Cross-Border Privacy Rules (CBPR) System: Policies, Rules and Guidelines)", 2019, s. 4. https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf (E.T.: 01.08.2025)

[55] Avrupa Konseyi (Council of Europe), Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunmasına İlişkin Sözleşme (Sözleşme 108) *(*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data– Convention 108), 1981, s. 1. https://rm.coe.int/1680078b37 (E.T.: 01.08.2025)

[56] Avrupa Konseyi, Kişisel Verilerin Otomatik İşlenmesine İlişkin Sözleşmeyi Değiştiren Protokol (Sözleşme 108+) *(*Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*)*, CETS No. 223, 2018, s. 6. https://rm.coe.int/16808ac918 (E.T.: 01.08.2025)

[57] GDPR, m. 1, 3, 5, 7.

[58] GDPR, m. 3.; Avrupa Birliği Adalet Divanı (CJEU), Google v. CNIL, C-507/17, 2019. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17 (E.T.: 01.08.2025)

Property Organization– WIPO) tarafından yayımlanan "*Trade Secrets Protection*" rehberinde ticarî sırların ifşâsı haksız rekabet, gizlilik yükümlülüğünün ihlali ve ekonomik zarar kaynağı olarak nitelendirilmiştir. Rehberde ticarî sırların korunmasına ilişkin ilkeler belirlenmiştir[59]. Böylelikle sır ihlalleri sadece kişisel menfaatin değil, aynı zamanda kamusal çıkarların da zarar gördüğü bir kavram niteliği kazanmıştır[60].

Özetle, sır kavramının uluslararası hukukta da bireysel hakların korunması ve finansal sistemin güvenliğinin sağlanması açısından çift yönlü bir anlamı vardır. Dijitalleşme, yapay zekâ ve sınır ötesi veri akışlarının hızlandığı günümüzde sır kavramı yalnızca bireysel mahremiyetin değil, aynı zamanda uluslararası finansal düzenin de ayrılmaz bir parçası hâline gelmiştir. Bu sebeple düzenlemeler, teknoloji ve veri ekonomisinin dinamiklerine uyum sağlayacak şekilde sürekli olarak güncellenmektedir.

II. MÜŞTERİ SIRRI KAVRAMI

Müşteri sırrı kavramı, bankacılık faaliyetleri kapsamında, müşteriyle banka arasındaki güven ilişkisi çerçevesinde doğan ve müşterinin finansal, ekonomik veya kişisel durumuna dair her türlü bilgiyi içeren bir kavramdır[61]. Bankanın müşterisine ait kimlik bilgileri, hesap hareketleri, kredi kayıtları, mevduat durumu, finansal raporları, kişinin hangi bankayla çalıştığı bilgisi dahi müşteri sırrı olarak nitelendirilir[62]. Bu bilgilerin, müşterinin şahsi, ticarî veya malî durumuna ilişkin olması sebebiyle üçüncü bir kişi ile paylaşılması durumunda müşteri güveni sarsılabilmektedir. Bu yönüyle müşteri sırrı, bankacılık faaliyetleri içinde hem hukukî hem de etik yönleriyle korunması gereken çok boyutlu bir kavram niteliği taşımaktadır. Nitekim Yargıtay'ın 11/03/2019 tarihli bir kararına göre, müşterinin kredi kartı hesap dökümlerinin rıza dışı üçüncü kişiye aktarılması banka sırrının ihlali olarak nitelendirilmiş ve bu durum hukuka aykırı bir saldırı olarak nitelendirilerek banka aleyhine manevi tazminata hükmedilmiştir[63].

Benzer olarak, Yargıtay'ın 13/02/2025 tarihli kararında da bir mahkeme dosyasına talep edilmeyen dönemlere ilişkin müşteri hesap bilgilerini sunan bankanın sır saklama

[59] WIPO, "Ticarî Sırlar (Trade Secrets)". https://www.wipo.int/en/web/trade-secrets (E.T.: 01.08.2025)
[60] WIPO, "Ticarî Sırların Korunması: Uluslararası ve Ulusal Yaklaşımlara Genel Bakış, Protection of Trade Secrets: An Overview of International and National Approaches)", s. 6. https://www.wipo.int/publications/en/details.jsp?id=4528 (E.T.: 01.08.2025)
[61] Burak Başel, s. 74.
[62] İlknur Kaya, s. 151.
[63] Bkz. Yargıtay 11.HD 11/03/2019 Tarih ve E.2017/5213, K.2019/2006 sayılı kararı. (www.lexpera.com.tr E.T.: 01.08.2025)

yükümlülüğünü ihlal ettiği kabul edilmiştir. Kararda, bu bilgilerin daha sonra kimliği tespit edilemeyen kişilerce internet ortamında yayınlanmasının, bankanın kusur ve sorumluluğunu ortadan kaldırmadığı gibi zarar ve eylem arasındaki illiyet bağını kesmeyeceği vurgulanmıştır[64]. Bu karar ve benzeri içtihatlar, müşteri sırrının bankacılık sektöründe ne denli korunması gereken bir değer olduğunu ortaya koymaktadır.

Müşteri sırrı kavramı, bankacılık hizmeti alan bireylerin özel hayatının gizliliği hakkını ve finansal mahremiyetini güvence altına almakla beraber, bankaların itibarını ve sektörün geneline duyulan güveni koruyan bir nitelik taşımaktadır. AYM kararlarında da vurgulandığı üzere, müşteri sırrı yalnızca bireysel menfaatler için değil, finansal sistemin istikrarı ve güveni için de korunmaktadır. Bu nedenle fail somut bir zarara sebep olmasa dahi, bilgiyi ifşâ etmesi suçun oluşumu için yeterli kabul edilmektedir[65].

Bireysel müşterilerin kişisel ve malî verilerinin yanı sıra tüzel kişi müşterilere ait finansal bilgiler de müşteri sırrı kapsamındadır. Örneğin, bir bankanın kurumsal müşterisinin cirosu, krediyi geri ödeme performansı ya da çek ve senet bilgileri de müşteri sırrı niteliği taşımaktadır. Sadece gerçek kişilere dair kişisel verileri değil, tüzel kişilere ait finansal verileri de kapsaması bakımından müşteri sırrı, kişisel veriden daha geniş bir nitelik taşımaktadır. Nitekim bir şirketin bankadaki kredi limit bilgisi kesinlikle müşteri sırrıdır ancak o bilginin kişisel veri olup olmadığı tartışılabilir. Bu bakımdan müşteri sırrının hukukî koruması, veri sahibinin gerçek kişi olup olmamasına bakılmaksızın devreye girer. Diğer yandan, pratikte bankacılık işlemlerinden doğan sırların büyük kısmı aynı zamanda kişisel veri niteliği taşımaktadır. Başka bir deyişle, çoğu zaman bir bilginin hem müşteri sırrı hem de kişisel veri niteliği taşıdığı söylenebilir. Bu sebeple bankacılık sektöründe müşteri sırlarının korunması ile kişisel verilerin korunması çoğunlukla birbirini tamamlamaktadır. Ortak noktaları ise gizlilik ve güvene dayalı ilişkilerin muhafazası olmaktadır. Ancak müşteri sırrı kavramı, özellikle bankacılık ilişkisinde güven ve ticarî sır boyutunu da içerdiğinden kişisel veri korumasından ayrılan yönlere sahiptir.

Müşteri sırrı, öncelikle banka ve müşteri arasındaki sözleşmesel güven ilişkisine dayalı bir hukukî yükümlülük olarak karşımıza çıkar. Bankalar müşterilerinin kendilerine duyduğu güvene istinaden elde etmiş oldukları bilgileri, aralarındaki sözleşme ve ilgili mevzuat

[64] Bkz. Yargıtay 4.HD 13/02/2025 Tarih ve E.2022/3953, K.2025/2404 sayılı kararı. (www.lexpera.com.tr E.T.: 01.08.2025)
[65] AYM 03/03/2025 Tarih ve E.2022/32, K.2025/67 sayılı kararı. (www.anayasa.gov.tr E.T.: 01.08.2025)

hükümleri gereğince gizli tutmakla yükümlüdür. Bu yükümlülük, hesap sözleşmesi, kredi sözleşmesi gibi bankacılık sözleşmelerinin zımni bir unsuru olarak kabul edilir. Nitekim müşteri verilerini bankaya sunarken bu verilerin meşru bir neden olmadıkça banka tarafından ifşâ edilmemesini bekler. Sözleşmesel sadakat ve gizlilik borcu gereğince banka da bu beklentiye uygun davranmak zorundadır.

Bunun yanı sıra müşteri sırrı kişilik haklarının korunması ve özel hayatın gizliliği ilkeleriyle de yakından ilişkilidir. Müşteriye ait finansal veriler çoğu zaman onun özel hayatının bir parçasını oluşturmaktadır. Örneğin, harcama alışkanlıkları, malvarlığı, borçları gibi bilgiler kişinin mahremiyet alanının içindedir. Bu sebeple, müşteri sırrının korunması aynı zamanda Anayasa'da güvence altına alınan özel hayatın gizliliği hakkının bir uzantısı olarak görülmektedir. Nitekim AYM 12/11/2015 tarihli bir kararında kişisel verilerin (bankacılık verileri de bu kapsamdadır) bireyin özel hayatının ayrılmaz bir parçası olduğunu, bu verilerin izinsiz paylaşımının temel hak ihlali sayılacağını açık bir şekilde ifade etmiştir[66]. Bu karardan anlaşılmaktadır ki, müşteri sırrı sözleşmeden doğan nispi bir hak olmanın yanı sıra anayasal temelli ve üçüncü kişilere karşı da ileri sürülebilen bir kişilik hakkı niteliği taşımaktadır.

Müşteri sırrının hukukî dayanakları, ulusal ve uluslararası düzenlemelerdir. Türk hukukunda bankaların sır saklama yükümlülüğüne ilişkin açık hükümler bulunmaktadır. Bu hükümlere göre bankalar ve çalışanlarına müşteriye ait verileri koruma görevi yüklenmektedir. Bu yasal yükümlülük görevden ayrılan banka çalışanlarını dahi kapsamaktadır. Çalışanlar, görevleri dolayısıyla öğrendikleri müşteri verilerini kurumdan ayrılsa bile ifşâ edemeyeceklerdir. Aksi bir davranış söz konusu olduğunda ise suç kapsamında caydırıcı yaptırımlarla karşı karşıya kalabileceklerdir. Bu durum müşteri sırrı korumasının mutlak ve süreklilik arz eden bir borç olduğunu ortaya koymaktadır.

Yargı kararları da müşteri sırrının hukukî niteliğini destekler mahiyettedir. Yargıtay Hukuk Genel Kurulu'nun 22/11/2018 tarihli bir kararında, bankanın internet bankacılığı hizmetinde gerekli güvenlik önlemlerini almamasını hizmet kusuru olarak değerlendirilmiş ve banka ağır kusurlu görülmüştür. Somut olayda bir bankanın internet bankacılığı sistemindeki güvenlik açığı sebebiyle müşterinin hesabı üzerinden yetkisiz EFT işlemleri gerçekleştirilmiştir. Yargıtay, bankanın gerekli teknik güvenlik önlemleri almamasını

[66] AYM 12/11/2015 Tarih ve E.2015/32, K.2015/102 sayılı kararı. (www.anayasa.gov.tr E.T.: 01.08.2025)

tazminat sorumluluğu doğuran ağır bir kusur olarak görmüştür. Bu karar müşteri sırrının korunmasının yalnızca sırrı ifşâ etmeme şeklinde pasif bir yükümlülük olmadığını, aynı zamanda bankaların aktif olarak veri güvenliği tedbirlerini alma sorumluluğu taşıdığını göstermektedir[67].

Müşteri sırrının korunması, bankacılık sektörünün güvenilirliği ve sürdürülebilirliği açısından önem taşımaktadır. Bankacılık sektörüne duyulan güven, müşterilerin bankalara emanet ettikleri bilgilerin kötüye kullanılmayacağı beklentisi üzerine inşa edilmektedir. Müşteriler finansal mahremiyetlerinin teminat altına alındığına inanırlarsa bankalara rahatça bilgilerini verir ve işlemlerini sürdürürler. Bu güven ortamı müşteri ve banka ilişkisini güçlendirirken finansal sistemin itibar ve istikrarını sağlar. Nitekim bankaların müşteri sırrına riayet etmemesi yalnızca bireysel düzeyde hukukî sorunlar doğurmakla kalmayıp sektöre duyulan genel güveni sarsarak sistemin bütününe zarar verebilir. Örneğin, bir bankada yaşanan ciddi bir gizlilik ihlali haberi, tüm bankalara yönelik bir güvensizlik algısı yaratarak finansal piyasaların kötü etkilenmesine sebep olabilir. Dolayısıyla, müşteri verilerinin korunmasının, bankaların itibarını korumanın yanında finansal istikrar açısından önem arz ettiği söylenebilir.

Bankacılık faaliyetlerinde müşteri sırrının önemi ekonomik güvenlik boyutuyla da öne çıkar. Özellikle dijital bankacılığın ve büyük çaplı veri paylaşımına dayalı sistemlerin geliştiği ve verilerin toplandığı Risk Merkezi gibi bir kuruluşun oluşturulduğu günümüzde, müşteriye ait verinin sızması tek bir bireyi aşan toplumsal etkiler doğurabilmektedir. Bu sebeple düzenleyici otoriteler, yargı mercileri müşteri sırlarını korumayı kamusal düzenin bir parçası olarak ele almakta ve ihlaller karşısında ağır idarî para cezaları, tazminatlar ve cezaî yaptırımlar uygulamaktadır.

Müşteri sırrının önemi uluslararası alanda da göze çarpmaktadır. 1934 tarihli İsviçre Bankacılık Kanunu, banka müşterisine ait bilgilerin ifşâsını suç sayarak ihlal eden bankacılar için üç yıla kadar hapis cezası öngörmüştür. Her ne kadar son yıllarda uluslararası vergi şeffaflığı ve kara para ile mücadele baskılarıyla İsviçre bankacılık gizliliğini belli ölçüde esnetse de banka sırrını ceza tehdidiyle koruyan bu yaklaşım, İsviçre'ye küresel finans piyasalarında "*gizliliğin kalesi*" unvanını kazandırmıştır.

[67] Bkz. YHGK 22/11/2018 Tarih ve E.2017/2224, K.2018/1753 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

Müşteri sırrını korumak günümüzde bankaların uyacağı basit bir gizlilik kuralı olmanın ötesine geçerek hukukî, teknolojik ve sosyoekonomik boyutları olan bir kavram hâline gelmiştir. Bu değişime paralel olarak ulusal alanda KVKK, uluslararası düzeyde ise GDPR finansal verilerin işlenmesinde şeffaflık, izin, amaçla sınırlılık, veri minimizasyonu gibi ilkeler getirerek müşteri verilerinin işlenmesi ve üçüncü kişilerle paylaşılmasına önemli sınırlamalar getirmektedir. Bu çerçevede, bankalar ve finans kuruluşları müşteri bilgilerini ancak öngörülmüş olan hukukî sınırlar çerçevesinde işleyebilmekte ve müşterinin açık rızası olmaksızın bu bilgileri üçüncü kişilerle paylaşamamaktadır. Bu düzenlemelere uyulmadığı takdirde ise GDPR m. 83 uyarınca, kişisel verilerin korunmasına ilişkin yükümlülükleri ihlal eden kuruluşlar hakkında idarî para cezaları ve çeşitli yaptırımlar öngörülmektedir[68].

III. RİSK MERKEZİ KAVRAMI

1. Risk Kavramının Doğuşu ve Gelişimi

Risk kavramı insanlık tarihinin başlangıcından itibaren var olmakla beraber, bireylerin ve toplumların bilinmezlikler karşısında geliştirdikleri savunma mekanizmalarıyla sistemik bir yapı kazanmıştır. Riskin modern anlamda değerlendirilmesi ise, özellikle 17. yüzyılda olasılık teorisinin gelişmesiyle hız kazanmıştır[69]. Bu dönemde, özellikle deniz ticareti ve sigortacılık faaliyetleri sırasında karşılaşılan belirsizliklerin ölçülmesinin ihtiyacı, riskin metodik şekilde ele alınmasına sebep olmuştur[70].

20. yüzyıla gelindiğinde, finansal piyasaların genişlemesi sebebiyle artan ekonomik karmaşıklıklar riskin çok boyutlu biçimde değerlendirilmesini kaçınılmaz hâle getirmiştir. Artık risk sadece öngörülemeyen zararları değil fırsatları da içeren bir yönetim unsuru olarak, izlenmesi ve denetlenmesi zorunlu bir hâle gelmiştir[71]. Bu bağlamda kurumsal risk yönetimi anlayışı ortaya çıkarak kurumların yalnızca finansal değil, operasyonel, stratejik, itibar, uyum, siber güvenlik ve çevresel risklerini de içerecek şekilde ele alınmasına neden olmuştur[72]. Treadway Komisyonu Destekleyici Kuruluşlar Komitesi (Committee of

---

[68] GDPR, m. 5, 6, 7, 83.
[69] Peter L Bernstein, *Tanrılara Karşı: Riskin Olağanüstü Tarihi (Against the Gods: The Remarkable Story of Risk)*, John Wiley & Sons, 1996, s. 50.
[70] Mehmet Saraç ve Mehmet Burak Kahyaoğlu, "Risk Algısının Tarihsel Gelişimi", *Finans Politik ve Ekonomik Yorumlar*, Cilt 48, Sayı 556, 2011, s. 32.
[71] Saraç ve Kahyaoğlu, s. 37.
[72] Robert S. Kaplan ve Anette Mikes. "Risklerin Yönetimi: Yeni Bir Çerçeve (Managing Risks: A New Framework)", *Harvard Business Review*, 2012. https://hbr.org/2012/06/managing-risks-a-new-framework (E.T.: 01.08.2025)

Sponsoring Organizations of the Treadway Commission– COSO) tarafından geliştirilen "*Kurumsal Risk Yönetimi-Entegre Çerçeve*" modeli, riskin organizasyonel olarak kurumsallaşmasına hizmet etmektedir[73]. Benzer şekilde, Avrupa Merkez Bankası (European Central Bank– ECB)'nın 2024 tarihli Risk Kültürü Kılavuzunda da risk yönetimi sadece hesaplamaya dayalı bir faaliyet değil, aynı zamanda organizasyonel davranışın ve etik kültürün iç içe olduğu bir sistem olarak tanımlanır. Bu anlayış, risk farkındalığını tüm organizasyon geneline yaymayı amaçlamaktadır[74].

Türkiye'de ise risk yönetimi kültürü, 2001 finansal krizi sonrasında ivme kazanmış ve 6102 sayılı Türk Ticaret Kanunu ile yasal çerçeveye kavuşturulmuştur. Bankacılık sektöründe ise BDDK'nın düzenlemeleriyle iç denetim, risk yönetimi ve uyum birimlerinin kurulmasıyla kurumsal bir yapı tesis edilmiştir. Tüm bu gelişmelerle beraber sadece risk tespiti değil, riskin izlenmesi, değerlendirilmesi ve kurumsal yönetim süreçlerine aktarılması da sistematik bir yapıya kavuşturulmuştur. Bu kurumsal yapının merkezinde, uluslararası alanda da kabul görmüş olan "*üç savunma hattı*" modeli yer almaktadır. Bu modelde birinci savunma hattı operasyonel birimleri, ikinci hat risk kontrol ve uyum birimlerini, üçüncü hat ise bağımsız iç denetimi kapsamaktadır[75].

2. Risk Merkezi'nin Kurumsal Önemi ve İşleyişi

Türkiye'de Türkiye Bankalar Birliği bünyesinde faaliyet gösteren Risk Merkezi, bankacılık sektöründe ve finansal sektörde hizmet veren kuruluşlar tarafından bildirilen kredi ve borç bilgilerini merkezî bir sistemde toplayan, raporlayan ve ilgili kurumlarla paylaşan bir yapıdır[76]. Finansal risklerin etkin olarak izlenmesi amacıyla kurumsal düzeyde oluşturulan Risk Merkezi mikro düzeyde bireysel kredi risklerinin tespiti, makro düzeyde ise finansal sistemin istikrarı açısından önemli bir işlev üstlenmektedir.

Bu bağlamda, sadece finansal kuruluşlar için değil, Risk Merkezi gibi veriye dayalı karar süreçlerinde aktif rol üstlenen kurumlar için de benimsenen "*üç savunma hattı modeli*"

---

[73] Mehmet Mert Şener, "Kurumsal Risk Yönetimi Üzerine Bir Yazın Taraması", *Akademik Sosyal Araştırmalar Dergisi*, Cilt 6, Sayı 71, 2018, s. 461.

[74] ECB, "Yönetişim ve Risk Kültürüne İlişkin Taslak Kılavuz (Draft Guide on Governance and Risk Culture)", 2024, s. 7. https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon202407_draftguide.en.pdf (E.T.: 01.08.2025)

[75] Marc Eulerich, "Kurumsal Yönetişimin Yapılandırılması İçin Yeni Üç Hat Modeli (The New Three Lines Model for Structuring Corporate Governance)", *SSRN Elektronik Dergisi (SSRN Electronic Journal)*, 2021, s. 181. https://doi.org/10.2139/ssrn.3777392 (E.T.: 01.08.2025)

[76] Türkiye Bankalar Birliği, Risk Merkezi Yönetmeliği, Resmî Gazete, Sayı 28260, 2012, m. 3/ğ. https://www.resmigazete.gov.tr/eskiler/2012/04/20120410-5.htm (E.T.: 01.08.2025)

risk yönetiminin kurumsal sistematiğini oluşturmaktadır[77]. Söz konusu modelin çıkış kaynağı tam olarak bilinmemekle beraber, kurumsal yapıların karşı karşıya olduğu risklerin sistematik bir yaklaşımla izlenmesini, denetlenmesini ve yönetilmesini amaçlamaktadır. Temel dayanağı ise görev, yetki ve sorumlulukların birbirinden ayrıldığı üç katmanlı bir yapıdır. Birinci savunma hattı operasyonel birimleri, ikinci hat risk kontrol ve uyum birimlerini, üçüncü hat ise bağımsız iç denetimi kapsamaktadır. Bu üçlü yapı sayesinde, risklerin etkin bir şekilde tespiti, analizi ve kontrol altında tutulması mümkün olmaktadır[78].

Birinci savunma hattı, doğrudan kurumun operasyonel faaliyetlerini yürüten birimleridir[79]. Satış, pazarlama, kredi tahsis, operasyon, insan kaynakları gibi departmanlar birinci hattı oluşturan birimlere örnektir. Bu birimler, operasyonel faaliyetlerden kaynaklanan risklerin ilk ortaya çıktığı düzeyde yer almaktadır. Temel görevleri ise riski zamanında tespit ederek uygun kontrol mekanizmalarıyla ortadan kaldırmak veya kabul edilebilir bir seviyeye indirmektir. Riskin ilk koşulu olan kaynağında tanınması ve süreçlere entegre olarak yönetilmesi bu sayede mümkün olur[80].

İkinci savunma hattı, birinci hat tarafından yürütülen faaliyetlerin risk boyutunu değerlendiren ve gerekli kontrolleri sağlayan yapıdır. Bu katmanda yer alan risk yönetimi, iç kontrol ve uyum birimleri doğrudan operasyon yürütmez, yalnızca operasyonel birimlerinin işleyişini gözetler ve değerlendirir. Örneğin, risk yönetimi birimi kurumun risk toleransına uygun şekilde hareket edilip edilmediğini izlerken uyum birimi ise yasal düzenlemelere ve iç politikalara uyumunu denetler. Aynı zamanda kurumun genel risk stratejisinin oluşturulmasından, risklerin sınıflandırılmasından ve kontrol sistemlerinin yapılandırılmasından da sorumludur[81].

Üçüncü savunma hattı ise tamamen bağımsız çalışan iç denetim birimidir. Bu birim, birinci ve ikinci savunma hatlarının işlevlerini ne ölçüde yerine getirdiğini değerlendirir ve kurumun yönetim kuruluna doğrudan raporlama yaparak risk yönetiminin güvenilirliğini

---

[77] KKB, TBB Risk Merkezi Hizmetleri, 2025. https://www.kkb.com.tr/urunler/tbb-risk-merkezi-hizmetleri (E.T.: 01.08.2025)

[78] İç Denetçiler Enstitüsü (Institute of Internal Auditors - IIA), "Etkili Risk Yönetimi ve Kontrolde Üç Hatlı Savunma Modeli (The Three Lines of Defense in Effective Risk Management and Control)", 2013, s. 2. https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf (E.T.: 01.08.2025)

[79] IIA, s. 2.

[80] IIA, s. 3.

[81] Halil İbrahim Özbilger, "İç Denetime Yeni Bir Bakış: Üçlü Hat Modelinin Değerlendirilmesi," *Denetişim Dergisi*, Sayı 22, 2020, s. 43.

pekiştirir. İç denetim birimi, süreçlerin bağımsız olarak denetlenmesini sağlayarak kurumun bütüncül risk ve kontrol sisteminin işlerliğini teminat altına alır[82].

Üç savunma hattı modeli, sorumlulukların net olarak ayrılarak çakışma riskinin azaltıldığı ve kontrol mekanizmalarının birbirini tamamladığı bir sistem inşâ etmektedir. Bu sayede kurumlar sadece riskleri tanımlamakla kalmayıp onları analiz eder, kontrol altına alır ve zamanında aksiyon alarak zararın oluşmasını önleyebilir. Bu model, finans sektörü, kamu kurumları, büyük ölçekli şirketler ve sivil toplum kuruluşları tarafından benimsenmiş, yaygınlaşmış ve iç kontrol sistemlerinin vazgeçilmez bir bileşeni hâline gelmiştir. Ayrıca bu modelle, risklerin yalnızca üst yönetimin sorumluluğu olmadığı, tüm çalışanların katılımıyla yönetilmesi gereken dinamik bir süreç olduğu fikri, kurum kültürüne yerleştirilmektedir[83].

IV. RİSK MERKEZİNİN TARİHÇESİ VE YAPISAL GELİŞİMİ

Türkiye'de Risk Merkezi'nin tarihsel gelişimi, kredi sisteminde bilgi paylaşımının kurumsallaştırılması doğrultusunda şekillenmiştir. Bu amaçla ilk olarak, bankalar arası bilgi paylaşımını sağlama görevini, 1951 yılında TCMB bünyesinde kurulan Risk Santralizasyon Sistemi üstlenmiştir. TCMB nezdinde kurulmuş olan bu merkez, yalnızca bankaların müşterilerine ilişkin kredi risk bilgilerini toplayarak bu verilerin bankalar arasında paylaşılmasını amaçlamıştır. Bankalara kişilerin kredi borcunun olup olmadığı gibi bilgileri TCMB'ye müracaat ederek öğrenme imkânı sağlanmıştır[84].

Risk Merkezi'nin görev, yetki ve işleyişine ilişkin esaslar, 10 Nisan 2012 tarihli ve 28260 sayılı Resmî Gazete'de yayımlanan Risk Merkezi Yönetmeliği ile belirlenmiştir[85]. 6111 sayılı Kanun ile 5411 sayılı Bankacılık Kanunu'na eklenen 73/a maddesi uyarınca daha önce TCMB bünyesinde faaliyet gösteren Risk Santralizasyon Sistemi'nin görevleri TBB nezdinde kurulan Risk Merkezi'ne devredilmiştir[86]. Bu yapısal dönüşüm 28.06.2013 itibarıyla hayata geçirilmeye başlanmıştır.

---

[82] Halil İbrahim Özbilger, s. 43.
[83] IIA, s. 2.
[84] Adalet Hazar, Şenol Babuşçu, *Banka Hukuku*, Ankara, Seçkin Yayıncılık, 4. Baskı, 2025, s. 211.
[85] https://www.resmigazete.gov.tr/eskiler/2012/04/20120410-4.htm (E.T.: 01.08.2025)
[86] TCMB, "Risk Merkezi Duyurusu (DUY-2013/48)", 2013. https://www.tcmb.gov.tr/wps/wcm/connect/8064278a-fe74-4add-acc5-d4b9b40d0ca3/DUY2013-48.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-8064278a-fe74-4add-acc5-d4b9b40d0ca3-m3fC8mf (E.T.: 01.08.2025)

Öte yandan, bilgi paylaşımını daha etkin hâle getirmek amacıyla 1995 yılında Türkiye'deki dokuz banka aracılığıyla, özel sektör girişimiyle kurulan Kredi Kayıt Bürosu A.Ş. faaliyete geçirilmiştir[87]. BankK. m. 73/4'te öngörüldüğü üzere en az beş banka tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişini sağlamak üzere kurulmuş olan KKB'de üye statüsünde bulunan kuruluşlar, müşterilerine ait kredi bilgilerini Nisan 1999'dan bu yana birbirleriyle paylaşmaktadırlar. KKB, Risk Merkezi ile hukuken doğrudan bir bağa sahip olmamakla beraber faaliyetlerine Risk Merkezi'nin teknik ve operasyonel altyapı hizmet sağlayıcısı olarak işlev göstermektedir[88].

Risk Merkezi'nin yapısı yalnızca bankaları değil, aynı zamanda faktöring, finansman ve leasing şirketlerini de kapsayacak biçimde geniş tutulmuştur. Bu gelişme, özellikle EBA tarafından yayımlanan Guidelines on Loan Origination and Monitoring *(*Kredi Verme ve İzleme Rehberi) gibi düzenlemelerde, veri kalite kriterlerinin netleştirilmesi, otomatik skor sistemlerinin denetlenebilirliği ve algoritmik karar alma süreçlerinde şeffaflık gibi öne çıkan risklerin izlenmesi yönündeki eğilimle uyum sağlamaktadır. Türkiye, bu doğrultuda başta kredi verilerinin merkezî raporlama sistemleri olmak üzere önemli adımlar atmış ve Risk Merkezi'nin kurumsal yetkisini veri şeffaflığı üzerinden güçlendirmiştir. Günümüzde TBB tarafından aylık olarak yayımlanan Risk Merkezi bültenleri aracılığıyla, piyasadaki toplam bireysel ve kurumsal borçlanma durumu, tasfiye olunacak alacak miktarı ve karşılıksız çek istatistikleri gibi temel veriler düzenli şekilde kamuoyuyla paylaşılmaktadır. Bu da Risk Merkezi'ni yalnızca veri sağlayıcı değil, aynı zamanda piyasayı dengeleyen şeffaf bir otorite konumuna taşımıştır.

Özellikle 2014 yılı itibarıyla Risk Merkezi'nin dijital dönüşüm süreci hız kazanmış ve bu kapsamda veri güvenliğini temel alan modern bir raporlama sistemi geliştirilmiştir. Bu sistemle beraber kredi bilgilerinin düzenli olarak dijital ortamda toplanması, karşılaştırmalı analizlerin yapılması ve ilgili kurumlar tarafından hızlıca erişim sağlanması mümkün kılınmıştır. Bu sayede Risk Merkezi'nin bankacılık sistemi içerisindeki işlevi güçlendirilmiştir.

Risk Merkezi, bankalar ve diğer kuruluşlardan toplamış olduğu geçmiş kredi bilgilerini dijital ortamda analiz ederek şeffaflığı artırmaya yönelik kurulmuş önemli bir otorite konumundadır. Ancak bu dijital dönüşümün hukukî ve kurumsal altyapısının da aynı

[87] KKB, *2021 Faaliyet Raporu*. https://www.kkb.com.tr/faaliyetraporu2021/tr/m-1-1.html (E.T.: 01.08.2025)
[88] KKB, Tarihçe. https://www.kkb.com.tr/hakkimizda (E.T.: 01.08.2025)

ölçüde gelişmesine ihtiyaç vardır. Kredi raporlama süreçlerinde otomatik karar destek mekanizmalarının güçlendirilmesi gerekmektedir. Türkiye'nin bu eksiklikleri gidermek amacıyla Avrupa Birliği gelişmeleriyle paralel olarak veri yönetimi sistemleri ve kurumsal denetim mekanizmalarını hayata geçirme sürecinde olduğu gözlenmektedir.

V. BANKA İLE MÜŞTERİ ARASINDAKİ İLİŞKİ

Banka ile müşteri arasındaki sır ilişkisi, bankacılık sektörüne güvenin inşâsında temel unsurdur. Bu ilişki yalnızca bireysel mahremiyetin korunması bakımından değil, aynı zamanda finansal sistemin işleyişinin temini ve sektöre duyulan güvenin sürdürülmesine katkı bakımından da önem arz etmektedir. Bankacılık Etik İlkeleri'ne göre bankacılık sektöründe istikrar ve güvenin korunması meslekî onurun bir gereği olarak kabul edilmektedir. Bu çerçevede müşteri güveninin sağlanması bankacılık sisteminin istikrarı için temel koşul olduğundan, bankaların müşterilerine ait finansal verileri gizli tutma yükümlülüğü hem yasal hem de sözleşmesel yükümlülüklerle desteklenmektedir[89].

Banka ile müşteri arasındaki ilişki, çoğunlukla mevduat sözleşmesi veya kredi sözleşmesi gibi sözleşmelere dayanmaktadır ve bu sözleşmelerde banka, müşterinin rızası olmaksızın hiçbir kişisel bilgisini üçüncü şahıslarla paylaşmayacağını taahhüt etmektedir. Ancak bu durumun istisnaları bulunmaktadır[90]. Örneğin, bankalar, adlî makamların talepleri doğrultusunda, kanunen yetkilendirilmiş kurumlarla müşteri bilgilerini paylaşmak zorundadır[91]. Ayrıca, müşterinin rızasının olması durumunda, bankalar belirli üçüncü taraflarla veri paylaşımında bulunabilirler, fakat bu paylaşımın yine yasal sınırlar çerçevesinde olması gerekmektedir[92].

Müşteri sırrı yalnızca sözleşme süresince değil, sözleşme öncesi (culpa in contrahendo) görüşmelerde edinilen veriler ile sözleşmenin sona ermesinden sonra da menfaatin devam ettiği ölçüde korunmaktadır. Bu bağlamda, sır saklama yükümlülüğü

[89] İlknur Kaya, s. 149.
[90] Selin Kurt, *Ticarî Sır, Bankacılık Sırrı Veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu,* Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2019, s. 49.
[91] Gurbet Arife Yıldırım, Banka Çalışanlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Müşteri Sırlarını Koruma Yükümlülükleri", Yüksek Lisans Tezi, Ufuk Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2021, s. 72.
[92] Selin Kurt, s. 34.

yalnızca sözleşmeye değil, aynı zamanda dürüstlük kuralı gibi genel hukuk ilkelerine de dayanmaktadır[93].

Bankaların müşteri bilgilerini koruma yükümlülüğü yalnızca sözleşme süresiyle sınırlı olmamaktadır. Tüm bu yükümlülükler müşteriyle olan sözleşmesel ilişkinin sona ermesi durumunda dahi devam etmektedir. Örneğin, bir müşterinin bankadaki mevduat hesabını kapatması veya bankayla olan kredi ilişkisinin sona ermesi, bankanın bu müşteriye ait edindiği sır niteliğindeki bilgileri açıklamasına imkân vermemektedir. Müşterinin kredi geçmişi, ödeme alışkanlıkları veya hesap hareketleri gibi bilgiler sır niteliğini korumaya devam etmektedir. Nitekim KVKK Kurulu'nun 02/11/2021 tarihli kararı da bu yaklaşımı desteklemektedir. Banka nezdinde hesaplarını kapatmış olan eski bir müşteriye pazarlama amaçlı SMS gönderilmesi hukuka aykırı bulunmuş ve ilgili bankaya idarî para cezası uygulanmıştır[94]. Bu yaklaşım ile müşteri bilgilerini korumanın pasif bir sır saklama yükümlülüğünden öte ilişki sona erdikten sonra kullanmama yükümlülüğünü de kapsadığını göstermektedir.

Bankalar müşterilerinden edindikleri bilgileri saklamakla yükümlüdür[95]. Bu yükümlülük, yalnızca müşterilerinin özel hayatının gizliliğini korumayı değil, aynı zamanda ticarî ve finansal sırlarını muhafaza etmeyi de kapsamaktadır[96]. Bu çerçevede, müşterilerin hesap bilgileri, kredi durumu, bankacılık işlemleri ve finansal analizleri gibi ekonomik içerikli bilgileri sır niteliği taşımakla beraber; doğrudan sır niteliği taşımayan ancak müşteri ile ilgili olabilecek bilgiler de müşteri sırrı kapsamına dâhil edilerek geniş bir koruma sunulmaktadır[97]. Örneğin, şube tercihleri, işlem sıklığı, banka hizmetlerinden yararlanma eğilimleri, bankayla kurulan ilişkinin süresi veya kampanyalara katılım durumu gibi dolaylı nitelikteki bilgiler de gizlilik yükümlülüğü çerçevesinde korunmaktadır[98].

Ek olarak, her ne kadar müşteri sırrı niteliği taşımıyor olsa da bankacılık faaliyetleri sırasında edinilen bazı bilgilerin açıklanması durumunda sır saklama yükümlülüğünün ihlali söz konusu olabilmektedir ve üçüncü kişilere ait bilgiler dahi müşteri sırrı kapsamına

---

[93] Selin Kurt, s. 31.
[94] Bkz. KVKK Kurulu'nun 02/11/2021 Tarih ve 2021/1104 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)
[95] Yaşar Alıcı, s. 1288.
[96] Pınar Çağla Kandıralıoğlu, "Türk Hukukunda Bankaların Sır Saklama Yükümlülüğü", Doktora Tezi, İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 76.
[97] İlknur Kaya, s. 157.
[98] BDDK, Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik, 2021, m. 4 ve 5. https://www.resmigazete.gov.tr/eskiler/2021/06/20210604-6.htm (E.T.: 01.08.2025)

girebilmektedir[99]. Örneğin, bir kredi sözleşmesi kapsamında bankaya sunulan belgelerde yer alan kefile ilişkin veriler veya teminata konu taşınmaza ait bilgiler doğrudan müşteri sırrı olmasa da dolaylı olarak gizlilik yükümlülüğü kapsamında korunmaktadır.

Dijital bankacılığın gelişmesiyle beraber artan müşteri verilerine yetkisiz erişim riski sebebiyle, bankaların veri koruma politikalarını ve siber güvenlik önlemlerini güçlendirerek müşteri verilerini koruma konusunda daha dikkatli davranmaları gerekmektedir. Banka ile müşteri arasındaki güven ilişkisinin temeli olan gizlilik yükümlülüğü, yasal düzenlemelerle geliştirilip teknolojik gelişmelerle desteklenerek daha sağlam bir yapıya kavuşturulmalıdır. Nitekim Adana Bölge Adliye Mahkemesi'nin 20/09/2022 tarihli kararına göre, bankalar internet bankacılığı işlemlerinde işlem yapanın gerçek müşteri olup olmadığını belirleme bakımından, gelişen dolandırıcılık yöntemlerine karşı bunları önleyici gerekli altyapıyı sağlayarak güvenlik önlemlerini almak zorundadır[100].

VI. MÜŞTERİYE İLİŞKİN SIR NİTELİĞİNDEKİ BİLGİ VE BELGELER

Bankacılık sektöründe müşteriyle kurulan ilişkinin temelinde güven ilkesi yer almakta olup bu güvenin sağlanması büyük ölçüde müşteriye ait bilgilerin gizliliğine bağlıdır. Bu nedenle müşterilere ilişkin bilgi ve belgelerin sır kapsamında değerlendirilmesi yalnızca ticarî bir yükümlülük olarak değil, 5411 sayılı BankK. 73. maddesi, 6698 sayılı KVKK ve AY 20. maddesi hükümleriyle güvence altına alınmış anayasal bir hak olarak karşımıza çıkmaktadır.

BankK. 73. maddesinde düzenlenen banka sırrı kavramı, müşteri bilgilerinin koruması bakımından emredici bir hükümdür. Bu hükme göre, bankaların yönetim kurulu üyeleri, çalışanları, banka adına hareket eden kişiler, denetim birimleri, destek hizmeti sağlayan kuruluşları ve bağımsız denetim firmaları edindikleri müşteri bilgilerini yasal zorunluluklar dışında açıklayamaz. Sır saklama yükümlülüğünün ihlali hâlinde, banka çalışanının hizmet sözleşmesi sona ermiş veya kişi işten ayrılmış olsa dâhi banka eski çalışanının fiili nedeniyle sorumlu tutulmaktadır[101].

Bankacılık Kanunu'nda, müşteri sırrı kavramını sınırlayıcı şekilde tanımlamaktan kaçınılmış ve uygulamada geniş bir takdir alanı bırakılmıştır. Nitekim müşteri sırrı, sadece

[99] İlknur Kaya, s. 194.
[100] Adana BAM 9.HD 20/09/2022 Tarih ve E.2020/749, K.2022/1089 sayılı kararı. (www.lexpera.com.tr E.T.: 01.08.2025)
[101] İlknur Kaya, s. 176.

ad, soyad, TCKN ya da hesap numarası gibi dar kapsamlı bilgilerle sınırlı değildir[102]. Banka ile müşteri arasında kurulan hukukî ve ticarî ilişkinin her aşamasında doğrudan ya da dolaylı şekilde edinilen ve müşteriyi tanımlamaya yarayan her türlü bilgi, müşteri sırrı kapsamında değerlendirilmelidir.

Bu kapsamda sır niteliği taşıyan belgeler, müşteriyle ilk temas anından itibaren doğrudan veya dolaylı olarak edinilen bilgi ve belgelerden oluşur. Bunlar arasında müşterinin hesap hareketleri, kredi başvuruları, teminat bilgileri, borç ödeme geçmişi, yatırım eğilimleri, teminat mektupları, kefalet bilgileri, dijital işlem alışkanlıkları, finansal analiz raporları ve kredi notu gibi birçok veri grubu vardır. Söz konusu bilgiler yalnızca bankacılık sözleşmeleri veya formlar gibi fiziksel evraklarda değil, aynı zamanda dijital sistemler, log kayıtları, sesli müşteri hizmetleri görüşmeleri ve otomatik işlem kayıtları gibi çeşitli dijital ortamlarda da işlenmekte ve saklanmaktadır. Tüm bunlar içerikleri itibarıyla müşteri hakkında birçok bilgi içerdiklerinden ve kişisel veri kavramı ile büyük ölçüde örtüştüğünden sır niteliği taşımaktadırlar[103].

Özetle, müşteriyle kurulan bankacılık ilişkisinin her aşamasında elde edilen ve müşteriyi doğrudan veya dolaylı olarak tanımlayan her türlü belge sır niteliğindedir. Bu belgelerin korunması yalnızca ticarî etik açısından değil, aynı zamanda yasal bir yükümlülük olarak değerlendirilmekte ve bu yükümlülüğün ihlali hem hukukî hem cezaî yaptırımlara konu olmaktadır. Bu nedenle bankalar, söz konusu belgeleri yalnızca belirli kişilerle, hukukî dayanağa uygun ve ölçülülük ilkesine bağlı olarak paylaşmak zorundadır[104].

Aynı zamanda, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, müşteri bilgileri kişisel veri olarak kabul edilmekte ve bu verilerin işlenmesi, saklanması ve paylaşılması özel düzenlemelere tâbi kılınmaktadır. KVKK'nin 5. ve 6. maddeleri, kişisel verilerin işlenmesinde meşru amaç, ölçülülük ve veri minimizasyonu ilkelerine bağlı kalınmasını zorunlu kılmaktadır. Bu kapsamda veri sorumlusu sıfatına haiz bankalar, kişisel verilerin hukuka uygun işlenmesi ve korunması için gerekli teknik ve idarî tedbirleri almakla yükümlüdür.

[102] İlknur Kaya, s. 194.
[103] Lee Andrew Bygrave, s. 129.
[104] Güven, Onur Irmak ve Erkan Eren "5411 Sayılı Bankacılık Kanununda Müşteri Sırlarının Tâbi Olduğu Hukukî Rejim ve Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik Üzerine Değerlendirmeler", *Bankacılar Dergisi*, Sayı 122, 2023, s. 2.

Bankaların müşteri verilerini koruma yükümlülüğü, sözleşmesel bir taahhüdün ötesinde cezaî yaptırımlarla desteklenmiş bir zorunluluktur. Banka sırrının ihlali durumunda Türk Ceza Kanunu'nun 239. maddesi uyarınca, cezaî yaptırımlar söz konusu olmaktadır. Bu düzenlemeye göre, görev veya sıfatı gereği müşteri sırlarına vakıf olan kişilerin yetkisiz üçüncü kişilere bilgi aktarması suç teşkil etmekte ve bu kişiler hapis cezası ile cezalandırılmaktadır. Bu düzenleme ile sır saklama yükümlülüğüne aykırılığın özel hukukun yanı sıra kamu hukuku açısından da yaptırımının olduğu görülmektedir. Ek olarak, bu kişiler görevlerinden ayrılmaları durumunda dahi sırları ifşâ edemeyeceklerdir. Nitekim, Danıştay İdari Dava Daireleri Kurulu 07/11/2024 tarihli bir kararına göre, sıfat ve görevleri dolayısıyla banka veya müşterilerine ait sırları öğrenen kişilerin söz konusu sırları kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamayacakları ve bu yükümlülüğün görevden ayrıldıktan sonra da devam edeceğine yer verilmiştir[105].

Veri güvenliği bakımından, GDPR m. 32 önem arz etmektedir. Bu madde kapsamında, müşteri verilerinin güvenliğinin sağlanması amacıyla bankaların hukukî sınırlar çerçevesinde kalmanın yanında, uygun teknik ve organizasyonel tedbirleri almakla yükümlü olduğu belirtilmiştir. Bu kapsamda bankalar veri ihlallerine karşı gelişmiş güvenlik önlemleri tesis etmek, risk analizleri yapmak ve ihlal durumu söz konusu olduğunda durumu ilgili veri koruma otoritesine bildirmekle yükümlüdür. GDPR veri ihlali durumunda veri sorumlusu bankalara, ihlalin niteliğine göre yıllık küresel cirolarının %4'üne veya 20 milyon Euro'ya kadar idarî para cezası uygulayabilmektedir[106]. Örneğin, 2019 yılında Avrupa Birliği'nde gündeme gelen bir veri ihlalinde, Romanya'da faaliyet gösteren bir bankanın müşterilerinin şube tercihlerini ve kredi kullanım alışkanlıklarını üçüncü taraf pazarlama şirketleriyle paylaşmasını ağır bir veri koruma ihlali olarak değerlendirilerek bankaya 130.000 Euro idarî para cezası uygulanmıştır[107].

Nitekim Yargıtay Hukuk Genel Kurulu'nun 22/11/2018 tarihli kararında bankaların internet bankacılığı işlemlerinde ağırlaştırılmış özen yükümlülüğü olduğunu ve müşterilerini korumak için gerekli güvenlik tedbirlerini almak zorunda olduğu vurgulanmıştır. Bankanın

[105] Danıştay İDDK 07/11/2024 Tarih ve E.2022/2597, K.2024/2713 sayılı kararı. (www.danistay.gov.tr E.T.: 01.08.2025)
[106] GDPR, m. 83.
[107] Avrupa Veri Koruma Kurulu (European Data Protection Board - EDPB), "Romanya Denetim Kurumu Tarafından Verilen İlk Para Cezası (First Fine By The Romanian Supervisory Authority)", 2019. https://www.edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_en (E.T.: 01.08.2025)

gerekli güvenlik tedbirlerini almaması durumunda sorumluluğunun söz konusu olacağını ve bankanın müşterinin zararını tazminle yükümlü olacağı vurgulanmıştır[108].

Anayasa Mahkemesi'nin 19/03/2015 tarihli kararında açıkça belirtildiği üzere, kişisel veriler bireyin özel hayatının ayrılmaz bir parçasıdır ve bu verilerin izinsiz biçimde işlenmesi temel hakların ihlali anlamına gelmektedir. Mahkeme, kişisel veri korumasını yalnızca yasal düzenlemelerle korunan sınırlı bir hak olarak değil, Anayasa m. 20 uyarınca doğrudan anayasal koruma altındaki bir hak kapsamında değerlendirmiştir. Her ne kadar karar doğrudan müşteri sırrına ilişkin olmasa da, kişisel verilerin anayasal koruma altına alınması ve müşteri bilgilerinin korunmasının sözleşmesel yükümlülüğünün ötesinde anayasal düzeyde bir hakka dayandığının tespiti açısından önemli bir karar niteliği taşımaktadır[109].

GDPR'nin 5. maddesinde öngörülen amaçla sınırlı işleme ilkesi ve 17. maddesinde düzenlenen unutulma hakkı doğrultusunda bireylerin verileri üzerindeki kontrolü güçlendirilmiştir. Örneğin, bankalar müşterilerinden topladıkları verileri yalnızca belirli, açık ve meşru amaçlar doğrultusunda işleyebilmektedir. Bu amaçlar dışında bir işleme faaliyeti gerçekleştirebilmeleri için ilgili kişiden ayrıca açık rıza almaları gerekmektedir. Ayrıca, bireyler bankalardan kendilerine ait olan kişisel verilerin silinmesini talep ederek sözleşme ilişkisinin sona ermesinden sonra dahi veri üzerindeki kontrollerini sürdürebileceklerdir.

İsviçre hukukuna bakıldığı takdirde ise banka gizliliği, bireysel mahremiyeti yıllardır sıkı şekilde ve mutlak bir koruma altında tuttuğu görülmektedir. İsviçre Bankacılık Kanunu'nun 47. maddesinde, banka sırrı koruma altına alınmakla beraber, aynı maddenin 5. fıkrasınca diğer kanunlardan doğan bilgi verme yükümlülüklerini sır korumasının dışında bırakılmaktadır. Böylece kara para aklama, vergi kaçakçılığı ve terörün finansmanı gibi ciddi suçlar söz konusu olduğunda geleneksel banka gizliliğine istisnalar getirilmekte ve gerekli makamlara bilgi verilip gerekli delillerin sunulacağı kabul edilmektedir[110]. Özellikle 2008 küresel finans krizi sonrasında uluslararası şeffaflık baskıları ve kara para aklama ile

[108] Bkz. YHGK 22/11/2018 Tarih ve E.2017/2224, K.2018/1753 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)
[109] Bkz. AYM, 19/03/2015 Tarih ve E.2014/180, K.2015/30 sayılı kararı. (www.anayasa.gov.tr E.T.: 01.08.2025)
[110] İsviçre Bankalar ve Tasarruf Bankaları Federal Yasası (Bankengesetz– BankG / Federal Act on Banks and Savings Banks), m. 47. https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en; Kara Para Aklanmasının Önlenmesine İlişkin Federal Yasa (Geldwäschereigesetz– AMLA / Anti-Money Laundering Act), 2015, m. 9. https://www.fedlex.admin.ch/eli/cc/2015/791/en (E.T.: 01.08.2025)

mücadele gereklilikleri doğrultusunda bu korumaya belirli istisnalar getirilmiş ve İsviçre bankacılık sisteminin geleneksel anlayışında köklü değişiklikler yapılmıştır[111].

Buna paralel olarak İsviçre Federal Yüksek Mahkemesi 2017 tarihli bir kararında, banka sırrının mutlak olmadığını, özellikle vergi kaçakçılığı ve benzeri fiillerin soruşturulması için uluslararası bilgi paylaşımı gerektiğinde banka sırrı korumasının kamu yararı gerekçesiyle sınırlandırılabileceğini ifade etmiştir[112]. Bu sayede İsviçre'nin uluslararası sistemle uyumu artırılmış ve finansal sırları birey ve kurum açısından kamu yararına dengeleyen, uluslararası sistemle entegrasyonu daha güçlü olan bir yapıya evrilmiştir.

Sonuç olarak, müşteriye ait sır niteliğindeki bilgi ve belgeler, kimlik verilerinden finansal verilere, özel hayatı ilgilendiren hassas bilgilerden dijital izlere kadar geniş bir alanı kapsamakta ve hem ulusal hem uluslararası düzeyde çok katmanlı bir koruma sistemine tâbi olmaktadır. Bu bilgilerin hukuka aykırı biçimde paylaşılması hâlinde ise bankalar idarî yaptırımların yanında cezaî yaptırımlar ve tazminat sorumluluğu ile karşı karşıya kalmaktadır.

VII. MÜŞTERİ SIRRININ SAKLANMASINDAKİ YARARDAN DAHA ÜSTÜN ÖZEL VEYA KAMU YARARI

Müşteriye ait bilgiler her ne kadar sır niteliğinde oldukları gerekçesiyle hukukî koruma altına alınmış olsa da bu koruma hâlinin mutlak olmadığını söylemek mümkündür. Özellikle kamu düzeni, kamu güvenliği ya da daha üstün nitelikte özel menfaatlerin varlığı hâlinde müşteri sırrı istisnai de olsa açıklanabilmektedir[113]. Sır saklama yükümlülüğü ile açıklama ihtiyacının çatıştığı hâllerde hâkim, hangi yararın daha ağır bastığını tespit ederek bir karar verecektir.

Türk hukukunda bu dengeyi somutlaştıran en önemli düzenleme, 5411 sayılı Bankacılık Kanunu'nun 73. maddesidir. Buna göre bankalar, müşteri sırrını açıklayamazlar.

---

[111] Tobias Straumann, *Zürih ve Cenevre: Altın Çağın Sonu* (*Zurich and Geneva: The End of the Golden Age)*, International Financial Centres after the Global Financial Crisis and Brexit içinde, Oxford, Oxford University Press, 2018, s. 108.

[112] İsviçre Federal Mahkemesi, "Banka Sırrı ve Kamu Yararı Hakkında Karar (Decision on Bank Secrecy and Public Interest)", 2017, Karar No: 4A_83/2016, BGE 143 II 506. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F143-II-506%3Ade&lang=de&type=show_document (E.T.: 01.08.2025)

[113] İlknur Kaya, s. 241.

Ancak açık rıza, mahkeme kararı, denetim zorunluluğu veya kanuni yetki gibi hâllerde bu gereklilik ortadan kalkmaktadır. Ceza hukuku bakımından ise, müşteri sırrını ifşâ eden kişilere ceza öngörülse de hukuka uygunluk durumu söz konusu olduğu takdirde ifşâ fiili suç teşkil etmeyecektir.

Hukuka uygunluk sebeplerinden biri, daha üstün nitelikte bir özel veya kamu yararının varlığıdır. Örneğin bir kamu kurumu tarafından yürütülen soruşturmada müşterinin banka işlemlerine ilişkin bilgiler, kamu düzeni ve finansal sistemin gözetim ve denetimi amacıyla talep ediliyorsa bankanın sır saklama yükümlülüğü ortadan kalkabilir. Bu noktada üstün yarar, bireysel gizlilikten ağır basmaktadır[114].

ABD'de 1978 tarihli Finansal Mahremiyet Hakkı Yasası (Right to Financial Privacy Act– RFPA), federal devletin bilgilerini talep etmesi hâlinde müşteriye bildirilerek belli bir süre içinde itiraz etme hakkı tanısa da ulusal güvenlik, kamu düzeni veya adlî soruşturmalar gibi istisnai hâllerde bildirim yükümlülüğü ertelenebilmekte veya tamamen kaldırılabilmektedir. Böylece devlet, müşterinin önceden haberdar edilmesine gerek kalmadan finansal verilerine erişim sağlayabilmektedir. Bununla birlikte hem ulusal hem de yabancı hukuk sistemlerinde bu tür açıklamaların mutlak serbestlik taşıdığını söylemek mümkün değildir çünkü ilgili bilginin davayla doğrudan ilgili olması, yalnızca yetkili makama sunulması ve gerekli ölçüde açıklanması gerekmektedir[115]. Aksi takdirde, orantısız müdahale nedeniyle müşteri hakları ihlali söz konusu olacaktır.

Avrupa İnsan Hakları Sözleşmesi (AİHS) m. 8 uyarınca herkesin özel yaşamına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkı bulunmaktadır. Söz konusu hak yalnızca fiziksel mahremiyet ile sınırlı kalmayıp bireyin kimliğinin, kişisel verilerinin ve sır niteliği taşıyan verilerinin korunmasını da kapsamaktadır. Bu hakka yönelik müdahaleler ancak kanunla öngörülmüşse ve demokratik bir toplumda zorunlu olan, ölçülü ve meşru bir amaca dayalı ise hukuken kabul edilebilir nitelik taşır. AİHM, 4 Aralık 2008 tarihli kararında kişisel verilerin süresiz ve ayrım gözetmeksizin muhafaza edilmesini özel yaşam hakkına orantısız bir müdahale olarak değerlendirmiş ve böyle bir uygulamanın

[114] Pınar Çağla Kandıralıoğlu, s. 176.
[115] Amerika Birleşik Devletleri Kanunu (United States Code), Finansal Mahremiyet Hakkı Yasası (Right to Financial Privacy Act), 12 U.S.C. § 3409, 1978. https://www.govinfo.gov/content/pkg/USCODE-2021-title12/html/USCODE-2021-title12-chap35.htm (E.T.: 01.08.2025)

demokratik topluma uygun olmayacağını belirtmiştir[116]. Mahkeme suçsuz bireylerin parmak izi ve DNA gibi verilerinin süresiz olarak muhafazasının, suçlularla aynı muameleye tâbi tutulmaları nedeniyle kişileri damgalama riski taşıdığını ve bunun özel hayatın korunması ilkesiyle bağdaşmadığını eklemiştir. Her ne kadar bu karar doğrudan bankacılık sektöründeki veri işleme faaliyetlerine ilişkin olmasa da, Mahkemenin ortaya koyduğu ilkeler yol gösterici nitelik taşımaktadır. Özellikle bankacılık sektörü gibi veri işleme faaliyetlerinin yoğun olarak yürütüldüğü alanlarda, bireyin kendisi hakkında hangi bilgilerin açıklanıp açıklanmayacağına karar verebilmesi özel yaşam hakkının temel bir yansımasıdır. Bireylerin bu hakkı Avrupa Konseyi ve Avrupa İnsan Hakları Mahkemesi (AİHM)'nin yerleşik içtihatları ile veri gizliliğine ilişkin uluslararası düzenlemeler ile korunmaktadır.

Sonuç olarak, müşteri sırrının açıklanmasının hukukî olabilmesi için daha üstün olan özel ya da kamu yararının varlığı gereklidir. Bu sebeple müşteri sırrının açıklanması mutlak bir yasak olmaktan çok, sınırlı ve denetimli bir istisna niteliğindedir. Sırrı açıklamanın haklı görüldüğü üstün yarar durumlarında dahi, bu açıklamanın sadece gerekli bilgileri kapsaması ve ilgisiz kişilere yayılmaması bir zorunluluktur. Aksi hâlde açıklama, hem müşteri ile hizmet sağlayıcı arasındaki güvenin zedelenmesine hem de kişilik haklarının ihlaline sebep olacak ve Türk Ceza Kanunu m. 239 kapsamında ceza sorumluluğuna yol açacaktır.

VIII. BANKANIN MÜŞTERİ SIRRINI SAKLAMA YÜKÜMLÜLÜĞÜ

1. Bankanın Müşteri Sırrının Saklama Yükümlülüğü ve Kapsamı

Modern finansal sistemde banka, para akışını yöneten bir kurum olmakla beraber müşterilerin kişisel ve ekonomik bilgilerinin de emanet edildiği bir yapıdır. Bu yapının istikrarı, bankanın edindiği bilgileri hangi sınırlar içinde kullanacağına dair yükümlülüklerle yakından ilişkilidir[117]. Bankacılık faaliyetleri sırasında edinilen müşteri verilerinin korunması hem kişisel mahremiyetin güvencesi hem de finansal sistemin bütünlüğü açısından önem taşımaktadır. Bu bağlamda banka, müşterisine ilişkin her türlü veriyi yalnızca işlevsel amaçla işlemeli ve bir gizlilik içerisinde saklamalıdır. Bu sorumluluk

[116] Avrupa İnsan Hakları Mahkemesi (AİHM), S. ve Marper v. *Birleşik Krallık*, Başvuru No. 30562/04 ve 30566/04, 04.12.2008. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]} (E.T.: 01.08.2025)
[117] Güven, Irmak ve Eren, s. 19.

doktrinde ve uygulamada "*müşteri sırrını saklama yükümlülüğü*" olarak adlandırılmaktadır[118].

Müşteri sırrını saklama yükümlülüğü yalnızca veri paylaşımının yasaklanması anlamına gelmez. Müşteri bilgilerine izinsiz erişimin önlenmesi, verinin üçüncü kişiler tarafından kullanılmasının engellenmesi ve iç organizasyon yapısının buna uygun kurgulanması gibi pasif tedbirleri de içerir. Bu yönüyle bankanın sır saklama yükümlülüğü hem pasif bir açıklamama yükümlülüğü hem de aktif bir koruma yükümlülüğü niteliğindedir.

Söz konusu yükümlülük, yalnızca bankaların üst yönetim organlarını değil, aynı zamanda banka personelini, taşeron hizmet sağlayıcılarını, çağrı merkezi çalışanlarını ve bilgi teknolojileri desteği sunan dış firmaları da kapsamaktadır. 5411 sayılı Bankacılık Kanunu'nda bu durum açıkça düzenlenmiş ve sır saklama yükümlülüğü banka dışındaki kişi ve kuruluşlara da teşmil edilmiştir. Zira modern bankacılık sistemlerinde müşteri verileri genellikle dış kaynaklı yazılım altyapılarında tutulmakta veya hizmet sağlayıcılarla paylaşılmaktadır. Bu sebeple yükümlülük yalnızca çalışanlar arası etik ilkeye değil, aynı zamanda teknik erişim sistemleri üzerinde yapılan iç kontrol düzenlemelerine de dayandırılmalıdır.

Müşteri sırrını saklama yükümlülüğü süresiz bir yükümlülük niteliği taşımaktadır. Sözleşmenin sona ermesi, hesabın kapatılması ya da müşteriyle hukukî ilişkinin bitmesi, bu yükümlülüğü sona erdirmemektedir. Örneğin, bir müşteriye ait kredi risk bilgilerinin üçüncü kişilerle paylaşılması, sözleşme sona ermiş olsa dahi sır saklama yükümlülüğünün ihlali niteliği taşımaktadır. Bu doğrultuda müşterinin sırrını saklama yükümlülüğü, ilişkinin devam edip etmediğinden bağımsız olarak banka tarafından süresiz bir şekilde yerine getirilmelidir[119].

Bankacılık Kanunu m. 73 sır saklama yükümlülüğünü düzenlemekte ve açıkça bankaların bu yükümlülüğünü ilişki sona erdikten sonra da devam ettirmesi gerektiğini ortaya koymaktadır. Nitekim bir çalışanın görevi dolayısıyla edindiği müşteri sırrı niteliğindeki bilgileri görevinden ayrıldıktan sonra dahi açıklamasının Bankacılık Kanunu

[118] Güven, Irmak ve Eren, s. 19.
[119] Kemal Doruk Tekin, *Banka Sırrı Kavramı Yönünden Bankalarda Sır Saklama Yükümlülüğü*, Ankara, 2010, s. 19.

m. 73/3 kapsamında suç oluşturduğu ve bu yükümlülüğün görevin sona ermesiyle ortadan kalkmayacağı ortaya konulmuştur.

Banka açısından sır saklama yükümlülüğü sadece bireysel müşterilerle sınırlı olmamaktadır. Kurumsal müşteriler, tüzel kişiler, hatta potansiyel müşteriler bakımından da geçerlidir. Uygulamada, henüz bankacılık ilişkisi kurulmadan önce alınan bilgilerin bile sır kapsamında değerlendirilebileceği kabul edilmektedir[120]. Kişinin kredi talebi reddedilse dahi başvuru esnasında bankaya açıkladığı bilgiler müşteri sırrı niteliği taşımaktadır. Özellikle kredi ön değerlendirme sürecinde, yatırım danışmanlığı tekliflerinde veya kurumsal birleşme öncesi bilgi paylaşımında edinilen veriler sözleşme kurulmamış olsa dâhi müşteri sırrı niteliği taşımaktadırlar. Doktrinde bu çerçevede bankanın potansiyel müşterinin sunduğu bilgi ve belgeleri sözleşme kurulmasa bile ileride başka taraflarla paylaşmaması gerektiği, aksi takdirde hem haksız fiil bakımından hem de güven ilişkisine aykırılık nedeniyle sorumlu tutulabileceği ifade edilmektedir[121].

Müşteri sırrını saklama yükümlülüğü etik açıdan da önem arz eder. Türkiye Bankalar Birliği tarafından yayımlanan Bankacılık Etik İlkeleri'ne göre, banka çalışanları görevleri nedeniyle edindikleri bilgileri sadece yasal zorunluluk hâlinde yetkili mercilere açıklayabilecektir, aksi takdirde bu tür davranışlar hem kurumsal itibar hem de kişisel sorumluluk açısından olumsuz sonuç doğurmaktadır[122].

2. Bankanın Müşteri Sırrının Saklama Yükümlülüğüne İlişkin Tarihsel Süreç

Bankacılık faaliyetlerinde müşteri bilgilerinin korunmasına yönelik sorumluluk, zaman içinde hem etik bir norm hem de hukukî bir zorunluluk hâline gelmiştir. İsviçre Bankacılık Yasası'nın 1934 tarihli düzenlemesiyle banka sırrı cezaî yaptırımlarla koruma altına alınmış ve uluslararası prestij kazanmıştır[123]. Bu yasanın, müşterilerin kimliklerinin dâhi açıklanmasını yasaklayan katı hükümler içermesi, İsviçre bankalarına uluslararası düzeyde bir prestij sağlamış ve bu bankaların tercih sebebi olmasını sağlamıştır.

Bununla birlikte, 20. yüzyılın sonlarına doğru dijitalleşmenin etkisiyle müşteri verilerinin kapsamı genişlemiş, kimlik bilgilerinin yanında işlem alışkanlıkları, kredi

---

[120] Seza Reisoğlu, *Bankacılık Kanunu Şerhi*, Cilt 2, 2. Baskı, 2015, s. 1496.
[121] Seza Reisoğlu, s. 1497.
[122] Türkiye Bankalar Birliği, Bankacılık Etik İlkeleri, 2014, m. 10 ve 19/d. https://www.tbb.org.tr/pdf/faaliyetler/89/702 (E.T.: 01.08.2025)
[123] İlknur Kaya, s. 49.

geçmişi, dijital davranışları gibi bilgiler de sır kapsamında değerlendirilmeye başlanmıştır. Bu dönüşüm, hem müşteri sırrının kapsamını yeniden tanımlamış hem de bankaların sorumluluğunu yalnızca veriyi açıklamama açısından değil, aktif olarak koruma yönünde de geliştirmesini sağlamıştır[124].

Türk hukukunda müşteri sırrı kavramı, direkt olarak ilk kez 1985 tarihli 3182 sayılı Bankalar Kanunu'nda ele alınmıştır. Ancak bu düzenleme teknik anlamda oldukça yetersiz kalmıştır. Müşteri bilgilerinin korunmasına yönelik açık ve sistematik yükümlülükler, 2005 yılında yürürlüğe giren 5411 sayılı Bankacılık Kanunu ile netleşmiştir. Söz konusu Kanunun 73. maddesi, banka nezdindeki bilgilerin yalnızca müşteri rızası veya açık kanuni zorunlulukla paylaşılabileceğini düzenleyerek bu yükümlülüğü hem idarî hem cezaî sorumlulukla pekiştirmiştir. Aynı hüküm, yükümlülüğün yalnızca banka ile sınırlı olmadığını, tüm personel ve hizmet sağlayıcılarını kapsayacak şekilde geniş yorumlanması gerektiğini de ortaya koymuştur.

Müşteri sırrının korunmasına ilişkin bu ulusal düzenlemeler, 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile daha da güçlendirilmiştir. KVKK, müşterilere ait bilgilerin birer kişisel veri olarak değerlendirilmesi gerektiğini açıkça belirtmiştir. Böylece müşteri sırrı kavramı, veri güvenliği ilkeleriyle birleşerek hem özel hayatın gizliliği hem de bilgi güvenliği perspektifinden korunur hâle gelmiştir. Bu süreçte, Avrupa Birliği'nin 2018'de yürürlüğe koyduğu GDPR önemli bir rol model teşkil etmiş ve Türkiye'nin uyum sürecinde KVKK'ye yön vermiştir.

3. Müşteri Sırrını Saklama Yükümlülüğüne İlişkin Hukukî Düzenleme ve Yaptırımlar

Modern bankacılıkta müşteriler ekonomik verilerinin yanında kişisel, malî ve davranışsal verilerini de kuruma teslim etmektedir. Bu durum, bankaların sır saklama yükümlülüğünü yalnızca sözleşmesel bir borç olmaktan çıkarıp çok katmanlı ve normatif boyutta tanımlanması gereken bir yükümlülüğe dönüştürmektedir. Türk hukuk sistemi de bu

[124] Shoshana Zuboff, *Gözetim Kapitalizmi Çağı: İktidarın Yeni Sınırında İnsanlığın Geleceği İçin Mücadele* (*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power),* New York, PublicAffairs, 2019, s. 8.

ihtiyaca cevap vermek amacıyla müşteri sırrına yönelik özel düzenlemeler getirmiş ve müşteri sırrının ihlali durumunda çok yönlü yaptırımlar öngörmüştür[125].

Bu yükümlülüğün temel dayanağı 5411 sayılı Bankacılık Kanunu'nun 73. maddesidir. Maddeye göre, bankaların müşterilerine ait her türlü bilgi ve belgeyi, müşterinin açık rızası olmaksızın veya kanunda açıkça belirtilmiş hâller dışında üçüncü kişilerle paylaşmaları yasaktır. Kanun, yalnızca banka tüzel kişiliğini değil, yönetim kurulu üyelerini, çalışanlarını, dış hizmet sağlayıcılarını ve denetim firmalarını kapsayacak şekilde geniş bir sorumluluk çerçevesi tanımlamıştır. Bu sebeple sır saklama yükümlülüğü bireysel hata ile sınırlı olmaktan çıkarılıp kurumsal ve sistemsel bir sorumluluk olarak karşımıza çıkar. Ancak, 5411 sayılı Bankacılık Kanunu'nun 159. maddesinde bankaların, denetim ve gözetimle yetkili olan kamu kurum ve kuruluşlarının talebi hâlinde her türlü bilgi ve belgeyi sağlamakla yükümlü olduğu da belirtilmiştir. Bu düzenleme, sır saklama yükümlülüğüne kanuni bir istisna oluşturmakta ve yetkili mercilere yapılan veri aktarımını hukuka uygun kılmaktadır.

Ancak uygulamada 159. maddenin sınırlarının açıkça belirlenmemiş olması sebebiyle, müşteri sırrı kapsamındaki bilgilerin yetkili mercilere aktarımında ölçüsüzlük ve keyfiyet durumu söz konusu olabilmektedir. Kamu kurumlarına bilgi verme yükümlülüğü hukukî dayanağa sahip olsa da hangi verilerin, hangi amaç ve kapsamda paylaşılabileceğine dair ayrıntılı bir düzenleme bulunmaması hukuka uygunluk sınırının aşılmasına ve müşteri sırrına yönelik etkin bir koruma sağlanamamasına sebep olmaktadır. Bu maddenin geniş yorumlanmaya elverişliliği sebebiyle, hukukî güvenlik ve öngörülebilirlik ilkelerine uygun biçimde somutlaştırılması gerekmektedir[126].

Bankacılık Kanunu'nun öngördüğü düzenlemeler sadece kuralları belirlemekle kalmayarak ihlalin yaptırımla karşılık bulmasını da garanti altına almaktadır. Bu çerçevede, müşteri sırrının izinsiz açıklanması durumunda banka özel hukuk açısından tazminatla, kamu hukuku açısından ise idarî yaptırım ve cezalarla karşı karşıya kalmaktadır.

Müşteriler Türk Borçlar Kanunu'nun 58. maddesi uyarınca, kişilik haklarının ihlaline dayanarak manevi tazminat talep edilebilmektedir. Özellikle zarara uğrayan kişinin ekonomik ve psikolojik bütünlüğü dikkate alınarak banka tarafından verilen zarar manevi tazminat adı altında bir miktar para olarak telafi edilebilmektedir. Ancak hâkim manevi

[125] Merve Arslanhan, "Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması" *Kişisel Verileri Koruma Dergisi*, Cilt 6, Sayı 2, 2024, s. 39.
[126] Pınar Çağla Kandıralıoğlu, s. 136.

tazminatın ödenmesi yerine diğer bir zararı giderme biçimine karar vererek saldırıyı kınayan bir karara ve bu kararın yayımlanmasına hükmedebilir.

Ceza hukuku yönünden düzenleme ise 5237 sayılı TCK m. 239'da yer almakta olup görevi gereği müşterinin bilgilerini öğrenmiş bir kişinin bu bilgileri açıklaması hâlinde bir yıldan üç yıla kadar hapis ve beş bin güne kadar adlî para cezası öngörülmektedir. Ancak uygulamada TCK'nın 135. ve 136. maddelerinde düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi ve ifşâ edilmesi suçları ile birlikte de değerlendirilmesi mümkündür. Sırrın ifşâsının ekonomik çıkar sağlamak amacıyla veya basın yoluyla gerçekleştirilmesi hâlinde ise cezanın ağırlaştırılması öngörülmüştür. Bu hükmün amacı yalnızca zarar veren fiilleri önlemek değil, aynı zamanda güveni sarsacak potansiyel davranışlara karşı da caydırıcı olmaktır.

İdari yaptırımlar ise BDDK'nın denetim yetkisi kapsamında değerlendirilir. Bankacılık Kanunu'nun 146. ve devamı maddelerine göre, müşteri bilgilerinin izinsiz paylaşılması durumunda banka hakkında idarî para cezası, faaliyet kısıtlaması, yönetim değişikliği talebi, faaliyet izninin iptali gibi çeşitli düzenleyici önlemler alınabilmektedir. Özellikle bilgi güvenliği açıklarının tespit edildiği hâllerde, denetim raporları uyarınca bu yaptırımlar gecikmeksizin uygulanmaktadır.

Ayrıca bu yükümlülük, 6698 sayılı KVKK ile de doğrudan ilişkilidir. Müşteri verileri aynı zamanda bir kişisel veri kabul edildiğinden, KVKK kapsamında işlenen her tür verinin ihlalinde, idarî para cezası veya cezaî sorumluluk gibi sonuçlar doğmaktadır. Örneğin KVKK Kurulu 07/05/2020 tarihli kararında, bir bankanın iç kontrol zafiyetleri nedeniyle müşteri kredi bilgilerinin riskli bir şekilde işlenmesi sebebiyle 450.000 TL idarî para cezası uygulamıştır[127].

Hazine ve Maliye Bakanlığı tarafından 2015 yılında yayımlanan "*Kişisel Verilerin Korunması, Muhafazası ve Paylaşımı*" adlı kılavuzda, kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler ve uygulama örnekleri özetlenmiş ve Türkiye'deki uygulamalar karşılaştırmalı olarak ele alınmıştır. Bu rehberde, Türkiye'deki uygulamaların bu standartlara uyumu teşvik edilmiştir[128].

[127] Bkz. KVKK 07/05/2020 Tarih ve 2020/359 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)
[128] Hazine ve Maliye Bakanlığı, "Kişisel Verilerin Korunması, Muhafazası ve Paylaşımı Rehberi", 2015. https://ms.hmb.gov.tr/uploads/sites/12/2021/02/kisisel_verilerin_korunmasi_ve_paylsim_rehberi.pdf (E.T.: 01.08.2025)

Bu çerçevede TBB tarafından yayımlanan MASAK Şüpheli İşlem Bildirim Rehberi'nde, kara para aklama ile mücadele kapsamında yapılacak işlemlerde dâhi müşteri verilerinin gizliliğine azami özen gösterilmesi gerektiği vurgulanmıştır. Rehberin genel yapısı itibarıyla, müşteri sırrı niteliğindeki bilgilerin yalnızca yetkili mercilere yasal yükümlülük kapsamında açıklanabileceği, bu sürecin hukuka uygun olarak yürütülmesi gerektiği anlaşılmaktadır[129]. Bu durum bankaların finansal sistemin şeffaflığını ve güvenliğini temin etmek adına riskli işlemleri bildirirken bile, müşterilerin özel yaşamına saygı yükümlülüğü doğrultusunda gizliliği korumakla mükellef olduğunu gösterir.

Son olarak, müşteri sırrının ihlali yalnızca sırrı dış dünyaya açıklama ile değil, iç sistemlerdeki ihmalle de meydana gelebilir. Bu ihtimaller, bankaların iç denetim mekanizmalarını da sorumluluk altına sokar ve banka personelinin yetkisiz erişimi, kontrolsüz veri akışı, güvenlik önlemlerinin yetersizliği gibi teknik zafiyetler karşısında bankanın kendi çalışanına karşı iç disiplin mekanizmalarını işletmesini zorunlu hâle getirir. Nitekim Yargıtay'ın 22/06/2006 tarihli kararında, banka internet şubesinde kullanılan şifrelerin casus yazılımlar yoluyla ele geçirilerek müşterinin haberi olmadan yapılan işlemler nedeniyle gerekli ek güvenlik tedbirlerini almayan banka kusurlu ve sorumlu bulunmuş, hafif kusurdan bile bankanın sorumlu olduğu belirtilmiştir[130].

IX. ULUSLARARASI DÜZENLEMELERDE MÜŞTERİ SIRRININ KORUNMASI

Finansal sistemin dijitalleşmesi ve sınır ötesi veri akışlarının olağan hâle gelmesiyle birlikte müşteri sırrının korunması ulusal hukukun konusu olmaktan öte bir anlam kazanıp uluslararası normlar ve iş birliği mekanizmaları tarafından düzenlenen bir alana dönüşmüştür[131]. Bu gelişmeler ışığında birçok ülke, müşteri verilerinin korunmasına yönelik açık yasal düzenlemeler oluşturmuş, aynı zamanda çok taraflı anlaşmalar ve platformlar aracılığıyla ortak güvenlik standartları geliştirmiştir. Örneğin, GDPR, BCBS, FATF ve OECD gibi uluslararası kuruluşlar, müşteri bilgilerinin korunmasına yönelik detaylı düzenlemeler ve ilkelerle müşteri bilgilerinin korunmasını güvence altına almıştır.

AB'nin GDPR düzenlemesi, Basel Komitesi'nin Müşterini Tanı İlkeleri (Know Your Customer– KYC), FATF'ın 40 Tavsiyesi ve OECD'nin rehber ilkeleri, müşteri bilgilerinin

[129] Hazine ve Maliye Bakanlığı Malî Suçları Araştırma Kurulu (MASAK), "Şüpheli İşlem Bildirim Rehberi", 2024, s. 7. https://ms.hmb.gov.tr/uploads/sites/12/2024/05/MSK-RHB-SIB-001-2.pdf (E.T.: 01.08.2025)
[130] Bkz. Yargıtay 11. HD 22/06/2006 Tarih ve E.2005/4748, K.2006/7341 sayılı karar. (www.yargitay.gov.tr E.T.: 01.08.2025)
[131] Gurbet Arife Yıldırım, s. 143.

korunmasına yönelik uluslararası standartların oluşturulmasında büyük rol oynamaktadır. Türkiye'de ise KVKK, Hazine ve Maliye Bakanlığı'nın düzenlemeleri ve TBB'nin rehberleri doğrultusunda müşteri bilgileri korunarak uluslararası standartlara uyum sağlanmaktadır.

Avrupa Birliği'nin 2016 yılında kabul ettiği ve 2018'de yürürlüğe giren GDPR, kişisel verilerin korunmasına yönelik en kapsamlı ve en sert düzenlemedir. GDPR, bireylerin kişisel verilerinin işlenmesi ve korunmasına yönelik sıkı düzenlemelerle veri sorumlularına ve işleyenlere ciddi yükümlülükler öngörmüştür[132]. GDPR kapsamında bankalar, müşteri verilerini sadece açık rızayla işleyebilmekte ve bu verilerin korunması için uygun teknik ve idarî önlemleri almak zorundadır. Bu düzenlemeyle beraber müşterilere kendi kişisel verileri üzerinde geniş bir kontrol yetkisi tanınmakta ve unutulma hakkı gibi müşteri lehine haklar getirilmektedir. Bankaların, müşteri verilerini üçüncü kişilerle paylaşırken belirlenmiş olan hukukî çerçevelere uyması ve düzenleyici kurumlara hesap verebilir durumda olması gerekmektedir.

GDPR m. 83 kapsamında, sır ihlalinde uygulanacak yaptırımlar oldukça ağırdır. Şirketler, 20 milyon Euroya kadar veya yıllık küresel cirolarının %4'üne kadar para cezası ile karşı karşıya kalabilmektedir[133]. Bu yaptırımlar şirketler açısından ağır sonuçlara sebep olabilmektedir. Örneğin, Almanya'da H&M adlı firmaya 2020 yılında, çalışanlarının davranışsal ve özel hayat verilerini hukuka aykırı biçimde kaydettiği ve kullandığı gerekçesiyle 35,3 milyon Euro ceza kesilmiştir[134]. Bir diğer örnek olarak, Fransa'da Google'a 2019 yılında, kullanıcıların kişisel verilerinin işlenmesine ilişkin şeffaflık sağlanmaması, bilgilendirme yükümlülüğünün yerine getirilmemesi ve kişisel verilerin işlenmesine yönelik geçerli bir açık rızanın alınmaması nedeniyle 50 milyon Euro para cezası uygulanmıştır[135].

---

[132] Berna Akçalı Gür, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 2019, s. 860.

[133] GDPR, m. 83.

[134] EDPB, "Hamburg Veri Koruma Komiseri, H&M'e 35,3 Milyon Avro Para Cezası Verdi (Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations)", 2020. https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en (E.T.: 01.08.2025)

[135] EDPB, "CNIL Kısıtlı Komitesi, Google LLC'ye 50 Milyon Avro Para Cezası Uyguladı (CNIL's Restricted Committee Imposes Financial Penalty of 50 Million Euros Against Google LLC)", 2019. https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (E.T.: 01.08.2025)

GDPR kapsamında bireylerin veri işleme faaliyetlerine itiraz hakkı ve işlenmiş verilerini sildirme hakkı da güvence altındadır. Avrupa Veri Koruma Kurulu (EDPB)'nin 2022 tarihli "*Right of Access*" rehberine göre, bireyler yalnızca veri toplandığını bilmekle kalmamalı, aynı zamanda bu verilerin nasıl işlendiğini ve kimlerle paylaşıldığını da öğrenebilmelidir[136]. Türkiye'de ise Risk Merkezi üzerinden işlenen verilerin paylaşım zinciri müşteriler tarafından doğrudan görülememektedir. Bireyler, e-Devlet üzerinden Risk Raporu gibi belgelere erişebilse de verilerinin nasıl işlendiğine veya kimlerle paylaşıldığına dair bilgiye ulaşma ve doğrudan Risk Merkezi ile etkileşime geçme olanaklarına sahip değillerdir. Bireylerin kendi verilerinin kimlerle ve nasıl paylaşıldığını doğrudan takip edememesi, veri sahipliği ve şeffaflık ilkelerinin zedelenmesine yol açmaktadır. Bu durum, modern veri koruma anlayışının temelini oluşturan veri öznesinin aktif rolü ilkesine aykırılık teşkil etmektedir.

Uluslararası düzlemde, AB'nin GDPR sistematiği bireyin aktif veri öznesi olmasını esas alırken, uygulamada Almanya'daki SCHUFA gibi kuruluşlar verileri bireyin rızaya veya meşru menfaat gerekçesine dayalı olarak işler. Meşru menfaate dayalı veri işleme, veri sorumlusunun ya da üçüncü bir tarafın ekonomik, ticarî veya güvenlik gibi çıkarlarının, bireyin temel hak ve özgürlüklerine ağır basmadığı durumlarda kişisel verilerin açık rıza olmaksızın işlenmesine olanak tanır. Bu meşru menfaat gerekçesi, veri işleme açısından güçlü bir dayanak olmakla beraber, bireyin mahremiyet haklarını zedeleyecek riskler taşıdığı için Avrupa'da ve özellikle Almanya'da tartışmalı bir alan olarak öne çıkar.

Nitekim Avrupa Birliği Adalet Divanı C-634/21 SCHUFA kararında, kredi skoru üretiminin meşru menfaate dayanarak yapılmasının GDPR'nin 22. maddesi anlamında otomatik karar verme yasağına takılıp takılmayacağını eleştirmiş ve bu bağlamda veri işleme faaliyetlerinin sınırlarının ne şekilde çizilmesi gerektiğini ele almıştır[137]. Kararda, SCHUFA'nın kredi skorlama faaliyetlerinin bireyin hukukî durumunu ya da ekonomik koşullarını ciddi bir şekilde etkileyebileceğini, bu nedenle sadece meşru menfaat gerekçesine dayanılarak yapılan otomatik işlemelerin GDPR kapsamındaki özel koruma hükümlerine tâbi olması gerektiği vurgulanmıştır. Mahkeme, her somut olayda meşru menfaat ile bireyin

[136] EDPB, "Erişim Hakkına İlişkin Rehber 01/2022 (Guidelines 01/2022 on Right of Access)", 2022, s. 10. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (E.T.: 01.08.2025)

[137] Avrupa Birliği Adalet Divanı (Court of Justice of the European Union– CJEU), "Veri Koruma Hukuku Bağlamında Karar (Judgment on Data Protection Law)", 2023, C-319/22, m. 22. https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=EN (E.T.: 01.08.2025)

temel hak ve özgürlükleri arasında dengenin kurulmasının zorunlu olduğuna işaret etmiş, meşru menfaat gerekçesinin sınırlarının genişletilerek birey haklarının zedelenmesine yol açmaması gerektiğini belirtmiştir.

Amerikan hukuk sistemi ise müşteri sırrına ilişkin korumayı daha çok faaliyet alanına özgü yasalar yoluyla sağlamaktadır. Örneğin, 1978 tarihli RFPA, bankacılık faaliyetleri sırasında elde edilen finansal bilgilerin federal kurumlarca izinsiz erişimini sınırlandırmış ve müşteriye bilgi edinme ve itiraz hakkı tanımıştır[138]. Ancak ulusal güvenlik, terörün finansmanı ve malî denetim gibi alanlarda USA PATRIOT Act kapsamında bu korumaya istisna getirilerek bankanın belirli durumlarda müşteriyi bilgilendirmeksizin veri paylaşabilmesine olanak tanınmıştır[139]. Bu durum, ABD sisteminde müşteri sırrının, gözetim odaklı güvenlik anlayışı ile çatışmalı bir şekilde korunduğunun bir göstergesidir.

Öte yandan, Equifax, TransUnion ve Experian gibi kredi büroları belirli koşullarda bireyin rızası olmaksızın veri işleyebilmektedir ancak Fair Credit Reporting Act (FCRA) kapsamında bireyler, kredi raporlarına yılda en az bir kere erişme, kredi raporuna dayanılarak verilen olumsuz kararlar hakkında bilgilendirme, hatalı bilgilerin düzeltilmesi veya silinmesini talep etme gibi haklara sahiplerdir[140]. Bu çerçevede ABD'de müşteri sırrının hem ticarî veri işleme serbestliği hem de yasal koruma mekanizmaları arasında bir denge gözetilerek korunduğunu söylemek mümkündür.

Türkiye'de ise Risk Merkezi bu derece kapsamlı bir kullanıcı denetimi mekanizması sunmamakta, veri sahibinin raporlarına erişimi teknik olarak mümkün olsa da itiraz ve düzeltme süreçleri oldukça sınırlı biçimde işletilmektedir. Bireyler, yalnızca ilgili bankaya başvurarak bilgi edinebilmektedir ve kendi verisinin nasıl işlendiğini, kimlerle ve ne amaçla paylaşıldığını izleyememektedir. Bu durum, GDPR'nin açık rıza, unutulma hakkı ve otomatik karar alma karşısında bireyi koruma ilkeleriyle örtüşmemekte ve Türkiye'deki veri koruma sisteminin kullanıcı merkezli olmadığını ortaya koymaktadır.

---

[138] Schulz Fritz, s. 128.

[139] USA PATRIOT Act, Yaşamı ve Özgürlüğü Korumak (Amerika'yı Terörizmi Önlemek İçin Gerekli Araçlarla Birleştirme ve Güçlendirme Yasası) (PATRIOT Act– Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), 2001. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (E.T.: 01.08.2025)

[140] Amerika Birleşik Devletleri Federal Ticaret Komisyonu (Federal Trade Commission– FTC), Adil Kredi Raporlama Yasası (Fair Credit Reporting Act– FCRA), 2023, s. 47. https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf (E.T.: 01.08.2025)

Bu bağlamda, yalnızca GDPR gibi yasal düzenlemeler değil, aynı zamanda sektörel standartlar da veri korunması konusunda etkilidir. Özellikle, Bankacılık Denetiminde Basel Komitesi (Basel Committee on Banking Supervision– BCBS), finans sektöründe risk yönetimi ve iç denetim standartlarına ilişkin ve bankaların müşteri bilgilerini nasıl işlemesi ve saklaması gerektiğine dair çeşitli standartlar belirlemiştir. Basel II ve Basel III çerçevesinde, bankaların müşteri verilerini güvenli bir şekilde saklaması ve bu bilgileri sadece finansal istikrar ve risk yönetimi açısından gerekli olduğunda paylaşılması önerilmektedir[141]. Her ne kadar Basel düzenlemeleri hukuken bağlayıcı nitelik taşımasa da, üye ülkeler kendi iç hukuklarına uyarlamak suretiyle bu düzenlemelere fiilen bağlayıcılık kazandırmakta ve uluslararası bankacılık uygulamaları için örnek teşkil etmektedir.

Basel düzenlemeleri ve uluslararası finansal gözetim standartları çerçevesinde geliştirilen KYC ilkeleri bankaların müşteri kimliklerini doğrulamalarını, şüpheli işlemleri izlemelerini ve gerekli durumlarda yetkili mercilere bildirimde bulunmalarını zorunlu kılmaktadır. KYC politikaları, özellikle kara para aklama ve terörizmin finansmanıyla mücadelede hem ulusal hem de uluslararası alanda önemli bir araç olarak görülmektedir. Dolayısıyla, bankalar için KYC prosedürlerinin uygulanması hem itibarlarını korumaları hem de yasal riskleri azaltmaları açısından stratejik önem taşımaktadır[142].

Diğer bir uluslararası düzenleyici çerçeve FATF tarafından oluşturulmuştur. FATF, kara para aklama ve terörizmin finansmanı gibi ekonomik suçlarla mücadele amacıyla uluslararası standartlar geliştiren bir kuruluştur. FATF'ın 40 Tavsiyesi, ülkelerin finansal suçlarla mücadelede alması gereken önlemleri kapsamaktadır. Bu tavsiyeler finansal kuruluşların müşteri durum tespiti yapmalarını, şüpheli işlemleri bildirmelerini zorunlu kılmaktadır. Ayrıca, veri gizliliğine saygı gösterilmesini ve müşteri bilgilerinin yasal çerçevede korunmasını teşvik etmektedir. Özellikle, FATF'ın 10 numaralı tavsiyesi, müşteri durum tespitinin açıkça tanımlanmasını ve titiz bir şekilde uygulanmasını öngörmektedir[143].

---

[141] BCBS, *Etkili Risk Verisi Toplama ve Risk Raporlaması İlkeleri (Principles for Effective Risk Data Aggregation and Risk Reporting*, BIS, 2013, m. 1 ve 6. https://www.bis.org/publ/bcbs239.pdf (E.T.: 01.08.2025)

[142] FATF, "Kara Paranın Aklanması ve Terörizmin ve Kitle İmha Silahlarının Finansmanıyla Mücadeleye İlişkin Uluslararası Standartlar– FATF Tavsiyeleri (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation– The FATF Recommendations)", 2023, s. 14. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (E.T.: 01.08.2025)

[143] FATF, "Kara Paranın Aklanması ve Terörizmin ve Kitle İmha Silahlarının Finansmanıyla Mücadeleye İlişkin Uluslararası Standartlar– FATF Tavsiyeleri", s. 14.

Bu düzenlemelere paralel olarak, veri koruma alanında daha erken bir dönemde uluslararası çerçeve oluşturan kuruluşlardan biri de merkezi Paris'te bulunan OECD'dir. OECD, kişisel verilerin korunmasına ilişkin uluslararası çerçeve oluşturmak amacıyla ilk olarak 1980 yılında "*Özel Hayatın Gizliliği ve Sınır Ötesi Kişisel Veri Akışı Rehber İlkeleri*"ni yayımlamıştır. Bu ilkeler, veri kalitesi, amaç belirtme, kullanım sınırlaması, güvenlik önlemleri ve bireylerin erişim hakları gibi önemli unsurları içermekte olup hukuken bağlayıcı olmamakla beraber üye ülkelerin ulusal mevzuatlarına rehberlik etmekte ve uluslararası veri transferlerinde uyumun sağlanmasını amaçlamaktadır. Bu bağlamda, OECD'nin veri koruma ilkeleri müşteri bilgilerinin korunmasına yönelik uluslararası bir temel oluşturmaktadır[144].

İsviçre'de ise müşteri sırrının korunması, 1934 tarihli Federal Bankacılık Yasası'nın 47. maddesiyle sistemleştirilmiştir. Bu hüküm, banka personelinin müşteriye ait bilgileri üçüncü kişilerle paylaşmasını suç olarak düzenlemiş ve sır saklama yükümlülüğünü ceza hukuku temeline dayandırmıştır[145]. Ek olarak, müşteri sırrının korunması yalnızca ceza hukuku değil, aynı zamanda özel hukuk ve idarî denetim hukuku boyutlarıyla da ele alınmıştır. Nitekim İsviçre doktrininde banka sırrının aslında bankaya değil, müşteriye ait olduğu ve bunun anayasal kişilik hakkı kapsamında değerlendirilmesi gerektiği belirtilmektedir. Bu katı gizlilik rejimi uzun yıllar boyunca İsviçre'yi küresel finans sisteminde gizliliğin merkezi hâline getirmiştir[146].

Ancak son yıllarda özellikle OECD'nin ortak raporlama standartları (CRS), FATF'nin şeffaflık ilkeleri ve uluslararası vergi iş birliği baskıları sebebiyle İsviçre, mutlak gizlilik ilkesini kademeli olarak terk ederek geleneksel gizlilik anlayışında değişikliğe gitmiş ve 2018'den itibaren bazı ülkelerle bilgi paylaşımına başlamıştır[147]. Buna rağmen banka gizliliği İsviçre'de hâlen anayasal düzeyde kişilik hakkı olarak korunmakta, ancak kamu yararının üstünlüğü ilkesi çerçevesinde sınırlandırılabilmektedir[148]. Bu gelişme, millî mevzuatla uluslararası düzenlemeler arasında denge kurulmasını zorunlu hâle getirmiştir.

---

[144] OECD, "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımı Hakkında Rehber İlkeler", s. 10.
[145] Pınar Çağla Kandıralıoğlu, s. 55.
[146] Kunz, Peter V., *İsviçre'de Banka (Müşteri) Sırrı,* çeviren: Erhan Seyfi Moroğlu, Banka ve Tüketici Hukuku Sorunları Sempozyumu, On İki Levha Yayıncılık, 2010, s. 139.
[147] OECD, "Finansal Hesap Bilgilerinin Otomatik Değişimi Standardının Uygulanması (Implementation of the Standard for Automatic Exchange of Financial Account Information)", 2019, s. 22. https://www.cbr.ru/Content/Document/File/84568/OECD_AEOI-Implementation-Report-2018.pdf (E.T.: 01.08.2025)
[148] İlknur Kaya, s. 204.

Türkiye de bu sisteme 2017 yılı itibarıyla resmi olarak taraf olmuş, fiili olarak 2021 yılından itibaren belirli ülkelerle otomatik bilgi paylaşımına başlamıştır[149].

[149] OECD, *Finansal Hesap Bilgilerinin Otomatik Değişimine İlişkin Akran Değerlendirme Rapor*u *(Peer Review of the Automatic Exchange of Financial Account Information)*, 2020, s. 10. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/peer-review-of-the-automatic-exchange-of-financial-account-information-2020_845ac93f/175eeff4-en.pdf (E.T.: 01.08.2025)

2. BÖLÜM

RİSK MERKEZİNİN İŞLEYİŞİ VE UYGULAMADA KARŞILAŞILAN SORUNLAR

I. BANKACILIKTA KARŞILAŞILAN RİSK TÜRLERİ

1. Faiz Oranı Riski

Faiz oranı riski, bankaların kredi ve mevduat gibi işlemlerinin faiz oranlarının farklı zamanlarda yeniden belirlenmesi veya faiz oranlarında ani değişiklik olması sebebiyle zarar görme olasılığıdır. Finansal sistemin temel yapı taşlarından biri olan faiz oranı, kredi verme ve kredi alma süreçlerini direkt olarak etkilemektedir. Örneğin, sabit faizle verilen uzun vadeli bir kredinin karşılığında toplanan mevduatların kısa vadeli ve değişken faizli olması durumunda faiz oranlarında meydana gelen artışlar, bankanın faiz giderini yükseltirken gelirini sabit tutmaktadır. Bu da net faiz marjını daraltmaktadır[150].

Türkiye'de sık değişen para politikaları sebebiyle faiz oranı riski daha da belirgin bir hâle gelmektedir. Örneğin, 2021–2023 yıllarında Türkiye Cumhuriyeti Merkez Bankası'nın politika faizindeki dalgalanmalar sebebiyle bankaların fonlama maliyetleri doğrudan etkilenmiş ve net faiz gelirlerinde hareketliliğe yol açmıştır[151]. Bu sebeple Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından, faiz oranı riskinin yönetimine ilişkin birtakım düzenlemeler getirilmiştir. "*Faiz Oranı Riski Yönetimi Rehberi*" ve "*Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik*" uyarınca bankaların yeniden fiyatlama, vade uyum, senaryo analizleri ve stres testleri gibi yöntemleri kullanarak riskleri izlemeleri ve raporlamaları beklenmektedir[152].

---

[150] Mehmet Ali Candoğan, "Ticarî Bankalarda İtibar Riski Yönetimi ve İtibar Riski Hesaplama Model Önerisi: Borsa İstanbul Bankacılık Endeksinde Ampirik Bir Uygulama", Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2023, s. 14.

[151] TCMB, *2022 Yılı Para ve Kur Politikası*, 2021. https://www.tcmb.gov.tr/wps/wcm/connect/e9d73d1f-1523-46ea-a307-bb74fe366389/2022+Para+ve+Kur+Politikas%C4%B1.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-e9d73d1f-1523-46ea-a307-bb74fe366389-nU4.h6f (E.T.: 01.08.2025)

[152] BDDK, Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, m. 41, 2014. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19864&MevzuatTur=7&MevzuatTertip=5; BDDK, "Faiz Oranı Riski Yönetimi Rehberi", 2016, s. 9. https://www.bddk.org.tr/Mevzuat/DokumanGetir/957 (E.T.: 01.08.2025)

Uluslararası düzeyde faiz oranı riskinin yönetimi konusundaki en kapsamlı düzenlemeler BCBS tarafından geliştirilen Basel III çerçevesinde tanımlanmaktadır. "*Interest Rate Risk in the Banking Book (IRRBB)"* başlıklı dokümanda, bankaların faiz oranı riskinin yalnızca ticarî portföylerinde değil, bankacılık hesaplarında da göz önünde bulundurulması ve sermaye yeterliliği değerlendirmelerinde bu riskin etkilerinin dikkate alınması gerektiği vurgulanmaktadır[153].

Modern risk yönetimi çerçevesinde bankalar gap analizi, duration analizi ve senaryo analizleri gibi yöntemlere ek olarak *"Net Faiz Geliri (Net Interest Income– NII)*" ve "*Ekonomik Özsermaye Değeri (Economic Value of Equity– EVE)"* gibi ölçütlerle de farklı faiz senaryolarının bankanın gelirine ve sermayesine etkileri incelenmektedir[154]. Risk Merkezi tarafından yayımlanan veriler ise dolaylı olarak bu riskin izlenmesine katkı sağlamaktadır. Kredi türleri, vadeleri ve faiz yapılarının aylık olarak paylaşılması, sistemin genelinde faiz duyarlılığı analizinin yapılmasını kolaylaştırmakta ve politika geliştirme sürecinde erken uyarı işlevi görerek destek olmaktadır.

2. Piyasa Riski

Piyasa riski, finansal piyasalardaki dalgalanmalardan kaynaklı olarak bankaların karşılaşma ihtimali olan zararları ifade eder. Bu risk faiz oranlarından, döviz kurlarından, hisse senedi fiyatlarındaki ani değişikliklerden ve emtia fiyatlarındaki dalgalanmalardan kaynaklanabilmektedir[155]. Özellikle menkul kıymetler ve türevleri gibi piyasa değeri hareketli olan varlıklara yoğun bir şekilde yatırım yapan bankalar açısından piyasa riski önem taşımaktadır[156].

Piyasa riski genellikle dört ana başlık altında incelenir: faiz oranı riski, kur riski, hisse senedi fiyatı riski ve emtia riski[157]. Bu sınırlandırma ticarî portföy kapsamındaki varlık ve işlemler için geçerlidir. Örneğin, döviz kurundaki artış, döviz açık pozisyonu bulunan bir bankada ciddi malî kayıplara sebep olabilirken, borsa endekslerindeki düşüşler sermaye piyasası faaliyetlerini yürüten bankalar açısından risk yaratmakta, hisse senedi fiyatlarındaki

[153] BCBS, "Bankacılık Portföyünde Faiz Oranı Riski (IRRBB) (Interest Rate Risk in the Banking Book (IRRBB))", BIS, 2016, s. 4. https://www.bis.org/bcbs/publ/d368.pdf (E.T.: 01.08.2025)
[154] BCBS, "Bankacılık Portföyünde Faiz Oranı Riski", s. 1 ve s. 8.
[155] BCBS, "Piyasa Riski İçin Asgari Sermaye Gereklilikleri (Minimum Capital Requirements for Market Risk)", BIS, 2016, s. 7. https://www.bis.org/bcbs/publ/d352.pdf (E.T.: 01.08.2025)
[156] BCBS, "Piyasa Riski İçin Asgari Sermaye Gereklilikleri", s. 1.
[157] BCBS, "Piyasa Riski İçin Asgari Sermaye Gereklilikleri", s. 65.

gerilemeler ise benzer olarak zararları artırabilmektedir. Emtia riski ise özellikle emtiaya dayalı sözleşmeler ya da doğrudan emtia yatırımı yapılması durumlarında söz konusu olmaktadır.

Faiz oranı riski de yalnızca ticarî portföyde yer alan faiz getirili finansal varlıklar bakımından piyasa riski kapsamında değerlendirilmekte, buna karşın bankaların alım satım amacı gütmeden uzun vadeli olarak bilançolarında tuttukları kredi, mevduat ve benzeri kalemleri içeren bankacılık kitabında (IRRBB) ortaya çıkan faiz oranı riski olarak ayrı bir şekilde ele alınmakta ve Basel düzenlemelerinde Pillar 2 başlığında anlatılmaktadır[158].

Türkiye'de piyasa riski, özellikle makroekonomik dalgalanmanın yüksek olduğu dönemlerde daha da önemli hâle gelmektedir. Örneğin, 2022-2023 yıllarında yaşanan faiz ve döviz kuru hareketliliği birçok bankanın kâr marjlarında ve döviz pozisyonlarında dalgalanmalara neden olmuştur. Bu durum, bankaların hem risk yönetim süreçlerini gözden geçirmelerini hem de sermaye yeterliliklerini yeniden değerlendirmelerini zorunlu kılmıştır[159].

BDDK, "*Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik*" kapsamında, standart yöntem veya içsel modeller aracılığıyla piyasa riskinin hesaplanması ve yönetilmesine ilişkin düzenleyici yükümlülükler getirmiştir. Bu çerçevede bankalar faiz oranlarını, döviz kurlarını ve hisse senedi pozisyonlarını ayrı ayrı ve günlük olarak izleyip raporlamak zorundadır[160].

Piyasa riskinin ölçümünde "*Riske Maruz Değer (Value at Risk– VaR)*" yöntemi en yaygın kullanılan tekniklerdendir. VaR belirli bir güven düzeyi ve belirli bir zaman aralığında oluşabilecek en yüksek zararı tahmin etmeye yarayan istatistiksel bir yöntemdir. Ayrıca stres testleri ve senaryo analizleri gibi ileri düzey teknikler de bankaların olası kriz senaryolarına hazırlıklı olmalarını sağlar[161]. Risk Merkezi'nin topladığı ve sınıflandırdığı aylık veriler de kredi portföyü yapısı, vade dağılımları ve döviz bazlı yükümlülükler gibi öğeler üzerinden piyasa riski analizlerinde dolaylı olarak kullanılabilir. Bu tür veriler, makro

[158] BCBS, "Bankacılık Portföyünde Faiz Oranı Riski", s. 1.
[159] TCMB, *Finansal İstikrar Raporu, Sayı 38,* 2024, s. 37. https://www.tcmb.gov.tr/wps/wcm/connect/tr/tcmb+tr/main+menu/yayinlar/raporlar/finansal+istikrar+raporu/2024/sayi+38 (E.T.: 01.08.2025)
[160] BDDK,Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik, 2022. https://www.bddk.org.tr/Mevzuat/DokumanGetir/1290 (E.T.: 01.08.2025)
[161] John C. Hull, *Risk Yönetimi ve Finansal Kurumlar* (*Risk Management and Financial Institutions)*, Wiley, 3. Baskı, 2012, s. 479.

ihtiyati politika geliştirme süreçlerinde erken uyarı sistemlerinin temel girdisi olabilmektedir.

Uluslararası düzeyde ise BCBS, 2019 yılında yayımladığı "*Minimum Capital Requirements for Market Risk*" belgesi ile, uluslararası alanda piyasa riski hesaplamasında daha duyarlı ve risk odaklı bir yaklaşım benimsemiştir. Yeni düzenlemeler ile, özellikle bankaların maruz kaldığı pozisyonların likidite yapıları ve kriz dönemlerinde yaşanan değer kayıpları daha gerçekçi bir şekilde analiz edilmeye başlanmıştır. Böylece yalnızca düzenleyici uyum değil, aynı zamanda stratejik ve sürdürülebilir risk yönetimi perspektifi benimsenmiştir[162].

3. Likidite Riski

Likidite riski, bir finansal kuruluşun kısa vadeli yükümlülüklerini karşılamak için yeterli nakit ya da kolayca nakde çevrilebilir varlıklara zamanında erişememesi durumunda karşı karşıya kaldığı riski ifade etmektedir[163]. Finansal piyasalarda güven eksikliğinin söz konusu olduğu dönemlerde likidite riski daha belirgin hâle gelmektedir. Bu risk, ödeme kabiliyetlerini kaybetmemesi, finansal kurumların faaliyetlerini sürdürebilmesi ve yükümlülüklerini yerine getirebilmesi açısından önem taşımaktadır. Likidite daralmalarının domino etkisiyle diğer kurumlara da yayılma ihtimalinin olması sebebiyle Risk Merkezi, likidite eğilimlerini zamanında izleyerek özellikle kısa vadeli kredi hareketleri, gecikmeli tahsilat oranları ve nakit dönüş hızları bakımından adeta erken uyarı mekanizması görevi görmektedir[164].

Likidite riski iki ana başlık altında incelenmektedir: finansman likiditesi riski ve piyasa likiditesi riski. Finansman likiditesi riski, bankanın kısa vadeli yükümlülüklerini yerine getirecek fonları zamanında bulamaması; piyasa likiditesi riski ise, bankanın varlıklarını makul bir fiyat ve makul hızla elden çıkaramaması durumudur[165]. Piyasa likiditesi riskine örnek olarak, bir kriz anında devlet tahvillerinin bile istenen fiyattan satılamaması durumu örnek gösterilebilir. Bu durum güven kaybına yol açmaktadır[166]. Finansman likiditesine örnek olarak, 2018 ve 2020 yıllarında yaşanan döviz kuru krizleri sırasında bazı bankaların

[162] BCBS, "Piyasa Riski İçin Asgari Sermaye Gereklilikleri", s. 1.
[163] John C. Hull, s. 537.
[164] Joël Bessis, *Bankacılıkta Risk Yönetimi* (*Risk Management in Banking)* , Wiley, 3. Baskı, 2010, s. 8.
[165] Joël Bessis, s. 3
[166] Viral Acharya, Douglas Gale ve Tanju Yorulmazer, "Yenileme Riski ve Piyasa Donmaları (Rollover Risk and Market Freezes)", *The Journal of Finance,* Cilt 66, Sayı 4, 2011, s. 5.

kısa vadeli yükümlülüklerini yerine getirmekte zorlanmasıyla beraber Merkez Bankası'nın acil likidite destek mekanizmalarını devreye sokması verilebilir[167]. Bu durum, likidite riskinin yalnızca bireysel banka düzeyinde kalmayıp aynı zamanda sistemik etkiler yaratabileceğini ortaya koymaktadır.

2008 Küresel Finansal Krizi'nin ardından, bankacılık sektöründe likidite riskinin sistemik krizlere yol açabilecek boyutlara ulaşabileceği anlaşılmış ve bu riski sınırlamaya yönelik yapısal düzenlemeler geliştirilmiştir. Bu kapsamda Basel III düzenlemeleri çerçevesinde getirilen iki temel likidite oranı olan Likidite Karşılama Oranı (Liquidity Coverage Ratio– LCR) ve Net İstikrarlı Fonlama Oranı (Net Stable Funding Ratio– NSFR), bankaların kısa ve uzun vadeli likidite risklerini ölçmek ve yönetmek için kullanılmaktadır[168]. LCR, bir bankanın 30 gün içerisinde yaşanabilecek bir likidite stresine karşı bankanın dayanıklılığını ölçerken; NSFR, bankanın uzun vadeli yükümlülüklerini karşılayabilecek fon kaynaklarına sahip olup olmadığını değerlendirir[169].

BDDK'nın 2015 yılında yürürlüğe koyduğu "*Likidite Karşılama Oranı Tebliği*" ile LCR iç hukuka dâhil edilmiştir ve bankaların belli stres senaryolarına dayanabilecek yüksek kaliteli likit varlıkları elinde bulundurmaları zorunlu hâle gelmiştir[170]. NSFR ise devam eden yıllarda Basel III uyum süreci çerçevesinde yapılan ikincil düzenlemelerle mevzuata aşamalı olarak eklenmiştir. Böylece her iki düzenleme ile LCR ve NSFR Türkiye'de bankacılık mevzuatına entegre edilerek bankalar için bağlayıcı hâle getirilmiştir.

4. Kur Riski

Döviz riski olarak da adlandırılabilen kur riski, bankaların yabancı para cinsinden aktif ve pasiflerinin döviz kurlarındaki hareketlilikten etkilenmesi sebebiyle ortaya çıkan finansal olumsuzlukları ifade etmektedir. Kur riski, kur dalgalanmalarının yoğun olarak yaşandığı dönemlerde hem bankaların bilanço yönetimini hem de finansal sistemin istikrarını tehdit

---

[167] TCMB, *2018 Yılı Faaliyet Raporu*, s. 23. https://www3.tcmb.gov.tr/yillikrapor/2018/files/tr-full.pdf (E.T.: 01.08.2025)

[168] BCBS, "Basel III: Likidite Riski Ölçümü, Standartları ve İzlenmesine İlişkin Uluslararası Çerçeve (Basel III: International Framework for Liquidity Risk Measurement, Standards and Monitoring)", BIS, 2010, s. 3. https://www.bis.org/publ/bcbs188.pdf (E.T.: 01.08.2025)

[169] BCBS, "Basel III: Likidite Karşılama Oranı ve Likidite Riski İzleme Araçları (Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools)", BIS, 2013, s. 1. https://www.bis.org/publ/bcbs238.pdf (E.T.: 01.08.2025)

[170] BDDK, Likidite Karşılama Oranı Hakkında Tebliğ, Resmî Gazete, Sayı: 29294,, 21 Mart 2014. https://resmigazete.gov.tr/eskiler/2014/03/20140321-7.htm (E.T.: 01.08.2025)

edebilecek niteliğe sahip olmasından ötürü dikkatle yönetilmesi gereken risk türlerinden biridir. Özellikle, dışa açıklık oranı yüksek olan Türkiye gibi ülkelerde bu riskin boyutu daha belirgin olarak hissedilmektedir[171].

Kur riski üç alt başlıkta sınıflandırılabilir: işlem riski, çeviri riski ve ekonomik risk. İşlem riski, bankaların yabancı para cinsinden gerçekleştirdiği işlemlerin ödeme günü ile muhasebeleştirme günü arasında kurda meydana gelen değişiklik nedeniyle ortaya çıkan risktir. Çeviri riski, yabancı para cinsinden varlık ve yükümlülüklerin, raporlama para birimine çevrilmesi sürecinde oluşan söz konusu değer farklarını ifade eder. Ekonomik risk ise, döviz kuru değişimlerinin bankanın rekabet gücü ve uzun vadeli nakit akışları üzerindeki etkisini kapsamaktadır[172].

Türkiye'de 2018 ve 2021 yıllarında yaşanan kur şoklarının finansal piyasalarda büyük bir baskı yaratması sebebiyle, bu dönemde bankalar döviz pozisyonlarını yeniden yapılandırmak durumunda kalmıştır. TCMB'nin 2022 yıl sonu itibarıyla yaptığı değerlendirmelere göre, Türk bankacılık sektöründe yabancı para cinsinden kalemlerin bilanço içindeki payı yüksek seviyelerde seyretmektedir. Bu durum aktif ve pasif tarafında yabancı para dengesizliklerinin devam ettiğini ve sistem genelinde kur riskinin varlığını sürdürdüğünü ortaya çıkarmaktadır[173].

Kur riski yönetiminde bankalar genellikle hedge stratejilerine başvurmaktadır. Vadeli döviz işlemleri, opsiyonlar ve swap sözleşmeleri, bankaların açık döviz pozisyonlarını sınırlandırmasına yardımcı olmaktadır. Ayrıca, Risk Merkezi'nin döviz kredilerine ilişkin verileri, borçluların döviz bazlı kredi riskinin izlenmesinde önemli rol oynamaktadır[174].

Kur riskini sınırlayıp önlem almak amacıyla BDDK ise, uygulamalarında yaygın olarak net genel döviz pozisyonlarının özkaynaklara oranında %20 sınırını esas almaktadır. Ayrıca bankaların döviz yükümlülükleri için zorunlu karşılık oranları, TCMB tarafından belirlenen oranlarda döviz veya altın cinsinden tesis edilmekte ve raporlanmaktadır.

---

[171] Hüseyin Selimler, Süleyman Kale, "Türk Bankacılık Sektöründe Yabancı Para İşlemler", *Maliye ve Finans Yazıları*, 2012, s. 37.
[172] David K. Eiteman, Arthur I. Stonehill ve Michael H. Moffett, *Çok Uluslu İşletme Finansmanı* (*Multinational Business Finance)*, Pearson. 15. Baskı, 2021, s. 307.
[173] TCMB, *Finansal İstikrar Raporu*, Sayı 38.
[174] BDDK, Bankaların Özkaynaklarına İlişkin Yönetmelik, Resmî Gazete, Sayı 28756, 5 Eylül 2013,. https://www.lexpera.com.tr/resmi-gazete/metin/bankalarin-ozkaynaklarina-iliskin-yonetmelik-28756-1 (E.T.: 01.08.2025)

Uluslararası düzeyde ise BCBS tarafından, kur riskinin piyasa riski kapsamında sermaye yeterliliği hesaplamalarına dâhil edilmesi öngörülmüştür. MAR31.8'de, bankaların iç modellerinde önemli döviz pozisyonları için risk faktörleri kullanması zorunlu tutulmaktadır. Bu düzenleme, kur riskinin piyasa riski kapsamında sermaye hesaplamalarına entegre edilmesini sağlamaktadır[175].

5. Operasyonel Risk

Basel II düzenlemelerine göre operasyonel risk, yetersiz veya başarısız iç süreçlerden, çalışanlardan, sistemlerden ya da dışsal olaylardan kaynaklanan zarar riskidir. Operasyonel riskin kapsamı oldukça geniştir. Bu riskler arasında bilgi teknolojisi riskleri, siber güvenlik açıkları, çalışan suistimalleri, dolandırıcılık vakaları, yangın, sel gibi fiziki zararlar da yer almaktadır. Bu risk, finansal risklerin dışında kalması sebebiyle çoğunlukla içsel kontrol sistemleriyle önlenebilecek olsa da bazen öngörülemez olaylardan doğabilecek riskleri de kapsamaktadır[176].

2020 yılında COVID-19 pandemisiyle beraber uzaktan çalışma sistemlerinin yaygınlaşması sebebiyle bankacılık faaliyetlerinde dijital bağımlılık artmış ve operasyonel kontrollerin önemi artmıştır[177]. Türkiye'de operasyonel riskin yönetimine ilişkin çerçeve, BDDK tarafından oluşturulmuştur. "*Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik*" kapsamında bankaların operasyonel risklerini tanımlaması, ölçmesi, izlemesi, raporlaması ve gerekli kontrolleri sağlaması gerekmektedir[178]. Ayrıca 2022 yılında yürürlüğe giren "*Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Uygulama Tebliği*"nin 6. ve 7. maddeleri finansal kuruluşların siber risklere karşı organizasyonel yapılar kurmasını, bilgi

[175] BCBS, "MAR31– İçsel Model Yaklaşımı: Model Gereklilikleri (MAR31– Internal Models Approach: Model Requirements)", BIS, 2023, s. 2. https://www.bis.org/basel_framework/chapter/MAR/31.htm (E.T.: 01.08.2025)
[176] BIS, "Sermaye Ölçümünün ve Standartlarının Uluslararası Uyumlaştırılması: Gözden Geçirilmiş Çerçeve (International Convergence of Capital Measurement and Capital Standards: A Revised Framework)", 2004, s. 137. https://www.bis.org/publ/bcbs107.pdf (E.T.: 01.08.2025)
[177] Rodrigo Coelho ve Jermy Prenio, "Covid-19 ve Operasyonel Dayanıklılık: Pandemi Sürecinde Finansal Kurumların Operasyonel Zorluklarının Ele Alınması (Covid-19 and Operational Resilience: Addressing Financial Institutions Operational Challenges in a Pandemic)", FSI Briefs No. 2, BIS, 2020, s. 2. https://www.bis.org/fsi/fsibriefs2.pdf (E.T.: 01.08.2025)
[178] TBB, Risk Merkezi Yönetmeliği, 2014. https://www.tbb.org.tr/pdf/faaliyetler/71/784 (E.T.: 01.08.2025)

sistemlerinin sürekliliğini sağlamasını ve dijital risklere karşı operasyonel dayanıklılığını artırmasının gerektiğini belirtmektedir[179].

Operasyonel riskin ölçümünde bankalar, genellikle Basel düzenlemeleri kapsamında üç farklı yöntem kullanmaktaydı: temel gösterge yaklaşımı, standart yaklaşım ve gelişmiş ölçüm yaklaşımları. Bu üç yaklaşım, bankaların operasyonel kayıplardan kaynaklanabilecek potansiyel zararlarını ölçmesine ve bu risklere karşı yeterli sermaye tutmasını sağlamaya yönelik Basel düzenlemeleri kapsamında geliştirilmiştir. Ancak BCBS'nin uluslararası alanda faaliyet gösteren bankalar için hazırladığı en son standart olan Basel IV ile, bu üçlü yöntem sistemi yerine tüm bankalar için geçerli olacak tek bir Standartlaştırılmış Operasyonel Risk Yaklaşımı (Standardised Measurement Approach - SMA) getirilmiştir. Yeni yaklaşım ile, bankanın gelirlerinin yanında geçmiş operasyonel kayıplarını da dikkate alıp sermaye gereksinimini belirleyerek hem yöntem birliği sağlanmakta hem de bankalar arası karşılaştırılabilirlik artırılmaktadır. Böylece karmaşık hesaplamalar ve farklı uygulamalara neden olan sistemin yerine, tüm bankaların aynı şekilde hesaplama yaptığı, daha sade, şeffaf ve karşılaştırılabilir bir yapı kurulmuştur[180].

Operasyonel risk yönetimi yalnızca finansal kayıplarla sınırlı olmayıp aynı zamanda bankaların bilgi yönetimi ve veri doğruluğu süreçlerini de doğrudan etkilemektedir[181]. Risk Merkezi ile operasyonel risk arasında, veri işleme süreçleri üzerinden dolaylı bir etkileşim ortaya çıkmaktadır ve bu yönüyle Risk Merkezi, operasyonel risk yönetimi açısından önemli bir konumdadır. Örneğin, müşteri verilerinin korunmasına ilişkin KVKK ihlalleri ya da operasyonel yetersizliklerin bir sonucu olarak Risk Merkezi'ne gönderilen eksik veya hatalı veriler bankalara karşı hukukî yaptırımlar uygulanmasına sebep olabilmektedir. Nitekim Yargıtay 21/02/2024 tarihli bir kararında, kredi borcu bulunmamasına rağmen bankanın Risk Merkezi'ndeki olumsuz kaydı güncellememesi sebebiyle borçlunun itibarının zedelenmesi sebebiyle bankanın tazminat ödemeye mahkûm edildiğini belirtmiştir. Bu karar

[179] BDDK, Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Uygulama Tebliği, Resmî Gazete, Sayı 32044, 25.03.2022. https://www.mevzuat.gov.tr/mevzuat?mevzuatno=39442&mevzuattur=9&mevzuattertip=5 (E.T.: 01.08.2025)

[180] BCBS, "Operasyonel Risk için Standartlaştırılmış Yaklaşım– Giriş (The Standardised Approach for Operational Risk– Introduction)", BIS, 2017. https://www.bis.org/basel_framework/chapter/OPE/25.htm (E.T.: 01.08.2025)

[181] Murat Mazıbaş, "Operasyonel Riske Basel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme", 2005, BDDK Araştırma Raporu No: 2005/1, s. 5. https://www.bddk.org.tr/ContentBddk/dokuman/duyuru_basel_0001_44.pdf (E.T.: 01.08.2025)

bankaların Risk Merkezi'ne doğru ve güncel veri bildirme yükümlülüğünün operasyonel risk yönetimi açısından önemini ortaya koymaktadır[182].

Uluslararası düzeyde de operasyonel riskin özellikle siber saldırılarla iç içe geçmesi, bu alandaki düzenlemelerin güncellenmesini zorunlu kılmıştır. ECB'nin, 2022 yılında yayımladığı "*Siber Dayanıklılık Gözetim Beklentileri* (*Cyber Resilience Oversight Expectations)*" başlıklı belgede, operasyonel riski azaltmaya yönelik en iyi uygulamaları sıralanmış, bilgi güvenliğine dayalı sistemlerin bankacılık sisteminde önceliklendirilmesi gerektiğini belirtilmiştir[183].

6. Kredi Riski

Kredi riski, bir borçlunun finansal yükümlülüğünü zamanında ve eksiksiz olarak yerine getirememesi sebebiyle bir finansal kuruluşun zarara uğrama ihtimalidir. Kredi riski borçlunun temerrüdü, geri ödeme kabiliyeti zayıf müşterilerle çalışılması, ekonomik dalgalanmalara karşı hassasiyet ve teminatların yetersizliği gibi farklı faktörlerin birleşimiyle ortaya çıkmaktadır[184]. Bankacılık faaliyetlerinin temelini oluşturan bu risk, finansal sistemin istikrarı üzerinde doğrudan etkiye sahiptir. İlk bakışta kredi riskinin yalnızca bireysel kredilerle sınırlı olduğu düşünülse de ticarî krediler, tahsili gecikmiş borçlar ve diğer alacak kalemleri de bu kapsama dâhildir[185]. Türkiye'de bu risk türü özellikle ekonomik belirsizlik dönemlerinde artış göstermektedir. Örneğin, 2018 ve 2020 yıllarında yaşanan finansal hareketlilikle, bankaların takipteki alacak oranları belirgin şekilde yükselmiş ve kredi karşılıkları önemli ölçüde artmıştır.

Bankalar kredi riskini yönetmek amacıyla çeşitli stratejiler kullanmaktadır. Örneğin, müşteri kredi skorlama sistemleri, teminatlandırma politikaları, kredi limitleri, sektör ve müşteri bazlı portföy çeşitlendirmesi gibi yöntemler kullanarak riski yaymayı hedeflemektedirler[186]. Türkiye'de bu sistemlerin işleyişinde Risk Merkezi, birey ve

---

[182] Bkz. Yargıtay 3. HD 21/02/2024 Tarih ve E.2023/2804, K.2024/747 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

[183] ECB, "Bilgi ve İletişim Teknolojileri ile Güvenlik Risklerinin Yönetimine İlişkin Rehber (Guidelines on ICT and Security Risk Management)", 2020, s. 21. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf (E.T.: 01.08.2025)

[184] BCBS, "Kredi Riskinin Yönetimine İlişkin Prensipler *(*Principles for the Management of Credit Risk)",, 2000, s. 22. https://www.bis.org/publ/bcbs75.pdf (E.T.: 01.08.2025)

[185] John C. Hull, s. 431.

[186] BCBS, "Kredi Riskinin Yönetimine İlişkin Prensipler", s. 1.

şirketlerin geçmiş kredi performanslarına dair bankalar arası bilgi paylaşımını sağlayarak, borçluların tüm finansal yükümlülüklerine ilişkin görünürlük sağlayıp bilgi asimetrisini azaltmayı amaçlamaktadır. Ayrıca, Kredi Kayıt Bürosu ve Findeks gibi yapılar da kredi riskinin yönetiminde Risk Merkezi ile uyumlu olarak çalışarak kredi notu sistemleri üzerinden borçluların ödeme alışkanlıklarını takip edip kredi riskini öngörme noktasında yardımcı kurumlar olarak destek sağlamaktadırlar.

Uluslararası alanda kredi riskinin yönetimi, Basel II ve III düzenlemeleriyle çerçevelendirilmiştir. Basel II'ye göre bankalar, ya uluslararası derecelendirme kuruluşlarının notlarını esas alan "*Standart Yöntem*" ile ya da "*İçsel Derecelendirmeye Dayalı Yaklaşım (Internal Ratings-Based– IRB)"* ile borçluların temerrüt olasılıklarını ölçebilmektedir. Basel III ile birlikte ise, bankaların yalnızca kredi riskine karşı değil, tüm risklere karşı daha güçlü bir sermaye yapısı tesis etmeleri amaçlanmış. Türkiye'de ise BDDK bu düzenlemeleri, "*Bankaların Kredi İşlemlerine İlişkin Yönetmelik*" ve "*Sermaye Yeterliliği Yönetmeliği*" ile iç hukuka entegre etmiştir[187].

7. İklim Riski

İklim riski, finansal kurumların iklim değişikliğinin sebep olduğu çevresel ve politik etkilerinden kaynaklanan finansal zararlar veya fırsat kayıpları ile karşı karşıya kalma ihtimalidir[188]. Bu riskler, iklim değişikliğinin fiziksel etkilerinden veya iklim politikaları sebebiyle değişen piyasa tercihlerinin yarattığı dolaylı etkilerden kaynaklanabilmektedir. İklim riski genel olarak iki ana kategoriye ayrılır: fiziksel riskler ve dönüşüm riskleri[189].

Fiziksel riskler, şiddetli hava durumları, sel, kasırga, kuraklık gibi iklim değişikliğine bağlı meydana gelen zararlardır. Bu riskler, ekonomik varlıkların değer kaybına sebep olarak banka portföylerinde önemli zararlar oluşturabilmektedir. Örneğin, seller sebebiyle tarım sektöründeki bir müşterinin üretiminin azalması dolayısıyla kredinin geri dönüşünü riske sokabilmektedir[190].

---

[187] Şükrü Cicoğlu, Celal Gökhan Çil, "Türkiye'de Uygulanan Basel Kriterleri ve Basel III Kriterlerinin Türk Finans Sistemine Etkileri*", Politik Ekonomik Kuram*, 2019, Cilt 3, Sayı 1, s. 98.

[188] EBRD, "Finansal Aracı Kuruluşlar için İklim Riski Yönetimi *(*Climate Risk Management for Financial Intermediaries)", 2024, s. 1.

[189] ECB, "İklimle İlgili ve Çevresel Risklere İlişkin Rehber *(*Guide on Climate-Related and Environmental Risks)", 2020, s. 10. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf (E.T.: 01.08.2025)

[190] ECB, "İklimle İlgili ve Çevresel Risklere İlişkin Rehber", s. 10.

Dönüşüm riskleri ise, iklim politikaları, teknoloji değişiklikleri ve pazar tercihlerindeki dönüşümlerin yarattığı riskleri ifade etmektedir. Bu riskler, karbon vergilerinin yükselmesi veya temiz enerjiye geçiş maliyetleri gibi giderleri içerebilir. Örneğin, karbon fiyatlandırması politikaları nedeniyle kömür işletmelerinin kredi değerliliği olumsuz etkilenebilir[191].

Diğer tüm sektörleri de etkileyen iklim riskinin bankacılık sektöründe özel olarak ele alınmasının nedeni, bu sektörün ekonomi genelinde kaynak tahsisi, kredi verme ve finansman yaratma durumları ile doğrudan bağlantılı olmasıdır. Bankalar yüksek miktarda kredi portföyü ve yatırım pozisyonları ile iklim riskine dolaylı olarak maruz kalmaktadır. Kredi teminatlarının fiziksel tehditlere açık olması, müşterilerin geçiş sürecindeki malî baskılara olan dayanıklılıklarının azalması gibi durumlar finansal istikrarı ve dolayısıyla bankacılık sektörünü tehdit etmektedir. Ayrıca bankalar yalnızca iklim riskine maruz kalan taraf değildir. Bankalar iklim dostu yatırımlara finansal olarak destek sağlayarak projeleri teşvik edebilmekte ve bu yolla finansal istikrarın korunmasına katkı sağlamaktadırlar[192].

Uluslararası alanda, iklim riskinin finansal sistem üzerindeki etkileri giderek daha fazla önem kazanmıştır. Finansal düzenleyici kurumlar, iklim riskinin potansiyel risk taşıdığı görüşünde birleşerek bu risklerin ölçülmesi ve yönetilmesi için birtakım standartlar geliştirmektedir. Özellikle "*İklimle İlgili Finansal Beyanlar Görev Gücü* (*Task Force on Climate-related Financial Disclosures– TCFD)"* tarafından geliştirilen raporlama ve açıklama standartları, küresel finans piyasalarında iklim riskine dair şeffaflık ve karşılaştırılabilirlik sağlamak amacıyla yaygınlaşmaktadır. Kurumsal yönetim, strateji, risk yönetimi ile metrikler ve hedefler başlıklarından oluşan bu çerçeve aynı zamanda iklim risklerinin finansal etkilerinin ölçülmesi ve yönetilmesine yönelik katkılar sunmaktadır. Nitekim NGFS de bu standartların uluslararası düzeyde benimsenmesini desteklemektedir[193].

---

[191] BIS, "Yeşil Kuğu: İklim Değişikliği Çağında Merkez Bankacılığı ve Finansal İstikrar (The Green Swan: Central Banking and Financial Stability in the Age of Climate Change)", 2020, s. 18. https://www.bis.org/publ/othp31.pdf

[192] EBRD, "Finansal Aracı Kuruluşlar için İklim Riski Yönetimi", s. 1.

[193] NGFS, "Eylem Çağrısı: Finansal Risk Kaynağı Olarak İklim Değişikliği (A Call for Action: Climate Change as a Source of Financial Risk)", 2019, s. 32. https://www.ngfs.net/system/files/import/ngfs/medias/documents/ngfs_first_comprehensive_report_-_17042019_0.pdf (E.T.: 01.08.2025)

İklim riskinin finansal risk yönetimine entegrasyonu, bankaların sermaye yeterliliği ve risk politikalarında kritik bir yer tutmaktadır. Bu sebeple İngiltere Merkez Bankası'nın geliştirdiği "*İki Yıllık İklim Senaryosu (Climate Biennial Exploratory Scenario– CBES)"* gibi yapay zekâ ve senaryo analizine dayalı modeller, finansal kurumların iklim riskine dayanıklılıklarının ölçümünde rol oynamaktadır[194]. Ek olarak, ECB ve EBA gibi kurumlar da iklim riskini kapsayan stres testleri ve kurumsal rehberlikler yayımlayarak bu alandaki düzenleyici çerçeveleri desteklemektedir[195].

II. RİSK MERKEZİNİN FAALİYET ALANI VE AMAÇLARI

5411 sayılı Bankacılık Kanunu'nun 73. maddesi ve Ek m. 1 uyarınca kurulan Risk Merkezi, kredi kuruluşları ve finansal kuruluşlar tarafından müşterilere ait finansal verilerin toplanması, paylaşılması ve yükümlülüklerin izlenmesine yönelik yasal bir temele dayalı olarak faaliyet göstermektedir. Başlangıçta yalnızca bankacılık sektörü için faaliyet gösteren Risk Merkezi, zaman içinde faktöring, finansal kiralama, finansman, sigorta şirketleri gibi kuruluşları da kapsayacak şekilde genişlemiştir. Böylece, geniş tabanlı veri paylaşımıyla beraber finansal sistemin bütün olarak izlenebilmesi ve denetlenebilmesi mümkün kılınmıştır.

Risk Merkezi'nin temel amacı, finansal kuruluşların kredi tahsis süreçlerinde şeffaflık ve bilgiye dayalı olarak karar verme imkânlarını artırmaktır. Bu amaçla, müşterinin borç ödeme performansı, mevcut borç durumu ve geri ödeme alışkanlıkları hakkında tarafsız ve somut veriler içeren risk raporları oluşturarak hem kredi veren kuruluşlar için hem de kredi başvurusunda bulunan kişi veya işletmeler için stratejik karar desteği sunmaktadır[196].

Risk Merkezi bireylerin kredi borç bilgilerini, kredi kartı bilgilerini, çek ve senet işlem bilgilerini, karşılıksız çek kayıtlarını ve genel borçluluk durumlarına ilişkin bilgilerini bünyesinde bulundurmaktadır. Bununla beraber, yalnızca bireysel kredi riskleriyle sınırlı bir işlev üstlenmemekte, özellikle büyük meblağlı kurumsal kredilerin tahsislerinde firma bazlı

---

[194] İngiltere Merkez Bankası, "2021 İki Yıllık İklim Senaryosu (CBES) Sonuçları *İ*klim Değişikliğinden Kaynaklanan Finansal Riskler *(*Boe Publishes Results Of The 2021 Biennial Exploratory Scenario: Financial Risks From Climate Change)", 2022. https://www.bankofengland.co.uk/news/2022/may/boe-publishes-results-of-the-2021-biennial-exploratory-scenario-financial-risks-from-climate-change (E.T.: 01.08.2025)

[195] ECB, "2022 Euro Sisteminin Bilançosuna Yönelik İklim Riski Stres Testi Sonuçları *(*Results of the 2022 Climate Risk Stress Test of the Eurosystem Balance Sheet)", 2023. https://www.ecb.europa.eu/press/economic-bulletin/focus/2023/html/ecb.ebbox202302_06~0e721fa2e8.en.html (E.T.: 01.08.2025)

[196] BDDK, Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği, m. 1 ve m. 6.

piyasa risklerini ve likidite yapılarını izlemeye olanak sağlaması yönüyle sistemik riskleri önleme fonksiyonuna da sahiptir. Bu anlamda Risk Merkezi erken uyarı sinyalleri veren destek altyapısına sahip bir mekanizma niteliği taşımaktadır.

Bireysel müşterilerin yanında ticarî müşterilere ait veriler de Risk Merkezi tarafından analiz edilmekte ve firmaların finansal geçmişleri, borç yükleri, teminat durumları ve sektörel risk analizleri gibi bilgiler Risk Merkezi aracılığıyla toplanmakta ve bankalara rasyonel karar alma süreçlerinde kullanılmak üzere iletilmektedir. Kredi riski yönetimi süreci yalnızca bireysel temerrüt tahminlerine değil, aynı zamanda yapısal ve kurumsal bilgi paylaşımı mekanizmalarına da dayanmaktadır. Risk Merkezi, topladığı müşteri kredi bilgilerini geçmiş ödeme davranışlarına dayalı olarak analiz ederek finansal kuruluşların daha sağlıklı bir şekilde kredi tahsis kararları almalarına destek olmaktadır. Bu kapsamda uygulanan veri analizi yöntemleri hem müşteri ilişkileri yönetimi ve stratejilerinin geliştirilmesinde hem de kredi tahsis süreçlerinde daha isabetli kararlar alınmasını sağlamaktadır[197].

Özellikle son yıllarda büyük veriye dayalı tahmin sistemlerine olan ihtiyacın artmasıyla Risk Merkezi, kredi skorlama, risk sınıflandırması ve otomatik karar destek mekanizmaları ile bankacılık sektörüne stratejik katkılar sağlamaktadır. Risk Merkezi veri aktarımını sağlamanın yanı sıra finansal kuruluşlara analiz edilmemiş ham veriler sunması sayesinde geçmişe dönük veri toplayan pasif bir yapı olmaktan çıkıp kredi risk yönetim süreçlerini destekleyen aktif bir bilgi paylaşım mekanizmasına dönüşmektedir[198]. Finansal kuruluşlar bu verileri kullanarak kendi risk değerlendirme ve skorlama süreçlerini geliştirmekte; böylece kredi başvurularında onay veya ret kararları daha nesnel, veri temelli ve otomatik bir şekilde verilebilmektedir[199].

Risk Merkezi, bankalar ve diğer finansal kuruluşlardan topladığı müşteri verileri sayesinde kişilerin ya da şirketlerin ödeme kabiliyetleri, gecikmiş borçları ve geçmiş kredi performanslarını içeren raporlar oluşturmaktadır. Bu raporlara hem finansal kuruluşlar hem

[197] Talha Öcal, "Bankacılıkta Kredi Riski Yönetimi, Kredi Riski Ölçüm Modelleri ve Türkiye Uygulaması", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2022, s. 1.
[198] BDDK, Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği, m. 3/h.
[199] Caner Taş, "Şimdi Al Sonra Öde Müşterilerinin Kredi Risk Skorlamasında Makine Öğrenmesi ve Standart Kredi Risk Modellerinin Performanslarının Karşılaştırılması (Comparison of Machine Learning and Standard Credit Risk Models Performances in Credit Risk Scoring of Buy Now Pay Later Customers)", Yayımlanmamış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi, 2023, s. 11.

de bireyler tarafından e-Devlet üzerinden erişilebilmekte, bu durum veri şeffaflığı ve bireysel finansal farkındalık açısından önemli bir gelişme olarak nitelendirilmektedir[200].

Ek olarak, dijitalleşme ve teknolojik gelişmeler doğrultusunda yapay zekâ, büyük veri analitiği gibi araçların kullanımının Risk Merkezi'nin veri işleme kapasitesini artırmasına katkı sağlayabilir. Bu kapsamda sadece geleneksel kredi geçmişi değil, müşterilere ait sosyodemografik bilgiler, kredi kartı işlem geçmişi, hesap hareketleri ve sosyal medya verilerinin de analiz süreçlerine dâhil edilmesi, veri çeşitliliğinin artmasına ve yeni nesil risk analiz yöntemlerinin gelişmesine katkı sağlayabilir.

III. RİSK MERKEZİ'NİN ROLÜ VE ETKİLERİ

Türkiye Bankalar Birliği bünyesinde faaliyet gösteren Risk Merkezi, finansal kuruluşların bireylere ve kurumlara kredi tahsis ederken yararlandığı merkezî bir yapı olarak, objektif risk verileri sunmaktadır. Müşterilere ait finansal verilerin merkezî bir yapıda toplanması, bankacılık faaliyetlerinde risk analizinin daha isabetli yapılmasını sağlamaktadır. Bununla beraber, Risk Merkezi aynı zamanda kredi piyasalarının güvenliğini sağlama, sistematik riskleri azaltma ve bireysel finansal davranışları şekillendirme gibi etkilere sahiptir. Böylece, kredi tahsis süreçlerinde karar verici mekanizmaların güvenilirliği artmakta ve borçluların finansal davranışlarının da kayıt altına alınması mümkün kılınmaktadır. Bu anlamda, Risk Merkezi, kamu yararı ve özel sektörün ihtiyaçları arasında dengeli bir yapı sunarak veri temelli finansal anlayışın somut bir yansıması olmaktadır.

Kredi veren kuruluşlar, Risk Merkezi'nin sağladığı raporlarda yer alan bireysel ve ticarî kredilere ilişkin toplam kredi bakiyeleri, takipteki alacak tutarları, protestolu senet bilgileri ve kredi türlerine göre borç dağılımları gibi veriler aracılığıyla müşterilerin genel borçluluk düzeyini ve finansal durumunu değerlendirebilmektedir. Böylece kredi piyasasında bilgi asimetrisi azalmaktadır[201]. Bunun yanı sıra, tüm bu değerlendirmeler yalnızca bireysel müşteri bazında değil, sektörel ya da bölgesel düzeydeki kredi risklerini analiz etmek için de kullanılmaktadır. Örneğin, TCMB ve BDDK gibi otoriteler, makroekonomik analizler için Risk Merkezi'nin sunduğu veri altyapısından faydalanmaktadır. Bu durum Risk Merkezi'ni mikro düzeyde bireysel kredi notlarının oluşturulmasından, makro düzeyde ise sektörel risk analizlerine kadar uzanan bir veri

[200] TBB Risk Merkezi, Türkiye Bankalar Birliği Risk Merkezi Raporlarının E-Devlet Kapısından Sunulmasına İlişkin Kamuoyu Duyurusu, 2019. https://www.tbb.org.tr/duyurular/pdf/2816 (E.T.: 01.08.2025)
[201] Türkiye Bankalar Birliği Risk Merkezi, "2023-2024 Faaliyet Raporu", s. 39.

ekosistemi hâline getirmektedir. Bu sayede Risk Merkezi finansal sistemin erken uyarı mekanizmalarından biri olarak da vücut bulmaktadır. Bu da Risk Merkezi'nin sadece veri sağlayan bir yapı değil, aynı zamanda veri etiği ve sorumluluğu taşıyan bir kurum olması gerektiğini ortaya koymaktadır[202].

Tüm bu gelişmeler çerçevesinde, Risk Merkezi'nin yalnızca bilgi depolayan bir yapı olarak değil, aynı zamanda yüksek sorumlulukla veri yöneten bir kurum olarak sürekli denetime açık, şeffaf olarak KVKK ile uyumlu bir yapıda faaliyet göstermesi gerekmektedir. Finansal sistemde güvenin tesis edilmesi için müşteri bilgilerinin doğru ve güvenli bir şekilde işlenmesi gerekmektedir. Risk Merkezi'nin gelecekte daha gelişmiş teknolojilerle desteklenmesi veri analiz süreçlerini daha etkin hâle getirecektir, bu sayede finansal sisteme katkı sunulacaktır.

Ek olarak, TBB tarafından düzenli olarak yayımlanan Risk Merkezi Bültenleri sayesinde, bireyler ve tüzel kişiliklere ilişkin borçluluk düzeyi, tasfiye edilecek alacakları, ödeme davranışları, kredi kartı gecikmeleri gibi göstergelere ulaşabilmektedir. Bu da ekonomik karar alma süreçlerinde veri temelli yaklaşımların gelişmesine katkı sunmaktadır ve bu sayede finansal piyasalardaki güven unsuru güç kazanmaktadır.

Risk Merkezi bireylerin ve işletmelerin krediye erişim koşullarını dolaylı olarak şekillendirdiğinden, ödeme alışkanlıklarına dair bilgiler müşterilerin finansal davranışlarını daha temkinli hâle getirmektedir. Örneğin, bir kişinin kredi kartı borçlarını zamanında ödememesi Risk Merkezi kayıtlarına yansıyacak ve bu durum ilerleyen süreçte kredi notunu düşürerek konut kredisi veya taşıt kredisi gibi yüksek tutarlı finansman imkânlarına erişimi zorlaştırabilecektir. Bireysel düzeyde bakıldığında kredi skorları, bireylerin sadece finansal yaşamını değil, aynı zamanda sosyal yaşamlarını da etkileyebilmektedir. Örneğin, kiralama, abonelik gibi hizmetlere erişimi kısıtlayabilmekte, finans sektörü gibi özel alanlarda istihdam fırsatlarını da dolaylı olarak etkileyebilmektedir. Bu sebeple, kredi notlarının bireyler arasında eşitsizlik yaratabilecek potansiyeli göz önünde bulundurularak veri işleme süreçlerinin etik değerlere ve kişisel haklara uygun olarak yürütülmesi gerekmektedir.

Risk Merkezi'nin kredi geçmişi bulunmayan bireylerin ödeme alışkanlıklarını yansıtan alternatif veri kaynaklarını sisteme entegre ederek kişi profilleri oluşturması, kredi bilgisi mevcut olmayan bireylerin değerlendirilmesi bakımından faydalı olacaktır. Bu

[202] Türkiye Bankalar Birliği Risk Merkezi, "2024-2025 Faaliyet Raporu", s. 56.

kapsamda fikir verecek olan elektrik, su, doğal gaz, telekomünikasyon ve internet hizmetleri gibi kamuya dönük ödeme kalemlerine ilişkin verilerle mobil hat ve belediye tahsilatlarına ilişkin ödeme geçmişi bireylerin ödeme alışkanlıkları hakkında fikir veren göstergeler olarak değerlendirilebilir. Söz konusu veriler, bu hizmetleri sağlayan kurumlarla TBB Risk Merkezi veya teknik uygulayıcısı olan KKB A.Ş. arasında imzalanan veri protokolleri çerçevesinde KVKK'ya uygun olarak, açık rıza temelli mekanizmalar aracılığıyla temin edilebilir. Bu şekilde aktarılacak bilgiler, veri transfer altyapıları ile sisteme entegre edilerek kredi skoru mevcut olmayan bireyler için başlangıç niteliğinde bir risk profili üretmeye yardımcı olabilir.

Tüm bunların sağlanması ve mevcut potansiyeli sebebiyle Risk Merkezi'nin stratejik önemi ve geleceğe yönelik dijital dönüşüm vizyonu önem taşımaktadır. Gelecekte yapay zekâ destekli ileri veri analitiği yöntemlerinin entegre edilmesi, merkezin pasif veri toplayıcı olmanın ötesine geçerek aktif ve öngörücü risk yönetimi fonksiyonları üstlenmesini sağlayacaktır. Bu kapsamda, şeffaflık ve hesap verebilirlik ilkelerinin uygulanması sayesinde veri sahiplerinin hakları daha fazla koruyacak ve finansal piyasaların güvenliği artıracak sürdürülebilir bir veri yönetim modeli oluşturulması gerekmektedir.

IV. RİSK MERKEZİ'NİN UYGULAMADAKİ YETKİSİ

Risk Merkezi yasal olarak Bankacılık Kanunu ve Risk Merkezi Yönetmeliği'ne dayansa da yetkisinin uygulamada nasıl kullanıldığı ancak kamuya açıklanan veriler incelendiğinde somut olarak değerlendirilebilmektedir. TBB Risk Merkezi tarafından yayımlanan aylık bültenler, bu bağlamda önemli bir nitelik taşımaktadır. 2024 yılına ait Ocak, Mart, Haziran, Eylül ve Aralık aylarına ilişkin Risk Merkezi bültenleri incelendiğinde, müşteri verilerinin türü, kapsamı, toplanma biçimi ve paylaşım yoğunluğu hakkında değerlendirme yapabilmek mümkündür.

İlk olarak, toplam kredi bakiyeleri ve bu bakiyelerin kredi türlerine göre dağılımı üzerinden müşteri verilerinin kapsamı değerlendirilebilir. Ocak 2024'te toplam nakdi kredi bakiyesi 11,5 trilyon TL iken, Aralık 2024'te bu tutarın 13,9 trilyon TL'ye ulaştığı görülmektedir. Bu artış sadece ekonomik büyümenin değil, Risk Merkezi'nin işlediği müşteri verisi hacminin de genişlediğini ifade etmektedir. İşlenen veriler bireysel krediler,

konut kredileri, taşıt kredileri, kredili mevduat hesapları ve kredi kartı borçları gibi kalemlerden oluşmaktadır[203].

Bültenlerde en ayrıntılı olarak paylaşılan veri setlerinden biri müşteri sayısıdır. Örneğin Haziran 2024'te bireysel nitelikli müşteri sayısı yaklaşık 39,4 milyon olarak bildirilmişken, Aralık 2024'te bu sayı 40,8 milyona yükselmiştir. Bu artış hem veri havuzunun büyüdüğünü hem de Risk Merkezi'nin işleme yetkisinin bireysel düzeyde ne denli geniş bir kapsama ulaştığını ortaya koymaktadır[204].

Veri setlerinde dikkat çeken bir diğer unsur ise tasfiye olunacak alacakların toplam kredilere oranıdır. Ocak 2024'te bu oran %1,2 iken, Aralık 2024'te %1,8 olarak gerçekleşmiştir. Bu oranlar doğrudan müşteri risk skorlarını etkilemekte ve kredi verilme süreçlerinde belirleyici rol oynamaktadır[205].

Veri paylaşımı konusunda bültenler doğrudan kurum isimlerini açıklamasa da "*veri sağlayıcı kuruluşlar*" başlığı altında kredi bilgisi bildiren sektör sayıları verilmektedir. Mart 2024 itibarıyla 13.835 farklı finansal kuruluş Risk Merkezi'ne bildirimde bulunmuştur. Bu geniş katılım, müşteri verilerinin sektörel olarak nasıl yayıldığını ve Risk Merkezi'nin işleme yetkisinin oldukça güçlü bir konumda olduğunu göstermektedir[206].

Risk Merkezi'nin verileri nasıl işlediğine ilişkin önemli ipuçlarından biri de veri sıklığı ve güncellik düzeyidir. Nitekim Eylül 2024 bülteninde müşterilere ilişkin toplam gecikme oranları gibi göstergeler paylaşılmış, bu veriler kredi riskinin izlenmesine katkı sağlamıştır. Bununla birlikte bültenlerde bireysel düzeyde davranışsal veriler değil, toplu istatistiksel veriler sunulmaktadır. Bu sebeple Risk Merkezi'nin birey bazında detaylı analiz yaptığına dair kamuya açık bir kanıt bulunmamaktadır. Öte yandan, kredi riskine ilişkin verilerin düzenli olarak işlenmesi KVKK kapsamında kişisel veri işleme faaliyeti niteliği taşıması sebebiyle şeffaflık ilkesine uygun bir şekilde ve veri güvenliği gözetilerek yürütülmesi gerekmektedir[207].

[203] Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Ocak 2024, s. 5.; Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Aralık 2024, s. 5.
[204] Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Haziran 2024, s. 9.; Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Aralık 2024, s. 9.
[205] Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Aralık 2024, s. 6.
[206] Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Mart 2024, s. 3.
[207] Türkiye Bankalar Birliği Risk Merkezi, "Risk Merkezi Aylık Bülteni", Eylül 2024, s. 8.

Sonuç olarak, Risk Merkezi'nin uygulamadaki müşteri verisi işleme yetkisi, yasal sınırlar dâhilinde kalmakla birlikte, kapsam açısından oldukça güçlü ve yaygın bir boyuta ulaşmıştır. Bültenler, sadece kredi hacminin değil, veri işlemeye konu müşteri sayısının, veri türlerinin ve veri sağlayıcı kuruluş ağının da sürekli genişlediğini göstermektedir. Bu durum, Risk Merkezi'nin fiilî veri gücünü artırmakla birlikte, kurumun KVKK ve Bankacılık Kanunu kapsamında daha sıkı denetim ve şeffaflık mekanizmalarına tâbi olmasını zorunlu kılmaktadır.

V. RİSK MERKEZİ'NİN VERİ İŞLEME YETKİSİ

Risk Merkezi'nin müşteri verilerini toplama, saklama ve paylaşma yetkisi yalnızca teknik bir uyum işlevi değil, aynı zamanda bireylerin temel haklarını etkileyen hukukî bir yetkidir. Risk Merkezi'nin veri işleme faaliyetlerinin, bireysel hakları gözeten dengeli bir şekilde yürütülmesi ve yasal düzenlemelerin uygulamada da takip edilmesi önem arz etmektedir.

Türk hukukunda kişisel verilerin korunması 6698 sayılı KVKK ile güvence altına alınmıştır. KVKK'nin 5. ve 6. maddelerinde düzenlenen kişisel veri işleme şartları, açık rıza ilkesini temel almaktadır. KVKK'ye göre kişisel veriler, yalnızca ilgili kişinin açık rızası alınarak ya da kanunda öngörülen şartlara dayanılarak işlenebilmektedir. Ancak uygulamada açık rıza unsuru çoğunlukla bankacılık sözleşmeleri içine gizlenmekte, bu durum literatürde "*genel rıza*" olarak adlandırılmaktadır. Bu durum, genel rızanın özgür iradeye dayanma ve belirli amaca yönelik olma şartlarını karşılamadığı yönünde eleştirilere sebep olmaktadır. Nitekim veri paylaşımında yaşanan temel sorunların başında da açık rıza unsurunun zayıflığı ve aydınlatma yükümlülüğünün yeterince yerine getirilmemesi gelmektedir[208].

KVKK Kurulu'nun 31/05/2019 tarihli kararında bir anonim şirketin veri sorumlusu sıfatıyla ilgili kişinin açık rızası olmaksızın cep telefonuna kısa mesaj gönderdiği tespit edilmiştir. KVKK Kurulu, bu işlemin kişisel verilerin hukuka aykırı olarak işlenmesi niteliği taşıdığını ve herhangi bir veri işleme şartına dayanmadığını belirtmiştir. Ayrıca, veri sorumlusunun uygun güvenlik düzeyini sağlamaya yönelik teknik ve idarî tedbirleri almadığı gerekçesiyle 50.000 TL idarî para cezası uygulanmasına karar verilmiştir[209].

---

[208] Merve Arslanhan**,** s. 37.

[209] Kişisel Verileri Koruma Kurulu, 31/05/2019 Tarih ve 2019/162 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)

KVKK m. 10 uyarınca da veri sahiplerinin verilerinin kim tarafından, hangi amaçla işlendiği ve kimlerle paylaşıldığı konusunda bilgilendirilmesi gerekmektedir. Ancak Risk Merkezi'nin veri işleme süreçleri incelendiğinde, bu bilgilendirmelerin çoğu zaman yetersiz olduğu ve başvuru, düzeltme veya silme işlemlerinin karmaşık başvuru sistemlerine tâbi olduğu görülmektedir. Bu bağlamda, yasal düzenlemeler pratikte yeterince uygulanmamaktadır. Kredi başvuru sürecinde bireylerden açık rıza alınmamakta ya da alınan rıza örtük biçimde değerlendirilmekte, veri sahipleri Risk Merkezi kayıtlarını ancak olumsuz bir işlem sonrasında fark etmektedir. Bu sorunun çözümü için bireylere, hangi verilerinin ne amaçla işleneceği, kimlerle paylaşılacağı ve ne kadar süreyle saklanacağı açıkça bir şekilde bildirilmelidir. Ayrıca dijital platformlarda sade, anlaşılır ve geri alınabilir rıza modüllerinin geliştirilmesi de bu kapsamda önemli bir adım olacaktır.

Veri işleme yetkisinin bir diğer tartışmalı yönü ise, otomatik karar alma süreçlerinde veri güvenliği riskidir. TBB Risk Merkezi verileri genellikle pasif raporlama ve kredi raporlaması gibi işlemlerde kullanmaktadır. Bu sistemlerde kullanılan verilerin eksik, hatalı olması veya güncel olmaması durumunda, bireyler sistematik olarak haksızlığa uğrayabilmektedir. GDPR m. 22, bireylerin yalnızca otomatik işleme sonucunda haklarını etkileyen kararlara tâbi tutulamayacağını belirtmektedir. Türk hukukunda ise bu yönde açık ve bağlayıcı bir düzenleme bulunmamaktadır, dolayısıyla bu hakların mevzuatta karşılığı sınırlı olmaktadır. Ancak, Türk Ceza Kanunu (TCK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi düzenlemeler, kişisel verilerin güvenliği ve işlenmesi konusunda genel ilkeler getirmektedir. Bu sorun karşısında yapılması gereken, otomatik karar alma sistemlerinde şeffaflık ve hesap verebilirlik ilkelerini hayata geçirmektir. Bireylere bu kararlara itiraz etme ve kararların güncel olarak yeniden değerlendirilmesini talep etme hakkı tanınmalıdır.

Ayrıca, alternatif veri kaynaklarının kullanımı beraberinde bazı mahremiyet ve güvenilirlik risklerini de getirmektedir. Özellikle sosyal medya ve dijital takip verilerinin kullanımı konusunda henüz net düzenlemeler ve standartlar mevcut değildir. Bu durum, veri sahiplerinin bilgilendirilmesi ve onay süreçlerinin güçlendirilmesini gerektirmektedir. Ayrıca, bu tür verilerin doğruluğu ve yanıltıcı olmaması için denetim mekanizmalarının geliştirilmesi önem taşımaktadır.

Veri sorumlusu ve veri işleyen ayrımı da uygulamada sıkça karışıklığa neden olmaktadır. Risk Merkezi hukukî boyutta, verileri toplayan ve paylaşan bir yapı olarak veri

sorumlusu sıfatını taşımaktadır[210]. Ancak uygulamada müşteriler kendi verileriyle ilgili taleplerini önce muhatap bankaya iletmektedir. Risk Merkezi direkt olarak bireysel başvurulara açık bir mekanizmaya sahip olmadığından, fiilen veri sorumlusu olarak sahip olduğu yükümlülüklerin bir kısmı müşteriler nezdinde bankalar üzerinden ilerlemektedir. Bu durum, özellikle veri ihlali söz konusu olduğunda mağdur müşterinin hak arama sürecinde zorluk yaşamasına neden olmaktadır. Bu bağlamda Türkiye'deki mevcut modelin hem KVKK hem de uluslararası normlara uyumlu hâle getirilmesi gerekmektedir.

Sonuç olarak, Risk Merkezi'nin müşteri verilerini işleme yetkisi teknik olarak yasal düzenlemelere dayansa da uygulamada veri koruma hukuku, şeffaflık ve müşteri haklarıyla tam uyum içinde değildir. Türk hukukunda AB standartlarına yaklaştırılması gerektiğinden Risk Merkezi'ne bildirilen verilerin içeriği, kullanım amacı ve paylaşım biçimi daha sıkı denetim altına alınmalı, bireylerin veri üzerindeki kontrol mekanizmaları güçlendirilmelidir. Aksi durumda bu sistem bireylerin mahremiyet hakkı ile ilgili riskleri barındırmaya devam edecektir.

VI. RİSK MERKEZİ'NİN VERİ KORUMA YÖNTEMLERİ

Risk Merkezi tarafından işlenen müşteri verileri, yüksek güvenlik gerektiren finansal bilgiler içermesi nedeniyle özel güvenlik tedbirlerine tâbi tutulmaktadır. Ayrıca, bilgi güvenliği politikalarının belirlenmesi, veri ihlallerinin raporlanması, risk analizlerinin değerlendirilmesi ve teknik idarî önlemlerin takibi gibi görevler üstlenmiştir. Bu süreç, düzenli aralıklarla yapılan toplantılarla ve KVKK başta olmak üzere ilgili mevzuata uyumun sürekliliğini denetlenmesi suretiyle yürütülmektedir. Ayrıca, bilgi güvenliği risklerinin sürekli olarak değerlendirilmesi ve iyileştirilmesi amacıyla, "*Uluslararası Standardizasyon Örgütü (International Organization for Standardization– ISO)*" gibi uluslararası standartlar çerçevesinde, Deming Döngüsü olarak da adlandırılan "*PDCA Döngüsü (Planla– Uygula– Kontrol Et– Önlem Al)* (*Plan- Do- Check-Act– PDCA*)" takip edilerek bilgi güvenliği riskleri sürekli değerlendirilmekte ve iyileştirilmesi için gerekli adımlar atılmaktadır[211].

Risk Merkezi, veri sorumlusu sıfatıyla, KVKK'nin 12. maddesi doğrultusunda verilerin yetkisiz erişime, kazara silinmeye, değiştirilmesine ya da yasa dışı şekilde ifşâsına karşı korunması için gerekli idarî ve teknik tedbirleri almakla yükümlüdür. Bu kapsamda,

[210] Merve Arslanhan, s. 53.
[211] Bilgin Metin, "Sürdürülebilir Kişisel Veri Güvenliği Yönetişimi", *KVKK Akademik Derleme Çalışması* içinde, Kişisel Verileri Koruma Kurumu Yayınları, 2021, s. 355.

erişim kontrol sistemleri, log kayıtları ve çift faktörlü kimlik doğrulama mekanizmaları, şifreleme teknikleri, güvenlik duvarları, kullanıcı kimlik doğrulama sistemleri, düzenli sızma testleri ve ihlal hâlinde 72 saat içinde Kuruma ve ilgili kişilere bildirimde bulunulması gibi teknik tedbirlerle desteklenmektedir[212].

Veri güvenliğine dair eksiklikler hukukî olmanın yanı sıra kültüreldir. European Central Bank'ın vurgulandığı üzere, kurumların veri koruma kültürünü geliştirmesi gerekmektedir[213]. Türkiye'de ise veri koruma çoğunlukla teknik önlemlere sınırlı kalmakta, çalışan eğitimi, süreç denetimi ve yönetsel şeffaflık gibi unsurlar yeterince uygulanmamaktadır. Oysa teknik önlemler, insan kaynaklı veri sızıntısı risklerini tamamen ortadan kaldırmakta yetersiz kalabilmektedir.

Veri koruma kültürünün Türkiye'de geliştirilebilmesi mevzuata uyum sağlamanın yanında organizasyonun tüm katmanlarına gizlilik ve hesap verebilirlik bilincinin yerleşmesi ile mümkün olacaktır. Özellikle veri işleme ve raporlama birimlerinde çalışanların KVKK farkındalık düzeylerinin artırılması bu riskleri minimize etmekte etkili olacaktır. Nitekim KVKK Kurulu'nun 09/07/2020 tarihli kararında görüldüğü üzere, banka personelinin 23 müşteriye ait TBB Risk Merkezi skorlarını ve TCKN bilgilerini WhatsApp adlı uygulama üzerinden üçüncü kişilerle paylaşması ve aynı personelin 1.052 kişi için 10.529 adet KKB sorgulaması gerçekleştirmesine rağmen bu durumun fark edilmemesi iç denetim sistemlerindeki zafiyeti ortaya koymaktadır. Bu karar iç denetim veri güvenliği süreçlerinde yalnızca teknik tedbirlerin yeterli olmadığı, çalışan eğitimi, iç kontrol ve denetim mekanizmalarının da sürece dâhil edilmesi gerektiğini ortaya koymaktadır[214].

Müşteriye ait detaylı davranışsal ve performans verilerinin toplanması bu verilerin açık rıza temelli olmadan ve çoğu zaman anonimleştirilmeden sistemde işlenmesi, orantılılık ve ölçülülük ilkelerini ihlal eden bir uygulama olarak karşımıza çıkmaktadır. Bu bağlamda, Risk Merkezi'nin topladığı veri setlerinin genişliği ve bu verilerin işlenme amaçları arasındaki orantısızlık belirginleşmektedir. Önerilen çözüm ise veri işleme amacına uygun bir şekilde veri yelpazesinin daraltılmasıdır. Risk değerlendirme süreçlerine hizmet etmeyen ikincil nitelikteki verilerin toplanmasından kaçınılmalı, toplandığı takdirde ise

[212] Bilgin Metin, s. 366.
[213] ECB, Yönetişim ve Risk Kültürüne İlişkin Taslak Kılavuz, s. 7.
[214] KVKK Kurulu'nun 09/07/2020 Tarih ve 2020/530 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)

anonimleştirme veya maskeleme teknikleri zorunlu hâle getirilmelidir. Böylece veri güvenliği ve bireysel haklar arasında denge sağlanacaktır.

Bankacılık Kanunu'nun 73. maddesinde belirtilen finansal yükümlülüklere ilişkin bilgilerin paylaşılması hükmü, uygulamada veri türleri ve saklama süreleri bakımından oldukça geniş yorumlanmaktadır ve kişisel verilerin sınırsız süreyle muhafaza edilmesine zemin oluşturmaktadır. Risk Merkezi'nin bankalar, faktöring ve finansal kiralama şirketlerinden topladığı verilerin uzun süreli ve geniş kapsamlı analizlere tâbi tutulması, KVKK'ye aykırı sonuçlar doğurarak veri sahiplerinin temel haklarını tehdit etmektedir. Benzer şekilde, GDPR de veri işleme faaliyetlerinin spesifik, açık ve ölçülü olması gerektiğini vurgulamaktadır. Bu sebeple, veri işleme yetkisinin hem içerik hem de zaman açısından açık olarak sınırlandırılması gerekmektedir. Risk Merkezi yalnızca gerekli, belirli verileri işlemeli ve verilerin saklama süresi mevzuata uygun ve şeffaf bir şekilde netleştirilmelidir. Ayrıca, veri işleme gerekçeleri ve kapsamı hakkında müşteriler detaylı bir şekilde bilgilendirilmeli ve bu sürece ilişkin denetimler etkinleştirilmelidir.

Veri minimizasyonu ilkesi doğrultusunda yalnızca işlenmesi zorunlu olan veriler toplanmalıdır. Bu durum KVKK'nin 4. maddesinde yer alan veri minimizasyonu ve amaçla sınırlılık ilkeleriyle doğrudan ilişkilidir. Bu çerçevede, Risk Merkezi hem "*veri sorumlusu*" hem de "*veri işleyen*" sıfatlarıyla, KVKK ilkelerine doğrudan bağlı olarak özellikle açık rıza, veri minimizasyonu ve saklama süresi ilkeleri bakımından mevzuata uyumlu bir yapı sergilemek zorundadır[215]. Nitekim, KVK Kurulu 2023/1430 sayılı kararında, yemek kartı hizmeti sunan veri sorumlusunun mobil uygulamada T.C. kimlik numarasını gereksiz şekilde işlemesinin veri minimizasyonu ilkesine aykırı olduğunu ve ilgili kişilerin zarar görmesine sebep olabileceğini belirterek yalnızca telefon numarası ve kart bilgisi ile doğrulama yapılabileceğini belirtmiştir. Aynı zamanda, T.C. kimlik numarasının hukukî dayanak olmadan işlenmesi ve amaçla ölçülü işlenmesi ilkesine aykırılık nedeniyle veri sorumlusuna 200.000 TL idarî para cezası vermiştir. Bu karar minimizasyonu ilkesinin ihlali nedeniyle gereğinden fazla veri işlenmesinin hukuka aykırı olduğunu belirtmekle beraber, önemli bir uyarı olarak niteliği taşımaktadır[216].

[215] Ezgi Alımcı, "Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi", *Ankara Barosu Dergisi*, Cilt 80, Sayı 1, 2021, s. 58.
[216] Kişisel Verileri Koruma Kurulu, 17/08/2023 Tarih ve 2023/1430 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)

Uygulamada veri aktarımı konusunda bazı hukukî ihtilaflar gündeme gelmektedir. Özellikle bankaların, müşterilerin açık rızası olmaksızın Risk Merkezi'ne veri aktarması veya bu verilerin üçüncü taraflara paylaşılması hâlinde, KVKK'ye aykırılık iddialarıyla şikâyetler gündeme gelmektedir. Ancak KVKK Kurulu, bu tür uyuşmazlıklarda Risk Merkezi'nin kamu yararına hizmet eden bir yapı olduğunu ve mevzuat kaynaklı istisnai durumların veri aktarımı için yeterli yasal zemini sağladığını ifade etmektedir. Nitekim Kurul'un 31/08/2023 tarihli kararında, bankaların müşterilerine ait kişisel verilerini Risk Merkezi'ne aktarmasının KVKK m. 5'e dayanması sebebiyle hukuka uygun olduğu belirtilmiş olup, açık rıza olmaksızın Risk Merkezi'ne veri aktarımının yasal düzenlemelere dayandığı takdirde ilgili kişilerden açık rıza alınmasına gerek olmadığını ortaya koymuştur. Öte yandan, Kurul tarafından veri minimizasyonu ilkelerine uygun hareket edilmesi gerektiği belirtilmiş ve veri aktarımının yasal zemin üzerinden gerçekleştirilmesinin gerekli olduğu ifade edilmiştir. Özetle, Risk Merkezi'ne veri aktarımının belirli istisnalar çerçevesinde hukuka uygun olduğu ortaya koyulmuştur.[217]

KVKK'nin 4. maddesi uyarınca, kişisel verilerin amaçla bağlantılı kullanılabilmesi için işlenen verilerin doğru ve güncel olması gerekmektedir. Fakat, Risk Merkezi Yönetmeliği'nin 24. maddesi, Risk Merkezi'nin üyeler ya da kaynak kuruluşlar tarafından verilen bilgilerin doğruluğunu araştırma yükümlülüğü olmadığını ifade etmektedir. Otomatik karar alma sistemlerinde kişisel verilerin kullanıldığı dikkate alındığında, Risk Merkezi'nin pasif konumu, veri güvenliği ilkeleriyle bağdaşmamaktadır.

Bankalar tarafından Risk Merkezi'ne gönderilen verilerde hata, eksiklik olması veya güncellik olmaması hâlinde, bireylerin kredi notlarını doğrudan etkilendiğinden haksız bir şekilde finansal erişimlerin kısıtlanması söz konusu olabilmektedir. Örneğin, Kişisel Verileri Koruma Kurulu'nun 02/11/2021 tarihli bir kararında, bir bankanın müşterisinin ödeme davranışlarına ilişkin veriyi Risk Merkezi'ne yanlış aktarması sebebiyle, kişinin kredi notunun haksız şekilde düşük tutulduğu ve bu durumun ilgili kişinin önemli finansal faaliyetlerinde mağduriyet yaşamasına sebep olduğu vurgulanarak veri sorumlusuna 150.000 TL idarî para cezası verilmiştir[218].

[217] Kişisel Verileri Koruma Kurulu, 31/08/2023 Tarih ve 2023/1509 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)
[218] Kişisel Verileri Koruma Kurulu, 02/11/2021 Tarih ve 2021/1107 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)

Bu sorunun çözümü için Risk Merkezi'ne, kaynak kuruluşlardan aldığı verilerin doğruluğunu kontrol etme görevinin yüklenmesi gerekmektedir. Ayrıca, veri sahibi konumundaki bireyler, kredi puanı oluşum süreçlerine dair bilgiye ulaşamamakta, otomatik karar alma mekanizmalarına itiraz edememekte ve işlenen veriler üzerinde yeterli kontrole sahip olamamaktadır. Tüm bu sebeplerle, bireylere verileri üzerinde düzenleme, düzeltme ve güncelleme talebinde bulunabilecekleri şeffaf ve erişilebilir bir başvuru mekanizması üzerinden dijital sistemin ayrıcalıklarından faydalandırarak Merkez'e iletilen bilgilerin güncel olması da sağlanabilir.

Veri işleme faaliyetleri TBB Risk Merkezi Yönetmeliği'nin 11. maddesi ile de sınırlandırılmıştır. Bu maddeye göre, müşteri bilgilerinin kimlerle ve ne koşullarda paylaşılabileceği düzenlenmekte ve birtakım kurallara bağlanmaktadır. Paylaşılan veriler ise yalnızca yetkili kurum ve kişilere, yasal zorunluluk hâlinde ve açık rıza çerçevesinde iletilmekte, bu süreçte amaçla sınırlı kullanım ve belirli süre ile saklama ilkeleri esas alınmaktadır. Risk Merkezi tarafından hazırlanan raporların paylaşımı da bu yasal düzenlemelere uygun olarak gerçekleştirilmektedir.

Benzer şekilde Risk Merkezi Yönetmeliği'nin 19. maddesi, elde edilen verilerin yalnızca ilgili finansal kuruluşlar tarafından kendi faaliyetleri kapsamında kullanabileceğini belirtmesine rağmen bazı verilerin üçüncü kişilerle, özellikle faktöring şirketleriyle paylaşıldığı tespit edilmiştir. KVKK Kurulu'nun 03/03/2020 tarihli kararında, bazı faktöring şirketlerinin TBB Risk Merkezi üzerinden gerçekleştirdikleri veri paylaşımında yetkilerini aşarak kişisel verileri hukuka aykırı şekilde üçüncü kişilerle paylaştıkları ve bu verileri amaçları dışında kullandıkları belirtilmiştir. Bu durumun veri ihlali niteliği taşıması sebebiyle ilgili faktöring şirketlerine idarî para cezası uygulanmıştır. Bu kararlar, normatif düzenlemelere rağmen Risk Merkezi verilerinin koruma altına alınamadığını ve sistemde ciddi uygulama boşlukları bulunduğunu göstermektedir[219].

Her ne kadar Risk Merkezi bu karar bağlamında doğrudan sorumlu tutulmamış olsa da sistemin işleyişinde karşılaşılan bu tür ihlallerin önlenebilmesi için veri paylaşım süreçlerinin daha sıkı denetlenmesi ve taleplerin yalnızca yasal dayanağa ve belirli amaca uygun taleplerin karşılanması gerekmektedir. Ayrıca veri paylaşım protokollerinin yeniden gözden geçirilmesi, veri taleplerinin yalnızca mevzuata uygun, açık rızaya dayalı ve amaçla

[219] Kişisel Verileri Koruma Kurulu, 03/03/2020 Tarih ve 2020/191 sayılı karar. (www.kvkk.gov.tr E.T.: 01.08.2025)

sınırlı biçimde karşılanması sağlanmalıdır. Ayrıca, izinsiz veri aktarımı yapan kurumlara karşı etkin yaptırımlar uygulanması gerekmektedir.

Buna ek olarak, BDDK tarafından yayımlanan *"Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik"* bankaların müşteri verilerini üçüncü kişilerle yalnızca açık rıza ya da yasal zorunluluk hâllerinde paylaşabileceğini belirtmektedir. Bu Yönetmelik'te verilerin yalnızca açık rıza veya kanuni zorunluluk durumunda paylaşılabileceği belirtilmekle beraber, paylaşımların amaçla sınırlı ve orantılı olması gerektiği de vurgulanmaktadır. Bu durum meşru menfaat gibi dolaylı hukukî gerekçelerin de uygulamada dikkate alınabileceğini göstermektedir.

Risk Merkezi'nin veri işleme faaliyetleri alanında bağımsız ve proaktif bir denetim mekanizması mevcut değildir. KVKK Kurulu yalnızca şikâyet üzerine harekete geçmektedir. Oysa GDPR'nin 58. maddesi kapsamında, veri işleyen tüm merkezî yapılar bağımsız veri denetim otoriteleri tarafından düzenli olarak incelenmektedir. Veri transfer süreçleri teknik standartlara bağlanmış olsa da kamuya açık ve düzenli değerlendirme raporlarının olmayışı, şeffaflık ilkesini ihlal etmektedir. Bu sebeple, KVKK Kurumu ile koordineli çalışan bağımsız bir Veri Denetim Komitesi kurulması gerekmektedir. Bu komite, Risk Merkezi'nin veri işleme süreçlerini şeffaf biçimde incelemeli ve kamuoyuna düzenli raporlama yapmalıdır. Bu şekilde GDPR'de yer alan veri sorumlusu üzerindeki bağımsız denetim modeline benzer olarak hukuka uygunluk denetimi süreklilik kazanacaktır.

Türkiye'nin finansal altyapısının dijitalleşmeye uyum süreci devam ederken müşteri verilerinin doğru, güvenli ve öngörüsel olarak işlenmesi hem sistemsel risklerin azaltılmasını hem de sürdürülebilir bankacılığın inşasını sağlamaktadır. Ancak, müşteri verilerinin işlenmesi hem operasyonel hem de yasal ve etik sorumlulukları beraberinde getirmektedir. Nitekim, 2019 yılında TBB Risk Merkezi üzerinden bazı ING Bank çalışanlarının yaptığı usûlsüz sorguların, gerçek kişi tacirlere ait kredi verileri ve kimlik bilgileri gibi kişisel verilerin dışarıya aktarılmasına yol açtığı tespit edilmiş ve bu durum kamuoyuna duyurulmuştur. Kişisel Verilerin Korunması Kurumu tarafından yayımlanan 2019/43 sayılı kararda, veri sızıntısına neden olan yetkisiz erişimlerin Risk Merkezi sorgulama altyapısı üzerinden gerçekleştiği belirtilmiş ve bu kapsamda kamuoyunun bilgilendirilmesine karar verilmiştir[220]. Bu tür ihlallerin yalnızca hukukî değil, kurumsal

[220] Kişisel Verileri Koruma Kurulu, 01/03/2019 Tarih ve 2019/43 sayılı karar. (www.kvkk.gov.tr E.T.: 01.08.2025)

itibara ilişkin sonuçlar da doğurmasından dolayı, veri işleyen tüm kuruluşları daha güçlü teknik ve idarî tedbirler almak zorundadır.

ECB'nin 2024 tarihli "*Risk Culture Guide*" raporunda da belirtildiği üzere, veri güvenliği yalnızca teknik değil, kurumsal karar alma mekanizmalarının da konusu hâline gelmelidir. Bu kapsamda bankaların yönetim kurullarının veri koruma politikalarını düzenli olarak gözden geçirmesi önerilmektedir. Türkiye'de ise veri güvenliği uygulamalarının büyük oranda teknik personel düzeyinde yürütüldüğü ve üst düzey denetiminin artırılması gerektiği yönünde eleştiriler mevcuttur[221].

Bank for International Settlements (BIS) tarafından yayımlanan ve uluslararası bankacılık sistemlerinde veri işleme standartlarını belirleyen *"Principles for Effective Risk Data Aggregation and Risk Reporting"* başlıklı belgede de finansal veri işleme sistemlerinin şeffaf, zamanlı, doğru ve denetlenebilir olması gerektiği vurgulanmaktadır[222]. Risk Merkezi'nin aylık bültenlerinde de görüldüğü üzere, müşteri verileri kategorilere ayrılarak istatistiksel biçimde sunulmakta ancak veri kalitesine, güncelliğine ya da hukukî uygunluk derecesine veya herhangi bir iç kontrol mekanizmasına dair bilgi paylaşılmamaktadır.

Sonuç olarak, Risk Merkezi'nin veri işleme yetkisi, teknik bir işlem silsilesi olmanın yanında, temel hak ve özgürlüklerle bağlantılı, çok boyutlu bir sorumluluk anlamına gelmektedir. Anayasa'nın özel hayatın gizliliği ilkesine ve KVKK'nin temel ilkelerine uygunluk, bu sürecin meşruiyetinin en temel zeminini oluşturmaktadır. Verinin işlenmesi, paylaşılması ve analiz edilmesi süreçlerinde hem bankacılık etiğine hem de dijital çağın şeffaflık ilkelerine uygun davranmak, Risk Merkezi'nin sürdürülebilirliğini sağlamak açısından önem arz etmektedir.

VII. TBK AÇISINDAN BANKA SIRRI İHLALİNDE SORUMLULUK

Banka müşteri sırrını hukuka aykırı biçimde Risk Merkezi'ne aktardığı taktirde ortaya çıkan zarardan ilk olarak veriyi ifşa eden banka, ikinci olarak ise bu veriyi kullanarak zararın gerçekleşmesine katkıda bulunan Risk Merkezi sorumludur. TBK m. 61 uyarınca, birden fazla kişinin aynı zarara birlikte sebebiyet vermesi durumunda veya çeşitli sebeplerle aynı zarardan sorumlu olması halinde müteselsil sorumluluk söz konusudur. Bu çerçevede, müşteri dilerse zararın tazmini için yalnızca bankaya, yalnızca Risk Merkezi'ne veya dilerse

[221] Merve Arslanhan, s. 42.
[222] BIS, "Principles for Effective Risk Data Aggregation and Risk Reporting", 2013, m. 3, 5, 7, 12.

her ikisine birlikte başvurabilecektir. Sorumlular arasındaki kusur ve sorumluluk paylaşımı ise TBK m. 62 kapsamında aralarındaki rücu ilişkisince değerlendirilecektir.

Bu nedenle, müşteri uğradığı zararların tazmini için hem bankaya hem de eğer kusurlu bir katkısı mevcut ise Risk Merkezi'ne başvurabilir. Tazminatın hangi kurumdan istenebileceği hususunda, müşteri dilediğini seçmekte serbesttir. Uygulamada müşteriler öncelikle doğrudan muhatapları olan bankaya karşı dava açma eğilimindedir. Banka ile aralarında sözleşmesel bir ilişki de olduğundan, delillere erişim ve sorumluluğun ispatı daha kolay olabilir. Banka, hem sözleşmesel yükümlülüğünü ihlâl etmiş olması nedeniyle hem de TBK m. 49 uyarınca haksız fiil sorumlusu sıfatıyla, müşterinin maddi ve manevi zararlarını karşılamak durumundadır. Bunun yanında, Risk Merkezi'nin de hukuka aykırı eylemi tespit edilirse, müşteri doğrudan Risk Merkezi'ne karşı da tazminat talebinde bulunabilir. Böyle bir durumda TBK m. 61 gereği müteselsil sorumluluk söz konusu olacağından, müşteri hangisine müracaat ederse etsin, zararın tamamının tazminini isteyebilir.

Ancak müteselsil sorumluluğun uygulanabilmesi için Risk Merkezi'nin de hukuka aykırı bir fiilinin veya zarara katkısının bulunması gerekmektedir. Banka müşteri verisini kanuna aykırı biçimde paylaşmışsa, bu fiil ile müşteri sırrı zaten ihlâl edilmiş durumdadır. Eğer Risk Merkezi, bankanın hukuka aykırı elde ettiği veya ifşa ettiği veriyi kendisi de hukuka aykırı şekilde kullanmış veya yaymış ise, Risk Merkezi de müşteriye karşı doğrudan haksız fiil işlemiş sayılacaktır. Bu halde banka ile birlikte Risk Merkezi de TBK m. 61 kapsamında zararın tamamından müteselsilen sorumlu tutulabilir. Örneğin Risk Merkezi, bankanın sızdırdığı bilgiyi alıp mevzuatta izin verilmeyen bir tarafa aktarırsa, bu kendi fiili olur ve bundan sorumlu olur. Fakat Risk Merkezi, veriyi doğrudan bankadan alır ve sadece ilgili üye kuruluşlarla kanuni sınırlar dahilinde paylaşır ise bu kullanım zaten sır saklama istisnaları kapsamında ve hukuka uygun olduğundan bir sorumluluk söz konusu olmayacaktır. Özetle, müşteri sırrı önce banka eliyle ihlal edilmişse, bundan kaynaklı zararın sorumluluğu bankaya ait olacaktır. Müşterinin uğradığı zarar bankanın ifşasından doğmuş ve Risk Merkezi bu zararı artıran veya oluşturan bir fiilde bulunmamış ise, Risk Merkezi'ne sorumluluk yüklenmeyecektir.

Müşterinin zararının hangi aşamada doğduğu ise, ihlalin sonuçları ve sorumluların tespiti açısından önem taşımaktadır. Müşteri sırrının ihlâliyle doğan zarar, maddi ve manevi boyutlarıyla farklı zamanlarda tezahür edebilir. Manevi zarar, müşteri bilgisinin gizliliğinin ihlâl edilmesiyle birlikte derhal meydana gelir. Bankanın, müşteriye ait sır niteliğindeki

bilgiyi Risk Merkezi'ne izinsiz aktarması anında müşterinin özel hayatının gizliliği ve kişilik hakları zedelenmiş olur. Bu, tek başına manevi tazminat talebi için yeterlidir. Müşterinin zarar gördüğünü ispat için somut bir maddi kaybın gerçekleşmesi aranmaz. İhlalin gerçekleştiği an, manevi zarar doğmuş kabul edilir ve müşterinin banka aleyhine manevi tazminat talep etme hakkı doğar.

Maddi zarar ise genellikle biraz daha sonraki bir aşamada ortaya çıkmaktadır. Bankanın ifşa ettiği bilginin Risk Merkezi tarafından kullanılması sonucunda müşterinin maddi bir kayba uğrayıp uğramadığına bakılır. Örneğin, paylaşılan gizli bilgiler nedeniyle müşteriye kredi verilmemesi, müşterinin finansal itibarının zedelenmesi ve ticari kayıplarının söz konusu olması gibi sonuçlar doğabilir. Bu tür somut maddi zararlar, Risk Merkezi'nin veriyi finansal sisteme yayması veya üçüncü kişi kararlarında etki yaratması sebebiyle ortaya çıkar. Hangi aşamada meydana gelirse gelsin, bu maddi zararlar da başlangıçtaki ihlal ile illiyet bağı içinde değerlendirilir. Sonuç olarak bankanın veri ifşası olmasaydı müşteri bu kayıpları yaşamayacaktı, bu nedenle zarar zincirinin ilk halkası bankanın fiilidir.

Müşteri sırrının kamuya ifşasında ise ilk ifşa eden taraf tüm hukukî sonuçlara katlanır, ikinci açıklama mevcut ise artık "sır" ifşası sayılmayacağı için ek sorumluluk yaratmayacaktır. Eğer banka müşteriye ait gizli bilgileri kamuya ifşa ederse, bu fiil açıkça sır saklama yükümlülüğünün ihlalidir. Bu durumda banka, hem doğacak maddi ve manevi tazminattan hem de olası idarî ve cezaî yaptırımlardan birinci derecede sorumludur. Bu noktada Risk Merkezi hukuka aykırılığa dahil olmamışsa, hukukî sorumluluk tamamen bankaya ait olacaktır.

Bilgi halihazırda banka tarafından kamuya ifşa edilmişse, bilginin artık sır niteliği kalmamış sayılır ve daha sonra Risk Merkezi'nin aynı bilgiyi kullanması veya açıklaması, pratikte müşterinin zararını artırmaz. Zira sır zaten açığa çıkmıştır. Hatta hukuken, zaten alenileşmiş bir veriyi paylaşmak "*sır açıklama*" suçu veya haksız fiili olarak değerlendirilmeyecektir, zira ortada korunan bir sır kalmamıştır. Dolayısıyla, banka veriyi umuma açtıktan sonra Risk Merkezi'nin bu veriyi paylaşması müşteriye karşı yeni bir sorumluluk doğurmayabilir. Elbette Risk Merkezi yine de etiksel açıdan bakıldığında böyle bir durumda bilgiyi gereksiz yere dağıtmamalıdır ancak ilk ifşanın yarattığı zarar zaten oluşmuştur.

Eğer Risk Merkezi müşteriye ait bir sırrı tüm kamuya açarsa, doğrudan sır saklama yükümlülüğünü ihlal etmiş olur. Bu durumda ise öncelikli sorumluluk Risk Merkezi'ndedir. Risk Merkezi'nin umuma ifşası sonucu müşteri sırları aleniyet kazanır ve zarar gerçekleşir. Ardından bankanın aynı bilgiyi açıklaması hukuken anlamsız hale gelebilir. Zira bilgi zaten herkese mal olmuştur. Banka belki disiplin açısından veya sözleşmesel açıdan yine yükümlülüğünü ihlal etmiş sayılabilir, fakat müşterinin uğradığı ek bir zarar olmayacağı için tazmin sorumluluğu doğması tartışmalı hale gelir. Kısacası ilk açıklayan taraf zararın kaynağıdır.

Bununla birlikte, sır niteliğindeki bilginin alenileşmesi sonraki açıklamaları hukuken önemsiz kılsa da hiçbir banka veya kurum "sır nasılsa yayıldı" diyerek açıklama yapma serbestisine sahip değildir. Bankacılık mevzuatı, yetkili olmadıkça gizli bilgilerin paylaşılmaması gerektiğini vurgular. Ancak hukukî sorumluluk açısından değerlendirirsek umuma açıklama fiilini gerçekleştiren ilk fail, müşteriye karşı asıl sorumlu olandır. Daha sonra aynı bilgiyi ifşa eden diğer taraf, yeni bir zarar oluşturmadığından müşteriye karşı ek bir tazmin yükü üstlenmeyecektir.

Özetle, verinin umuma ifşasında sorumluluğun sıralaması, kimin önce ihlal ettiğine göre belirlenir. İlk ifşa eden tüm sonuçlardan sorumluyken, sonradan gelen ifşalar hukuken "sır açıklama" sayılmayabilir. Etik olan yaklaşım, bilginin alenileşmesi durumunda dahi diğer tarafın gizlilik ilkesine bağlı kalmasıdır ancak zarar ve tazminat açısından bakıldığında zararı tazmin anlamında talepler ilk ifşayı yapana yönelecektir.

VIII. RİSK MERKEZİ UYGULAMALARININ HUKUKA UYGUNLUK AÇISINDAN DEĞERLENDİRİLMESİ

Risk Merkezi'nin mevcut yapısı, öncelikle kişisel verilerin korunması ve özel hayatın gizliliği boyutunda çeşitli hukuka aykırılık iddialarına konu olmuştur. T.C. Anayasası'nın 20. maddesine 2010 yılında eklenen güvence ile kişisel verilerin ancak kanunla işlenebileceği hükme bağlanmıştır. Ancak Risk Merkezi'nin kanuni dayanağı mevcut olsa da bu dayanağın kanunda detaylı olarak düzenlenmediği ve idarî düzenlemelere geniş yetki bırakılması sebebiyle boşluk olduğu ortadadır. Nitekim AYM'nin 05/11/2024 tarihli kararında da kanunun idareye bıraktığı düzenleme alanının geniş olması eleştirilmiştir ve

Merkez'in organları, yetki sorumluluklarıyla çalışma usûl ve esaslarına dair temel çerçevenin kanunda düzenlenmemesini Anayasa'ya aykırı bulunmuştur[223].

Yargıtay'ın 31/03/2016 tarihli kararında, Risk Merkezi kapsamında gerçekleştirilen veri paylaşımı ve destek hizmeti kuruluşlarının faaliyetlerinin, uzun süre açık ve öngörülebilir bir yasal çerçeveye dayandırılmadan sürdürüldüğü tespit edilmiştir. Kararda bu durumun, hukukî güvenlik ve öngörülebilirlik ilkeleri bakımından sorunlu olduğu vurgulanmıştır. Bu tespit, Risk Merkezi'nin yapısal dayanağının açık ve net hükümlerle yasal güvenceye kavuşturulması gerektiğine işaret etmektedir. Aksi halde, Risk Merkezi'nin faaliyetleri hukuk devleti ilkesiyle bağdaşmayacak biçimde keyfi uygulamalara zemin oluşturacaktır[224].

Yargıtay içtihatlarınca, Risk Merkezi'nin veri paylaşım uygulamalarındaki hukukî belirsizliklerin ceza hukukuna da yansıdığı görülmektedir. Örneğin, yine Yargıtay'ın aynı kararında, bankaların uzun yıllardır sürdürdüğü veri paylaşım politikasının hukukî zemininin sorgulanmasıyla sanık bankacıların müşterilere ait sırları başkasına açıklama kasıtlarının bulunmadığı sonucuna varılmıştır. Mahkeme, uygulamanın idarî veya yasal düzenlemelerle netleştirilmemiş olmasının kişiler aleyhine cezaî sorumluluk doğuracak şekilde yorumlanamayacağını belirtmiştir. Bu karar Risk Merkezi ile ilgili mevzuatın muğlak kalmasının uygulayıcı olan kişileri bile suç isnadıyla karşı karşıya bırakabilecek riskler doğurduğunu ortaya koymaktadır. Dolayısıyla hukuka aykırılık sorununun bir yönünün düzenleyici netlik olduğu ortadadır ve mevcut uygulamalar net bir kanuni dayanağa kavuşturulmadıkça bireylerin mahremiyet gibi temel hakları ihlali söz konusu olacaktır.

Öte yandan KVKK ve KVKK Kurulu kararları çerçevesinde Risk Merkezi faaliyetleri sıkı bir hukukî denetime tâbi olmalıdır. KVKK kişisel verilerin işlenmesinde açık rıza, veri minimizasyonu ve amaçla sınırlılık gibi temel ilkeleri zorunlu kılmaktadır. Risk Merkezi hem veri sorumlusu hem de veri işleyen sıfatlarıyla bu ilkelere uyum sağlamakla yükümlüdür. Ancak, uygulamada birtakım ihlaller ortaya çıkmaktadır. Nitekim KVKK Kurulu'nun 03/03/2020 tarihli kararında, bazı faktöring şirketlerinin Risk Merkezi üzerinden elde ettikleri verileri amaç dışı kullandıkları ve yetkisiz üçüncü kişilerle paylaştıkları tespit edilmiş ve bu şirketler hakkında idarî para cezaları uygulanmıştır. Bu kararlar her ne kadar

[223] Bkz. AYM 05/11/2024 Tarih ve E.2021/78, K.2024/181 sayılı kararı. (www.anayasa.gov.tr E.T.: 01.08.2025)
[224] Bkz. Yargıtay 19. CD 31/03/2016 Tarih ve E.2016/20, K.2016/14268 sayılı kararı. (www.yargitay.gov.tr E.T.: 01.08.2025)

doğrudan Risk Merkezi'ni muhatap almıyor olsa da, Risk Merkezi'nin gözetim ve denetim mekanizmalarının yetersizliği sebebiyle kişisel verilerin kötüye kullanımına dolaylı olarak imkân tanıyabildiğini ve bu nedenle veri güvenliği bakımından yüksek riskler barındırdığını ortaya koymaktadır[225].

KVKK Kurulu'nun bazı kararları, Risk Merkezi aracılığı ile bankaların yapmış olduğu veri aktarımlarının ancak Bankacılık Kanunu m. 73 gibi özel düzenlemelere dayanması durumunda hukuka uygun sayılabileceğine işaret etmektedir. KVKK Kurulu'nun 31/08/2023 tarihli kararında, bankaların müşterilerine ait finansal verileri müşterinin açık rızası olmaksızın Risk Merkezi'ne aktarılmasının KVKK'nın 5/2-a maddesi gereğince "*kanunlarda öngörülen hâller*" kapsamında hukuka uygun olduğu belirtilmiştir. Ancak aynı kararda veri minimizasyonu ilkesine uyulması gerektiğini de özellikle vurgulanmıştır. Bu da yasal dayanak bulunsa dahi Risk Merkezi'ne aktarılan verilerin kapsamı ve işlenme yöntemlerinin mutlak bir serbestisinin olmadığını, Kişisel Verileri Koruma Kurumu tarafından izlendiğini ve sınırsız serbesti tanınmadığını göstermektedir[226].

Risk Merkezi yapısının hukukî sınırları ve işleyiş esasları, Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği ile bilgi paylaşımı, raporlama yükümlülükleri, üyelik koşulları ve veri güvenliği alanları belirlenmiştir. Bu yönetmeliğe göre Risk Merkezi, TBB bünyesinde faaliyet gösterse de ayrı bir organizasyonel yapı ve teknik altyapıya sahiptir. Bu çerçevede, bilgi güvenliği ve veri gizliliği yükümlülükleri doğrudan yasal çerçeveye bağlanmış durumdadır. Bu kapsamda, KVKK'nin veri sorumlusuna başvuru hakkını tanımasına karşın, Risk Merkezi gibi büyük çaplı veri işleyen kurumların yapısal olarak bu başvuruları değerlendirme kapasitesi sınırlı kalmaktadır. Veri işleme yetkisi yalnızca teknik bir yetki olarak değil, aynı zamanda hukukî ve anayasal sınırlarla çevrili bir görevdir. Anayasa'nın özel hayatın gizliliğine ilişkin hükümleri ve KKVK'nin temel ilkeleri bu süreçlerin meşruiyet zemini olarak kabul edilmektedir[227].

Bununla beraber, hukuka aykırılık unsuru Türk hukukunda yalnızca kusura dayalı bir sonuç değil özerk bir hukukî değerlendirme alanıdır. Sır niteliğindeki bilgilerin paylaşımı ancak açıkça tanımlanmış hukuka uygunluk nedenlerine dayandığı takdirde hukuka aykırı bir sonuç doğurmayacaktır. Aksi takdirde, sır saklama yükümlülüğünün ihlali başlı başına

[225] Kişisel Verileri Koruma Kurulu, 03/03/2020 Tarih ve 2020/191 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)
[226] KVKK Kurulu 31/08/2023 Tarih ve 2023/1509 sayılı kararı. (www.kvkk.gov.tr E.T.: 01.08.2025)
[227] T.C. Anayasası m. 20.

hukuka aykırılık olarak değerlendirilecek, zarar veya kusur aranmayacaktır. Bu açıdan bakıldığı takdirde, Risk Merkezi uygulamalarının sıkı bir hukuka uygunluk testinden geçmeli ve her veri işleme işleminin dayandığı gerekçesi ve verinin işlenme biçimi bakımından ayrı ayrı denetlenmesi gerekmektedir[228].

Mevcut düzenlemelerin teknik sınırlarının belirsiz ve yorumla genişletilmeye müsait oluşu hukuk devleti ilkesine aykırı bir uygulama alanı yaratmaktadır. Özellikle, BankK. 73. maddesi ve ilgili yönetmeliklerde kişisel verilerin ne kadar süreyle saklanacağı, hangi koşullarda üçüncü kişilere aktarılabileceği gibi konular açıkça nitelendirilmemiş. Bu durum veri sahipleri ve uygulayıcı kurumlar açısından gri alan oluşturarak keyfi uygulamaların doğmasına neden olabilmektedir.

Risk Merkezi'nin hukukî niteliği yalnızca iç hukukla değil, GDPR gibi uluslararası veri koruma standartlarına uyum bakımından da değerlendirilmelidir. GDPR ile KVKK arasında ciddi yapısal benzerlikler bulunmakta olup Risk Merkezi uygulamaları da bu paralellikler ışığında geliştirilmektedir. Kişisel Verileri Koruma Kurulu'nun kararlarında da görüldüğü üzere, veri sorumlularının kişisel veri işleme faaliyetlerinde açık rıza, veri minimizasyonu ve amaçla sınırlılık ilkelerine uyulması gerekmektedir. Bu ilkeler, GDPR yer alan temel veri koruma standartlarıyla örtüşmekte olup Türkiye'de uygulanan sistemin bu yönde gelişime açık olduğunu göstermektedir.

IX. RİSK MERKEZİ'NİN UYGULAMALARI VE MEVZUAT ARASINDAKİ BOŞLUK

Türkiye'de Risk Merkezi'nin veri işleme faaliyetleri hukukî temellerini Bankacılık Kanunu, Risk Merkezi Yönetmeliği ve KVKK'dan almaktadır. Ancak bu düzenlemeler, uygulamada yeknesak ve bütüncül bir veri koruma mekanizması oluşturmakta yetersiz kalmaktadır. Bankacılık düzenlemeleri, veri aktarımını teşvik eden bir sistem üzerine kuruluyken, KVKK veri işleme faaliyetlerini sınırlama ve denetim altına alma üzerine yoğunlaşmıştır. Bu birbirinden farklı yaklaşım farkı hem yorum farklılıklarına hem de Risk Merkezi'nin uygulamalarında boşluklara neden olmaktadır.

Mevzuat ve uygulama arasındaki en somut boşluk veri saklama süresi ve amaç sınırı konularındaki belirsizliktir. Risk Merkezi tarafından toplanan çeşitli verilerin ne kadar

[228] Pınar Çağla Kandıralıoğlu, s. 181.

süreyle saklanacağı, hangi amaçla işlendiği ve bu amacın meşruiyeti konularında mevzuatta açıklık bulunmamakla beraber, KVKK m. 4 ve m. 7'de düzenlenen belirli, açık ve meşru amaç ile veri silme yükümlülüklerine rağmen, Risk Merkezi verilerinin hangi süreyle tutulduğu, bu sürenin nasıl belirlendiği ve silme kararlarının nasıl denetlendiğine ilişkin net düzenlemeler bulunmamaktadır. Risk Merkezi'nin verilerinin daha sonra üçüncü kuruluşlar tarafından kredi skoru üretimi gibi amaçlarla kullanılması kişisel verilerin işlenme sınırlarının belirsizleşmesine yol açmaktadır. Bu durum, kişisel verilerin toplanma ve işlenme sebeplerine ilişkin yasal belirsizlikler doğurmaktadır[229].

5411 sayılı Bankacılık Kanunu'nun 73. maddesi, müşteri sırrı niteliğindeki bilgilerin üçüncü kişilerle ancak açık rıza ya da kanuni zorunlulukla paylaşılabileceğini belirtmektedir. Ancak, bu aktarımların kapsamı, süresi ve geri alınabilirliği açıkça belirtilmemiştir. Uygulamada da Risk Merkezi üyeleri bu verileri paylaşırken çoğu zaman açık rıza almaksızın hareket etmekte ve veri işleme faaliyetlerini kanuni yetki kapsamında saymaktadır. Bu durum, her ne kadar kanuni dayanak bulsa da KVKK'nin öngördüğü "*belirli, açık ve meşru amaçla sınırlı işleme*" ilkesine ters düşmektedir. Açık rızaya istisna tanınan bu durumda ölçülülük ve şeffaflık gözetilmediği için KVKK'nin rıza anlayışıyla örtüşmemektedir.

Benzer şekilde Risk Merkezi'nin uygulamalarında veri minimizasyonu ilkesinin ne derece uygulandığı da tartışmalıdır. KVKK m. 4/2-c gereği, kişisel verilerin işlendikleri amaçla sınırlı ve ölçülü olması gerekir. Oysa bireylerin kimlik numarası, kredi geçmişi, teminat bilgileri, çek senet hareketleri gibi detaylı veriler hem bankalar hem de Risk Merkezi tarafından tutulmakta ve aktarımlar bu detaylar üzerinden yapılmaktadır. Veri minimizasyonu ilkesine göre gerekli olandan fazla müşteri verisinin toplanmaması gerekirken Risk Merkezi bireyin tüm finansal verilerini tek elde toplamaktadır. Bu durum, yalnızca kredi değerlendirmesi değil, bireyin ekonomik hayatına ilişkin neredeyse tüm verilerinin merkezî bir havuzda toplanmasına ve potansiyel kötüye kullanıma açık hâle gelmesine yol açmaktadır.

Buna ek olarak, veri sahiplerinin bilgilendirilme ve itiraz hakkının kullanılamaması da önemli başka bir boşluktur. KVKK 11. maddesi uyarınca bireyler, kişisel verilerinin hangi kapsamda işlendiğini öğrenme, yanlış veya eksik verilerin düzeltilmesini veya silinmesini

[229] Merve Arslanhan, s. 37.

talep edebilirler. Fakat Risk Merkezi'nin uygulamasında bu hakların kullanımına yönelik mekanizmalar oldukça sınırlı kalmaktadır. Örneğin, kredi başvurusu reddedilen bireylerin, hangi risk kriterleri nedeniyle olumsuz karara maruz kaldıklarını öğrenmeleri neredeyse mümkün olmamaktadır. Oysa şeffaflık ilkesi yalnızca veriye erişim ile sınırlı olmayıp, veri işleme sürecinin mantığına, sonuçlarına ve karar yapısına ilişkin bilgilendirmeyi de kapsar. Bu noktada GDPR kapsamında otomatik karar alma süreçlerine maruz kalan bireylere bu karara itiraz etme hakkı tanınmaktadır. Ancak Türkiye'de henüz itiraz hakkı etkin olarak uygulamada yer bulamamaktadır. Bu durum Risk Merkezi'nin şeffaflık ve hesap verebilirlik ilkeleriyle bağdaşmamaktadır.

Risk Merkezi gerçek kişilerin yanında şirketlere ait kredi risk bilgilerini de bünyesinde barındırmaktadır. Her ne kadar KVKK hükümleri tüzel kişilere uygulanmasa da tüzel müşterilerin finansal verileri de BankK. m. 73 kapsamında sır niteliği taşımaktadır. Bununla beraber, Risk Merkezi uygulamalarında tüzel kişilere yönelik veriler bakımından KVKK'ya benzer bir denetim ve hak mekanizması bulunmamaktadır. Bu veriler bankacılık sırları kapsamında korunmakla beraber, tüzel kişilerin de kendi verilerine erişim ve hatalı verilerin düzeltilmesi noktasında çeşitli sorunlarla karşılaşmaları muhtemeldir. Bu durum uygulamada hakların kullanımını zorlaştıran ve hukukî korumada boşluk oluşturan bir eksiklik olarak değerlendirilebilir.

Veri güvenliğine ilişkin de mevzuat ve uygulama farkı mevcuttur. KVKK m. 12, veri sorumlusunun kişisel verilerin güvenliğini sağlamak için gerekli her türlü idarî ve teknik tedbiri almakla yükümlü olduğunu ifade etmektedir. Ancak Risk Merkezi'nin sunduğu altyapının, üyeler tarafından sağlanan verilerin doğruluğunu teyit etmeye yönelik bir kontrol mekanizması içermemesi ve BDDK veya KVKK tarafından düzenli bir dış denetim yapılıp yapılmadığına dair kamuya açık verilerin mevcutta bulunmaması, sistemin güvenilirliğini zedelemektedir. Bankanın Merkez'e yanlış veri bildirmesi durumunda, bu hatanın fark edilmesi veya düzeltilmesi büyük ölçüde ilgili bankanın inisiyatifinde olmaktadır. Risk Merkezi'nin pasif rolü mevzuatın öngördüğü veri sorumluluğu kavramının zayıflamasına neden olmaktadır.

Son olarak, düzenleyici kurumlar arası koordinasyon eksikliği uygulamadaki boşlukları derinleştirmektedir. Risk Merkezi'nin çalışma usûl ve esasları belirlenirken yalnızca BDDK'nın değil, KVKK, TCMB ve hatta Rekabet Kurumu gibi ilgili kurumların görüşlerinin alınması gerekmektedir. Nitekim Danıştay İdari Dava Daireleri Kurulu'nun

04/04/2022 tarihli kararında, kişisel veri niteliğindeki sağlık verilerinin paylaşımına ilişkin düzenlemelerde KVKK'nın görüşü alınmaksızın hareket edilmesini hukuka aykırı bulmuştur. Her ne kadar karar doğrudan sağlık verilerine ilişkin olsa da ortaya koyduğu ilke kişisel verilerin işlendiği tüm alanlarda, özellikle de Risk Merkezi gibi çok fonksiyonlu yapılar bakımından geçerlidir. Bu karar, veri paylaşımıyla ilgili kritik düzenlemelerin bütüncül bir bakış açısıyla ve ilgili otoritelerin katılımıyla yapılması gerektiğini ortaya koymaktadır[230]. Risk Merkezi özelinde de gelecekteki mevzuat düzenlemelerinin KVKK, Rekabet Kurumu ve TCMB gibi kurumların katkısıyla şekillendirilmesi mevcut uyumsuzlukların giderilmesi için gerekli görülmektedir.

Uluslararası sistemlere bakıldığında risk merkezlerinin yalnızca veri toplayıcı değil, aynı zamanda düzenleyici denetime açık, hesap verebilir ve birey odaklı yapılar hâlinde tasarlandığı görülmektedir. Örneğin İsviçre ve Almanya'da benzer sistemlerde bireylerin kredi geçmişine dair verileri doğrudan çevrimiçi platformlar üzerinden doğrudan görmeleri ve yanlış kayıtları düzeltebilmeleri mümkündür[231]. Türkiye'de ise bu düzeyde bir erişim ve düzeltme hakkı sadece dolaylı yollarla işletilebilmektedir ve bu durum mevzuatın öngördüğü etkin hak kullanımını sınırlandırmaktadır.

McKinsey tarafından 2022 yılında yayımlanan "*The Future of Risk Management in Banking"* adlı raporda geleceğin bankacılığında risk yönetimi fonksiyonunun stratejik planlamayla bütünleştirileceği ve müşteri geri bildirim sistemlerinin veri merkezleriyle entegre çalışacağı belirtilmiştir[232]. Türkiye'de Risk Merkezi'nin bu yönde dönüşüm sağlaması sadece teknik olarak değil, etik ve yasal düzeyde de gelişmiş bir veri yönetim yapısı kurulması ile mümkün olacaktır.

X. RİSK MERKEZİ'NİN İŞLEYİŞİNE YÖNELİK ÇÖZÜM ÖNERİLERİ

Risk Merkezi'nin daha etkin, güvenilir ve uluslararası standartlara uyumlu hâle gelebilmesi için kapsamlı bir dönüşüme ihtiyaç vardır. Bu dönüşüm veri paylaşımı, teknolojik altyapı, yapay zekâ entegrasyonu, uluslararası iş birlikleri, düzenleyici denetim,

[230] Danıştay İdari Dava Daireleri Kurulu 04/04/2022 Tarih ve E.2021/3516 ve K.2022/1217 sayılı kararı. (www.danistay.gov.tr E.T.: 01.08.2025)
[231] Pınar Çağla Kandıralıoğlu, s. 51.
[232] McKinsey & Company, *Bankacılıkta Risk Yönetiminin Geleceği* (*The Future of Risk Management in Banking*), 2022, s. 25. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.pdf (E.T.: 01.08.2025)

çalışan eğitimi ve kurumsal sorumluluk rejimi gibi alanlarda eş zamanlı adımlar atılmasını zorunlu kılmaktadır.

Mevcut sistem ağırlıklı olarak kredi risk bilgilerini toplamaya ve paylaşmaya odaklanmıştır. Ancak etkin bir risk yönetimi için finansal sistemdeki tüm risk türlerine dair veri akışının sağlanması gerekmektedir. Risk Merkezi'nin kapsamı piyasa riski, operasyonel riski, likidite riski ve günümüzde önem kazanan iklim riski alanlarını içerecek şekilde genişletilmelidir. Avrupa Birliği'nde bankacılık sektörü sadece kredi riski değil, aynı zamanda operasyonel ve sistemik risk verilerini de izlemekle yükümlüdür. Benzer olarak Almanya, Fransa gibi ülkelerdeki kredi bilgi merkezleri telekomünikasyon, enerji, sigorta gibi sektörlerden gelen ödeme verilerini de sisteme entegre ederek daha kapsamlı kredi skorları oluşturulması sağlanmaktadır. Türkiye'de de yasal çerçeve mümkün kıldığı ölçüde bankacılık dışı finansal veriler, hatta fatura ödemeleri gibi veriler de sisteme dâhil edilmelidir. Bu sayede daha bütüncül bir risk yönetimi sağlanabilecektir.

Ancak veri paylaşımının kapsamının genişletilmesi mahremiyetin korunması ve rekabetin bozulması gibi hassas dengeler gözetilerek gerçekleştirilmelidir. Nitekim bu tür geniş veri paylaşımı girişimlerinde Rekabet Kurumu'nun farklı sektörlerde vermiş olduğu kararlarda da vurguladığı üzere, tüm paydaşlar arasında adil erişim hakkının korunması ve rekabet koşullarının zedelenmemesi gerekmektedir[233]. Bu nedenle Risk Merkezi verileri anonimleştirilerek paylaşmalı, bireysel verileri ancak yasal zorunluluk kapsamında aktarıldığından emin olmalıdır. Türkiye Ödeme ve Elektronik Para Kuruluşları Birliği'nin geliştirmiş olduğu Veri Transfer Sistemi projesine Rekabet Kurulunca onay verilirken verilerin üye bazında erişime kapalı olması şartı vurgulanmıştır[234]. Risk Merkezi de benzer olarak bankacılık prensipleri çerçevesinde güvenli veri paylaşım altyapıları kurarak finansal gelişimi desteklemeli ve verilerin yalnızca gerekli durumlarda gerekli ölçüde paylaşılmasını sağlamalıdır.

Bununla beraber Risk Merkezi'nin kullanıcı arayüzleri ve raporlama formatlarının da güncellenmesi gerekmektedir. Günümüzde bireyler kendi risk raporlarına yalnızca belirli aralıklarla ve sınırlı olarak erişebilmektedir. Mevcut sistemde bireylerin veri işleme faaliyetlerine yönelik bilgilendirme, erişim ve düzeltme hakları oldukça sınırlı düzeydedir.

[233] Rekabet Kurulu 27/09/2017 Tarih ve 17-30/500-219 sayılı kararı. (www.rekabet.gov.tr E.T.: 01.08.2025)
[234] Rekabet Kurulu 20/10/2022 Tarih ve 22-53/806-332 sayılı kararı. (www.rekabet.gov.tr E.T.: 01.08.2025)

GDPR m. 15'e benzer şekilde, bireylere yalnızca veriye ulaşma değil, aynı zamanda kredi puanı oluşturma yöntemlerine itiraz etme ve mevcut sistem hakkında bilgi edinme hakları da tanınmalıdır. Risk Merkezi tıpkı uluslararası kredi bürolarının sunduğu gibi, güncel kredi skorları ve karşılaştırmalı risk analizleri gibi göstergeleri devreye sokmalıdır. Bu sayede Risk Merkezi verilerini doğru, esnek ve kapsamlı olarak sunabilecektir.

Kişisel veri işleme faaliyetlerinde veri sorumluluğu ve sorumluluk paylaşımı açık biçimde yeniden tanımlanmalıdır. Uygulamada, bankalardan Risk Merkezi'ne aktarılan müşteri verilerinde bir ihlal meydana geldiğinde, bireylerin doğrudan hangi kurumu muhatap alacağına dair ciddi bir belirsizlik söz konusudur. Veri ihlali durumunda bireylerin başvuracağı kurum açıkça belirlenerek etkin başvuru yolları belirlenmelidir. Teknik ve idarî kontrollerin etkin şekilde uygulanabilmesi için veri işleyen ile veri sorumlusu arasındaki sınırın net biçimde çizilmesi ve gerekli hâllerde Risk Merkezi'nin hukuken de veri sorumlusu olarak kabul edilmesi gerekmektedir. Bu bağlamda, yalnızca bireysel başvuru yollarının açıklığa kavuşturulmasıyla beraber, kurumlar arası veri sorumluluğu rejiminin sistematik şekilde tanımlanması ve müşterek sorumluluğa ilişkin ilkelerin yönetmelik düzeyinde belirlenmesi gerekmektedir. Böylece, veri ihlallerinde başvuru kanalları netleşecek, sorumluluk alanları ayrıştırılacak ve Risk Merkezi'nin kurumsal şeffaflığının artırılması mümkün kılınacaktır.

Risk Merkezi'nin aktifliğini artırmak amacıyla yasal düzenlemeler alanında da reformlar gerekmektedir. İlk olarak Basel III standartlarına uyumu tam olarak sağlanmalıdır. Bankacılık kanunu ve ilgili düzenlemelerin Basel standartlarına paralel olarak güncellenmesi Risk Merkezi'nin kapsamı ve sorumluluklarını da genişletecektir. Örneğin, bankaların kredi kararlarını müşteriye bildirirken kararın dayandığı risk raporunun özeti ve müşterinin itiraz prosedürünün de iletilmesi zorunlu tutulabilir. Ek olarak bu bireysel itiraz ve düzeltme taleplerini hızlı değerlendirecek bir platform kurulması gerekmektedir. Bağımsız denetim ve gözetim mekanizmaları ise kurumsallaştırılmalıdır.

ECB veri asgari saklama ilkesini ön plana çıkararak, veri tutarlılığı ve sürekliliği ile gereksiz veri birikiminin önüne geçilmesini önermektedir[235]. Ancak KVKK m. 7 kapsamında verilerin işlenme amacı sona erdiğinde silinmesi gerekirken, hâlihazırdaki

[235] ECB, "AnaCredit Raporlama Kılavuzu– Bölüm I: Genel Metodoloji (AnaCredit Reporting Manual– Part I)", 2019, s. 101. https://www.ecb.europa.eu/pub/pdf/other/AnaCredit_Manual_Part_I_General_Methodology_201905~e4b471a87e.en.pdf (E.T.: 01.08.2025)

sistemde bu süreler net ve kamuya açık değildir. Almanya'daki SCHUFA örneğinde olduğu gibi, kredi verilerinin en fazla 3 yıl tutulması yönünde süre sınırları getirilmeli ve bu verilerin süre sonunda otomatik olarak silinmesi güvence altına alınmalıdır.

Öte yandan Risk Merkezi'nin mevcut teknolojik altyapısı uluslararası standartlarla kıyaslandığında oldukça yetersiz ve durağan kalmaktadır. Equifax, TransUnion gibi uluslararası alanda önde gelen kredi bilgi kuruluşları, bireylerin kredi geçmişine dair oldukça zengin verileri aktif olarak işleyebilmekte ve sunabilmektedir. Buna karşılık Türkiye'deki sistemde veriler çoğunlukla geriye dönük ve sınırlı bir şekilde sunulmaktadır. Öngörüye dayalı analiz ise mevcut sistemde yeterince yer bulamamaktadır. Bu eksiklikler Risk Merkezi'ni kayıt tutucu rolüyle sınırlandırarak risk yönetiminin proaktif yapıya dönüşmesini engellemektedir. Oysa risk yönetimi, verinin yalnızca depolanmasını değil anlık olarak değerlendirilmesini ve öngörüler üretmesini gerektirmektedir.

Risk Merkezi'nin teknolojik altyapının yenilenmesi ve yapay zekâ uygulamalarının sisteme entegre edilmesi gerekmektedir. Örneğin, bankaların finansal dolandırıcılığı önlemek için kullandığı yapay zekâ destekli algoritma sistemleri, Risk Merkezi'nce kredi risk sinyallerini erken tespit etmek amacıyla kullanılabilir. Benzer olarak kredi borçlusunun temerrüde düşme ihtimalini önceden tahmin edebilen erken uyarı sistemleri geliştirilebilir ve bu sayede önleyici tedbirler alınmasına destek sunulabilir. Ek olarak, Risk Merkezi'nin veri havuzunun büyüklüğü göz önünde bulundurulduğunda, veriden değer üretmek amacıyla Büyük Veri (Big Data) analitiği ve raporlama araçları devreye sokulmalıdır. Düzenleyici teknolojiler (Regulatory Technologies– RegTech) olarak adlandırılan düzenleyici teknolojiler de Risk Merkezi, BDDK ve KVKK ile entegre bir şekilde dijital denetim altyapısı kurarak veri işlemlerinin mevzuata uyumunu gerçek zamanlı olarak izleyebilir.

BCBS, IMF, Dünya Bankası gibi kuruluşların finansal istikrar ve risk yönetimi konularındaki programlarına aktif katılım sağlamak da Türkiye'deki Risk Merkezi'nin dünya standartlarına ulaşabilmesi için önem taşımaktadır. Örneğin, IMF'nin Finansal Sektör Değerlendirme Programı (Financial Sector Assessment Program– FSAP) kapsamında Risk Merkezi'nin yapısı ve işleyişi değerlendirilerek uzmanlardan geri bildirimler alınabilir. BCBS tarafından 2013 yılında yayımlanmış olan "*Risk Verilerinin Toplanması ve Raporlanmasına İlişkin Prensipler (Principles for Effective Risk Data Aggregation and Risk Reporting– BCBS 239)"* adlı belge uygulamaya geçirilirken karşılaşılan zorluklar hakkında deneyimler paylaşılabilir. Avrupa Bankacılık Otoritesi ve Avrupa Merkez Bankası

(European Central Bank– ECB) ile temaslar artırılabilir. Türkiye her ne kadar AB üyesi olmasa da bankacılık sisteminin önemli bir kısmı yabancı sermayeli bankalardan oluştuğundan dolayı Avrupa Bankacılık Otoritesi ve Avrupa Merkez Bankası beklentileri Türkiye'yi de etkilemektedir. Özellikle Avrupa Merkez Bankası'nın 2021 tarihli İklim Riski Rehberi ve İngiltere Merkez Bankası'nın 2021 senesinde iklim riskine yönelik uyguladığı CBES gibi girişimler yakından takip edilmelidir ve iklim riski için kullanılan sistemlerin Türkiye'de uygulanması için teşvik edici olunmalıdır.

Bu uluslararası standartlara uyum sağlanabilmesi amacıyla yasal düzenlemeler alanında da reformlar gerekmektedir. Bankacılık kanunu ve ilgili düzenlemelerin Basel standartlarına paralel olarak güncellenmesi Risk Merkezi'nin kapsamı ve sorumluluklarını da genişletecektir. Örneğin, bankaların kredi kararlarını müşteriye bildirirken kararın dayandığı risk raporunun özetini ve müşterinin itiraz prosedürünün de iletilmesi zorunlu tutulmalıdır. Tüm bu bireysel itiraz ve düzeltme taleplerini değerlendirecek bir dijital platform kurulması gerekmektedir.

Öte yandan Risk Merkezi gibi sürekli ve büyük çapta veri işleyen bir kurumun düzenli olarak denetimi sağlanmalıdır. Oysa, KVKK Kurulu şikâyet üzerine denetimlerini gerçekleştirmektedir. 2024 yılı itibarıyla BDDK'nın getirdiği sınırlı bağımsız denetim yükümlülüğü, hâlihazırda yalnızca banka sistemlerini kapsamaktadır. Bu denetim yükümlülüğünün, veriyi doğrudan işleyen Risk Merkezi'ni de kapsayacak biçimde genişletilmesi gerekmektedir. Bu sayede, teknik altyapı güvenliği, açık rızanın gerçekten özgür iradeye dayanıp dayanmadığı, bilgilendirme süreçlerinin yeterliliği ve bireylerin bu sistemlere yönelik şikâyet haklarını kullanıp kullanamadıkları gibi çok boyutlu meseleler incelenebilir. Avrupa Birliği uygulamalarında da özellikle kredi sicil kuruluşlarına yönelik veri koruma denetimleri hem kurum içi kontrol sistemleriyle hem de veri koruma otoriteleri tarafından yürütülen dış denetimlerle sağlanmaktadır[236].

Türkiye'de benzer bir yapı oluşturulması amacıyla KVKK ve BDDK iş birliğiyle, uzmanlardan oluşan bağımsız bir denetim komisyonu oluşturulması gerekmektedir. Bu komisyonun oluşturduğu raporlar ise kamuoyuna sunulmalıdır. Bu sayede Risk Merkezi'nin hesap verilebilirliği güçlendirilecek ve şeffaflığı artırılmış olacaktır. Ek olarak, Risk Merkezi'nin stratejisini, hedeflerini, yatırım planlarını ve yönetim ilkelerini ortaya koyacak

[236] Lee Andrew Bygrave, s. 169.

şekilde kapsamlı bir strateji belgesi hazırlanmalıdır. Bu sayede Merkezin stratejik dönüşümü izlenebilir. Avrupa Merkez Bankası'nın Risk Kültürü Rehberinde belirtildiği gibi, bir kurumun güvenilirliği yalnızca iç kontrolle değil, bağımsız gözlem ve şeffaf raporlamayla sağlanabilir[237].

Uluslararası uyumun diğer bir boyutu da veri paylaşımının küresel entegrasyonunda karşımıza çıkmaktadır. Küresel kredi skorlama kuruluşları ve kredi büroları ile iletişim kanalları açılarak Türkiye'den yurt dışına yapılan yatırım ve borçlanma faaliyetlerinde Risk Merkezi verilerinin etkin kullanımı sağlanabilir. Günümüzde Risk Merkezi'nin verileri format ve içerik olarak uluslararası standartlara uyum sağlamadığından Türk şirketlerinin kredi profillerinin uluslararası alanda değerlendirilmesi zorlaşmaktadır. Bu sorunu gidermek amacıyla uluslararası risk raporlama standartları ile uyum için projeler geliştirilebilir. Ek olarak, Risk Merkezi'nin uluslararası alandaki kredi kayıt bürolarıyla (Almanya'da SCHUFA veya İspanya'daki CIR) düzenleyeceği çalışmalar Risk Merkezi'nin hem teknoloji hem finansal alanda atılması gereken adımlarda yol haritası çizilmesine yardımcı olabilir.

Son olarak Risk Merkezi çalışanlarının eğitimi ve kurumsal kültür yönünden de iyileştirme gereklidir. Risk Merkezi ve üye bankaların veri işleme birimlerinde çalışan personelin KVKK, Bankacılık Kanunu ve veri etiği konularında düzenli eğitimlerle kurumsal risk kültürünün güçlendirilmesi büyük önem taşımaktadır. Avrupa Merkez Bankası, bu doğrultuda çalışanların risk farkındalığını artıran anketlerin uygulanmasını ve bu verilerin düzenli analiz edilerek yönetime sunulmasını tavsiye etmektedir[238].

XI. RİSK MERKEZİ'NİN MEVCUT UYUM DURUMU

Risk Merkezi'nin uluslararası sistemle entegrasyonunda önemli farklar bulunmaktadır. Temel farklardan biri, Risk Merkezi'nin pasif ve sınırlı bir rol oynamasıdır. Almanya'daki SCHUFA, ABD'de Equifax, Experian ve TransUnion gibi kuruluşlar, özel hukuk hükümlerine tâbi olmalarına rağmen finansal kurumlara bireylerin borçluluk bilgilerini güvenilir şekilde sunmaktadırlar. Türkiye'de ise Risk Merkezi, kamu bünyesinde olmasına rağmen aktif olmayan bir yapı konumundadır. Bu durum Türkiye'nin finansal piyasalarının uluslararası alanda rekabet gücünü olumsuz etkileyebilecek bir eksiklik olarak değerlendirilebilir.

[237] ECB, "Yönetişim ve Risk Kültürüne İlişkin Taslak Kılavuz", s. 11.
[238] ECB, "Yönetişim ve Risk Kültürüne İlişkin Taslak Kılavuz", s. 14.

Veri kapsamı ve çeşitliliği açısından da Risk Merkezi'nin mevcut uyumu yetersiz kalmaktadır. Merkez daha çok bankacılık sektörü ile sınırlı veri havuzuna sahiptir. Oysa AB ve OECD ülkelerindeki kredi sistemleri telekomünikasyon, enerji, sigorta gibi birçok sektörden veri toplayarak bireylerin ve şirketlerin ödeme alışkanlıklarına daha kapsamlı bir finansal profil sağlamaktadır. Bu sayede yurt dışındaki bir kişinin veya firmanın sadece banka kredileri değil, faturalarını ödeyip ödemediği, kira ve vergi borçları gibi ödemeleri kredi raporuna yansıtılabilmektedir.

Türkiye'deki statik sistemde hem ülke içinde finansal riskler bütüncül olarak görülememekte, hem de yurt dışına yapılacak olan yatırımlarda veya kredi ilişkilerinde bilgi eksikliğine sebep olmaktadır. Örneğin, Türkiye'de faaliyet gösteren bir firmaya kredi verecek olan yabancı bir kredi kuruluşu Risk Merkezi aracılığı ile firmanın yalnızca yerel banka ilişkilerindeki borç durumunu öğrenebilmektedir. Oysa firmanın faturaları, borçları ve diğer sektörlerdeki borç durumları gibi önemli finansal bilgileri sistemde yer almamaktadır. Bu durum Türkiye kaynaklı kredi bilgilerinin uluslararası alanda değerlendirilmesini zorlaştırmakta ve finansal şeffaflık bakımından boşluk yaratmaktadır.

Karşılaştırma yapmak gerekirse, Çin'de merkez bankası bünyesinde kurulan ulusal kredi bilgi sistemi milyonlarca kişi ve şirket hakkında birkaç yılda 560 milyonun üzerinde birey ve 11,6 milyon işletme için kredi dosyası oluşturmuş, banka kredi bilgilerine ek olarak mahkeme kayıtları, vergi borçları, elektrik, su, gaz, telefon ödemeleri gibi finansal yükümlülükleri de entegre etmeye başlamıştır[239].

Risk Merkezi'nin kısıtlı veri kapsamı yalnızca analiz boyutunda değil, kullanıcı deneyimi ve erişim kolaylığı açısından da göze çarpmaktadır. ABD'deki Equifax ve TransUnion gibi kuruluşlar bireylerin kredi geçmişlerine dair verileri detaylı olarak işleyip kullanıcı dostu arayüzlerle sunarken Türkiye'deki Merkezin verilerine erişim e-Devlet üzerinden sağlanan basit bir risk raporuyla sınırlıdır ve bu rapor işlevsel olarak yetersiz kalmaktadır. Risk Merkezi'nin veri paylaşım formatlarının ve raporlama yapısının uluslararası standartlara ne ölçüde uyumlu olduğu oldukça belirsizdir.

Teknoloji ve veri işleme kapasitesi bakımından bakılacak olursa, uluslararası alanda kredi riski izleme sistemleri son yıllarda büyük ölçüde dijital dönüşüm geçirmiştir. Buna

[239] BIS, "Risk Yönetiminde Merkez Bankalarının Rolü (The Role of Central Banks in Risk Management)", 2007, s. 2. https://www.bis.org/review/r071026g.pdf (E.T.: 01.08.2025)

karşılık Türkiye'deki Risk Merkezi hâlen statik ve geriye dönük bir veri işleme anlayışına sahiptir. Örneğin, ABD'deki kredi büroları bireylerin ödeme alışkanlıklarındaki küçük değişimleri bile anlık olarak skor güncellemelerine yansıtabilirken, Türkiye'de veriler periyodik biçimde işlenmektedir. Gerçek zamanlı uyarı sistemleri ya da öngörüye odaklı analitik altyapıların henüz gelişmemesi Risk Merkezi'nin yalnızca kayıt tutucu bir işlevde sınırlı kalmasına neden olmakta ve ileriye dönük karar destek mekanizmasına dönüşmesini engellemektedir. Oysa BIS'in 2013 yılında yayımladığı *Principles for Effective Risk Data Aggregation and Risk Reporting* adlı belgeye göre, riskle ilgili verilerin zamanlı, doğru, tutarlı, kapsamlı ve esnek olması gerekmektedir[240]. Bu eksikliğin giderilmesi için Risk Merkezi'nin teknik altyapısının modernizasyonu zorunludur. Bu bağlamda, gerçek zamanlı veri toplama ve işleme kapasitesinin yapay zekâ ile entegrasyonu finansal risklerin etkin ve hızlı tespitini sağlayarak uluslararası standartlara yaklaşılmasını sağlayacaktır.

Risk Merkezi'nin günümüzde sunduğu geleneksel raporlama dışında bir analiz sunmaması da kurumu stratejik karar destek mekanizması olmaktan uzak tutmaktadır. Oysa risk yönetiminde yapay zekâ kullanımı, kredi tahsilatından, dolandırıcılık tespitinden, stres testlerine kadar pek çok alanda bir yenilik yaratmaktadır. McKinsey tarafından 2022 yılında yayımlanan "*The Future of Risk Management in Banking*" başlıklı rapora göre, modern bankacılık sistemlerinde risk yönetiminin yalnızca mevzuata uyum sağlayan pasif bir süreçten ibaret olmaktan çıkarak, proaktif ve stratejik bir yapıya bürünmesi gerektiği belirtilmektedir. Raporda, özellikle dijital dönüşümle beraber müşteri davranışlarının anlık izlenmesi, yapay zekâ ve gelişmiş analitik sistemlere entegre çalışan veri altyapılarının kurulmasının zorunluluk hâline geldiği vurgulanmıştır. Rapora göre risk yönetimi, yalnızca kontrol ve denetim mekanizması olmaktan çıkarak kurumsal strateji geliştirmenin temel bileşeni hâline gelmektedir[241]. Türkiye Risk Merkezi'nin bu gelişimin dışında kalması, bankacılıktaki risk yönetiminin de çağın gerisinde kalmasına sebep olmaktadır.

Risk Merkezi'nin elinde bulundurduğu bilgileri nasıl işlediği konusunda kamuoyunda yeterince bilgi bulunmaması şeffaflık ve hesap verilebilirlik ilkeleri bakımından eleştirilmesine neden olmaktadır. Bireyler kendilerine ait hangi verilerin tutulduğunu ve kimlerle paylaşıldığını tam olarak bilememektedirler. Sadece kendi raporlarını sınırlı olarak e-Devlet üzerinden görüntüleyebilseler de bu raporda yanlış veya eksik bilgi tespit etmeleri

[240] BIS, *Etkili Risk Verisi Toplama ve Risk Raporlaması İlkeleri*, m. 3 ve m. 6.
[241] McKinsey & Company, *Bankacılıkta Risk Yönetiminin Geleceği*, s. 3.

hâlinde, Merkez'e doğrudan başvurabilecekleri bir yol bulunmamaktadır. Hatalı verilerin düzeltilmesi için öncelikle bankaya müracaat edilmekte, bankanın düzeltmemesi durumunda uzun ve belirsiz bir süreç olan KVKK'ya şikâyet yoluna gidilmektedir. Şeffaflık ilkesi uyarınca, Risk Merkezi kendi bünyesinde hızlı ve etkin bir itiraz ve düzeltme mekanizmasına sahip olmalıdır. Bu eksiklik Merkez'i hesap verebilirlik açısından zayıf kılmaktadır. Zira hatalı verilerin sorumluluğunu üstlenmeyen bir yapı olarak görülmesi kurumun itibarını ve kamunun güvenini sarsmaktadır.

Merkez'de işlenen veriler bireylerin ekonomik hayatlarını büyük ölçüde etkilemektedir. Örneğin, Merkez'deki verilerde hata varsa veya kişi hakkında güncellenmemiş bir bilgi mevcutsa kişi bankalardan kredi alamama ve ticarî itibarının zedelenmesi gibi durumlarla karşılaşabilecektir. Bu durumda Risk Merkezi'nin bireylere karşı sorumluluk üstlenmeyişi yani hataların düzeltilmesinde doğrudan rol almayışı hesap verme mekanizmasının işlemediğini ortaya koymaktadır. Hatalı verinin kaynağının ilgili banka olduğu belirtilmekte ve vatandaşın mağduriyeti hızlı bir şekilde giderilmemektedir.

Risk raporlarının çoğu vatandaş için anlaşılır olmaması ve finansal okuryazarlığı düşük kesimlerde bireylerin kendi raporlarını anlayamaması dolayısıyla itiraz haklarını kullanmayışı göz önünde bulundurulduğunda yine finansal şeffaflık eksikliği göze çarpmaktadır. Halbuki bireyler finansal geçmişlerini temiz tutmaya teşvik edilmekle beraber hatalı kayıt varsa bunu düzeltmesi için kuruma güven duymalıdır. Örneğin, geçmişte kredi ödemesinde gecikme yaşamış olan kişi, Merkez'de hâla gecikme bilgisi tutulduğu için uzun süre yeni bir krediye erişemeyebilir. Bu kişi resmi kanallar aracılığıyla derdini anlatamadığında kayıt dışı finansman yollarına başvurabilir. Bu gibi örnekler Risk Merkezi'nin pasif, hesap verebilirlikten uzak ve gelişmemiş yapısının toplumsal etkilerini ortaya koymaktadır.

Risk Merkezi'nin uluslararası standartların gerisinde kalması, Türkiye'nin AB ile kişisel veri transferi konusunda yaşanan sıkıntıların temel sebebidir. Türkiye yeterli düzeyde veri korumasını sağlamış ülkeler arasında yer almadığından, AB'deki finansal kuruluşlar tarafından Türkiye ile kişisel veri paylaşımı konusunda tereddütler yaşanabilmektedir. Avrupa Merkez Bankası ve bazı Avrupa ülkeleri otoriteleri iklim riskine dair testlerini ve veri havuzlarını paylaşırken Türkiye henüz bu ağa katılamamıştır.

Özellikle son yıllarda iklim değişikliği sebebiyle ortaya çıkan riskler, finansal sistem açısından da bir tehdit unsuru olarak öne çıkmaktadır. Bu sebeple Avrupa ve ABD başta olmak üzere pek çok ülke finansal sistemlerinin dayanıklılığını artırmak amacıyla çeşitli adımlar atmaktadır. Avrupa Birliği ülkelerinde faaliyet gösteren bankalar, EBA tarafından belirlenen çerçeveye uygun olarak sadece kredi risklerini değil, aynı zamanda operasyonel ve sistemik riskleri de izlemek ve yönetmekle yükümlüdür[242]. Belirlenen bu çerçevede bankalar ve diğer kurumlar maruz kalabilecekleri çeşitli risk türlerini değerlendirmek amacıyla testler uygulamakta ve çeşitli ekonomik senaryolar üzerinden risk durumlarını analiz etmektedir[243]. Bu analizler, özellikle iklim değişikliği gibi yeni nesil risklere karşı bankaların hassasiyetlerini tespit etmeye ve stratejiler geliştirmeye yöneliktir.

Bu doğrultuda, İngiltere Merkez Bankası'nın geliştirmiş olduğu CBES sistemi ile iklim değişikliği riskleri analiz edilmektedir. Bu sistem sayesinde bankalar, iklim değişikliği risklerine karşı nasıl bir strateji geliştirmesi gerektiği analiz etmekte ve risklerini finansal olarak azaltmaya yönelik planlamalar yapmaktadır[244]. Avrupa Merkez Bankası da 2020 yılında yayımladığı "*Guide On Climate-Related And Environmental Risks"* adlı rehberle bankaların iklim riskini finansal istikrar açısından izlemesi ve yönetmesi için kurumsal çerçeveler oluşturulmasını teşvik etmektedir[245]. Fransa ve Hollanda bankaları da düzenleyici talepler doğrultusunda iklim riskine ilişkin risk raporlama sistemlerini geliştirmiştir. Hatta bazı Fransız bankaları, iklim risklerine özel sermaye tamponları oluşturmayı gündemlerine almıştır[246]. ABD'de ise Finansal Sektörü Düzenleme Kurumu (FINRA), yapay zekâ tabanlı sistemlerle finansal dolandırıcılık, kara para aklama ve piyasa suistimalleri gibi riskleri analiz etmekte ve bu teknolojileri gözetim ve uyum süreçlerinde aktif olarak kullanmaktadır. Ancak iklim riskine yönelik doğrudan yapay zekâ temelli bir model henüz geliştirilme aşamasındadır[247].

Türkiye'de ise iklim riskinin finansal sistem üzerindeki etkileri ve yönetimi konusunda henüz kapsamlı bir düzenleyici çerçeve ve entegre risk yönetimi modelleri tam anlamıyla

[242] NGFS, "Eylem Çağrısı: Finansal Risk Kaynağı Olarak İklim Değişikliği", s. 1.
[243] İngiltere Merkez Bankası, "2021 İki Yıllık İklim Senaryosu (CBES) Sonuçları".
[244] İngiltere Merkez Bankası, "2021 İklim İki Yıllık Araştırma Senaryosu Sonuçları (Results of the 2021 Climate Biennial Exploratory Scenario)", 2022. https://www.bankofengland.co.uk/stress-testing/2022/results-of-the-2021-climate-biennial-exploratory-scenario (E.T.: 01.08.2025)
[245] ECB, " İklimle İlgili ve Çevresel Risklere İlişkin Rehber", s. 3.
[246] NGFS, "Eylem Çağrısı: Finansal Risk Kaynağı Olarak İklim Değişikliği", s. 25.
[247] FINRA, "Menkul Kıymetler Sektöründe Yapay Zekâ (Artificial Intelligence in the Securities Industry)", 2020, s. 9. https://www.finra.org/rules-guidance/key-topics/fintech/report-artificial-intelligence-financial-services-industry (E.T.: 01.08.2025)

uygulanmamaktadır. TCMB ve BDDK, iklim riskine dair politika geliştirme aşamasındadır. TCMB'nin 2023 Finansal İstikrar Raporu'nda iklim değişikliğinin finansal sisteme etkilerine dair çalışmalar yürütüldüğü belirtilmiş, fiziksel ve geçiş risklerinin sektörel düzeyde incelendiği ifade edilmiştir. Ayrıca TCMB üyesi olduğu NGFS bünyesinde yürütülen çalışmalara katılım sağlayarak merkez bankalarının iklim politikalarındaki rolünü değerlendirmekte ve küresel düzeyde iklim riskini kapsayan finans politikalarının oluşturulmasına yönelik faaliyetlere dâhil olmaktadır[248].

BDDK da sürdürülebilir finansal sistemlerin kurulması yönünde çalışmalar yapmaktadır. Ancak, iklim riskinin sistematik olarak ölçülmesi, portföy analizlerinin yapılması ve bu risklerin sermaye planlamasına entegre edilmesi konularında henüz erken aşamadadır. Bu nedenle, Türkiye'de finansal kuruluşların iklim riskine yönelik kurumsal kapasitelerinin artırılması ve uluslararası standartlara uyumlu bir risk yönetim sisteminin geliştirilmesi önem arz etmektedir. Bu amaçla yapay zekâ gibi ileri teknoloji uygulamalarının iklim risklerinin ölçüm ve takibinde kullanımı mümkün kılınmalıdır. Ayrıca uluslararası finans kuruluşları ve düzenleyicilerle iş birliği yapılarak koordinasyonun güçlendirilmesi, CBES gibi standartlaştırılmış senaryo analiz modellerinin Türkiye'deki finans kurumlarında uygulanması teşvik edilmelidir. Ek olarak, iklim riskinin finansal piyasa üzerindeki etkileri konusunda farkındalık artırıcı eğitim ve bilgilendirme programlarının yaygınlaştırılması, sektör genelinde sürdürülebilir ve dirençli bir finansal ekosistemin oluşmasını sağlayacaktır[249]. Tüm bu adımlar finansal sistemin iklim risklerine karşı daha dirençli hâle gelmesi, sürdürülebilir ve dirençli bir finansal ekosistem için önem arz etmektedir[250].

Risk Merkezi'nin uluslararası finansal sistemle entegrasyonunda veri formatı ve raporlama standartları alanında da farklılıklar mevcuttur. Türkiye'deki finansal sistem ve uluslararası normlar sınırlı ölçüde örtüşmektedir. Veri işleme süreçleri, mevzuat uyumu, teknolojik altyapı ve şeffaflık gibi temel alanlarda çeşitli eksiklikler bulunmaktadır. Örneğin, ABD'de kredi kartı kullanımına ilişkin müşteri verilerinin çevrimiçi platformlar üzerinden kolayca erişilebilir olduğu ve verilerin finansal kurumlar tarafından pratik ve detaylı olarak

[248] TCMB, *Yıllık Faaliyet Raporu*, 2023, s. 50. https://www3.tcmb.gov.tr/yillikrapor/2023/pdf/TCMB-Faaliyet-Raporu-2023.pdf (E.T.: 01.08.2025)
[249] EBRD, "Finansal Aracı Kuruluşlar için İklim Riski Yönetimi", 2024, s. 1.
[250] BDDK, "2022-2025 Sürdürülebilir Bankacılık Strateji Belgesi", 2022, s. 11. https://www.bddk.org.tr/KurumHakkinda/EkGetir/18?ekId=360 (E.T.: 01.08.2025)

kullanıldığı belirtilmektedir[251]. Türkiye'de ise veri formatları ve raporlama yapısı uluslararası standartlara entegre olmamış bir yapıdadır. Bu durum Türkiye'deki kredi sistemi verilerinin yabancı yatırımcılar ve uluslararası kuruluşlar tarafından tam anlamıyla analiz edilip kullanılmasını zorlaştırmaktadır. Küresel ölçekte kredi bilgi altyapılarının gelişimi, ülkelerin finansal şeffaflığı, yatırım güvenliği ve uluslararası sermaye akışı üzerinde doğrudan bir etkiye sahiptir. Türkiye Risk Merkezi ise uluslararası alanda faaliyet gösteren kredi bilgi kuruluşlarıyla karşılaştırıldığı takdirde sınırlı bir etkiye sahip olmaktadır.

Küresel düzeyde kredi bilgi altyapılarının gelişimi, ülkelerin finansal şeffaflık, yatırım güvenliği ve uluslararası sermaye akışına entegrasyon süreçlerini doğrudan etkilemektedir. Türkiye'de faaliyet gösteren Risk Merkezi, ulusal düzeyde bankacılık sektörünün bilgi asimetrisini azaltma işlevi gösterse de uluslararası ölçekte faaliyet gösteren kredi bilgi kuruluşlarıyla karşılaştırıldığında sınırlı etkiye sahiptir. Avrupa Birliği ve OECD ülkelerinde, kredi bilgi sistemleri yalnızca bankacılık verileriyle sınırlı kalmayıp telekomünikasyon, enerji, sigorta gibi sektörlerden de veri toplayarak daha geniş tabanlı skorlama altyapıları oluşturmaktadır. OECD, kamuya ait veri sistemlerinin şeffaflık, yeniden kullanım, bireysel kontrol ve bir yazılımın başka bir yazılım veya sistemle iletişim kurmasına imkân tanıyan bir arayüz olan açık API gibi prensiplerle uyumlu olmasını önkoşul olarak belirlemektedir. Risk Merkezi sisteminin bu ilkelere ne ölçüde uyum sağladığı belirsiz olup uluslararası sistemlerle veri entegrasyonunu mümkün kılacak teknik yapıların varlığına ilişkin kamuya açık raporlar bulunmamaktadır[252].

Türkiye'deki Risk Merkezi uygulamaları, veri sahibi haklarının uluslararası sistemlerdeki karşılığına tam olarak denk değildir. GDPR kapsamında yer alan "*veri işlemeye itiraz hakkı*" gibi haklar, Türkiye'de yasal olarak tanınsa da Risk Merkezi bünyesinde henüz kurumsal düzeyde işletilmemektedir. Dolayısıyla bireyler, kendi verilerinin Risk Merkezi'nde nasıl saklandığını, ne amaçla işlendiğini ve kimlerle paylaşıldığını öğrenme konusunda doğrudan bir kanala sahip değildir. Bu eksiklik, şeffaflık ve hesap verebilirlik ilkeleri ile çelişmektedir. Bu kapsamda, Türkiye'de KVKK ve ilgili mevzuatta itiraz hakkının kapsamı netleştirilmeli ve uygulanabilirliği detaylandırılmalıdır.

---

[251] Fatma Özge Ersöyleyen, "Veri Madenciliği Yöntemleri Kullanılarak Kredi Kartı Müşterilerinin Ayrılma Analizi (Credit Cardholders Churn Analysis Using Data Mining Methods)", Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi, 2017, s. 44.

[252] OECD, *Açık Kamu Verisi Raporu: Sürdürülebilir Etki İçin Politika Olgunluğunu Geliştirme* (*Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*), 2018, s. 100. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/09/open-government-data-report_g1g94eac/9789264305847-en.pdf (E.T.: 01.08.2025)

Müşterilerin itirazlarını direkt olarak iletebilecekleri hızlı dijital başvuru sistemleri oluşturulmalıdır. İtirazlar için süreç belirlenmeli ve başvurular makul süre içinde incelenip gerekçelendirilerek veri sahibine geri dönütler verilmelidir. Ayrıca tüm bu süreci denetleyecek bağımsız denetim mekanizmaları oluşturulmalı ve mevzuata aykırılık durumunda gerekli yaptırımlar uygulanmalıdır. Şeffaflık ve hesap verilebilirliği artırmak amacıyla mevcut denetim yapısına ek olarak bağımsız dış denetim uygulamaları oluşturulmalı, bu sayede Risk Merkezi'nin karar alma ve veri işleme süreçleri hem iç hem dış uzman denetçiler tarafından düzenli olarak izlenip değerlendirilmelidir.

Avrupa Merkez Bankası tarafından geliştirilen Tek Denetim Mekanizması, bankaların ortak denetim süreçlerine tâbi tutulmasını ve tüm üye ülkelerde ortak bir risk yönetimi anlayışı oluşturulmasını teşvik etmektedir[253]. Türkiye bu mekanizmanın dışında olduğundan finansal şoklara karşı dayanıklılığı zayıf kalmaktadır ve bankacılık sektöründe uluslararası standartlara uyum sınırlı düzeyde gerçekleşmektedir. Bu durum, çok uluslu bankaların Türkiye operasyonları ile Risk Merkezi arasındaki veri akışlarını karmaşıklaştırmakta ve bilgi güvenliği açısından gri alanlar yaratmaktadır. Türkiye'nin "*yeterli veri koruması sağlayan ülke*" statüsünde olmaması nedeniyle Avrupa'dan Türkiye'ye yapılacak kişisel veri transferleri yasal olarak kısıtlı kalmaktadır[254]. Bu da uluslararası sermaye akışlarında güven sorunlarına yol açabilmektedir. Sonuç olarak, Türkiye'deki bankaların yabancı fonlama kaynaklarına erişimi zorlaştırmaktadır.

Uluslararası alanda finansal risklerin yönetiminde teknoloji kullanımına dair gelişmeler de dikkat çekicidir. Örneğin ABD'de bazı bankalar, finansal dolandırıcılığı engellemek amacıyla yapay zekâ destekli risk analiz sistemleri kullanmakta, böylece bankaların risk yönetimi süreçlerini izleyerek ve riskli işlemleri tespit ederek bankaları önlem almaya teşvik etme yoluyla riski optimize etmektedir[255]. Türkiye'deki Risk Merkezi ise henüz bu gelişmelere uyum sağlamamış olup çoğunluklu olarak geleneksel modellerle veri paylaşım sürecini işletmektedir.

[253] ECB, "Bankacılık Denetimine İlişkin Kılavuz (Guide to Banking Supervision)", Kasım 2014, m. 8 ve 9. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssmguidebankingsupervision201411.en.pdf (E.T.: 01.08.2025)

[254] Avrupa Komisyonu, "AB Dışı Ülkeler İçin Veri Koruma Yeterliliği Kararları (Data Protection Adequacy For Non-EU Countries)", 2025. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?utm_source (E.T.: 01.08.2025)

[255] McKinsey & Company, *Bankacılıkta Risk Yönetiminin Geleceği*, s. 11.

Avrupa Birliği'nin 2015/849 sayılı AML Direktifi doğrultusunda bankalar, finansal kurumlar, sigorta şirketleri gibi bazı kuruluşlar, müşteri kimliğinin doğrulanması yapmak, finansal işlemleri izlemek ve şüpheli işlem bildiriminde bulunmak gibi yükümlülüklere sahiptir. Bu yükümlülükler, suç gelirlerinin takibi ve önlenmesi açısından temel mekanizmaları oluşturur[256]. Türkiye ise hâla ağırlıklı olarak geleneksel yöntemler kullansa da Risk Merkezi tarafından toplanan ve paylaşılan veriler BDDK, MASAK ve ilgili otoriteler tarafından dolandırıcılık, kara para aklama ve şüpheli işlem tespiti gibi faaliyetlerin takibini kolaylaştırmaktadır. Bu sayede söz konusu kurumlar, ilgili risk alanlarına yönelik daha etkili denetim mekanizmaları geliştirebilmektedirler. Her ne kadar bu kullanım açıkça tanımlanmış olmasa da Risk Merkezi'nin sunduğu verilerin dolaylı olarak bir destek sunduğu görülmektedir.

Risk Merkezi'nin proaktif bir yapı kazanması ve pasif veri toplayan bir modelden çıkıp, aktif denetim ve stratejik rehberlik yapan bir modele dönüşmesi gereklidir. Bu dönüşümü sağlamak için dört temel stratejik alan mevcuttur. İlk olarak, veri paylaşım mekanizmalarının genişletilmesi gerekmektedir. Günümüzde mevcut sistem yalnızca kredi bilgilerini içerirken, diğer riskleri de örneğin piyasa riski, operasyonel risk ve likidite riski gibi ek verilerin de sisteme dâhil edilmesi gerekmektedir. İkinci olarak, teknolojik yatırımlar artırılmalı ve yapay zekâ destekli risk tahmin modelleri geliştirilmelidir. ABD ve Avrupa'daki risk yönetimi merkezlerinde kullanılan otomatik veri analizi ve dolandırıcılık tespit sistemleri, Türkiye'de de uygulanmalıdır Üçüncüsü ise, uluslararası iş birliklerinin güçlendirilmesidir. Risk Merkezi'nin IMF, Dünya Bankası, Basel Komitesi ve Avrupa Bankacılık Otoritesi gibi kuruluşlarla ortak projeler yürütmesi, küresel entegrasyonu hızlandıracaktır. Son olarak ise, düzenleyici reformların tamamlanması gerekmektedir. Türkiye'nin Basel III standartlarına tam uyum sağlaması, bankacılık sisteminin uluslararası rekabet gücünü artıracaktır.

Ek olarak, her ne kadar Risk Merkezi faaliyetleri BDDK ve TBB'nin denetimine açık olsa da kişisel verilerin korunması bakımından özel bir otorite olan Kişisel Verileri Koruma Kurumu (KVKK Kurulu) tarafından doğrudan bir denetim mekanizması işletilmelidir. Tüm bu eksikliklerin giderilmesi yalnızca birey haklarının korunması açısından değil, aynı

[256] Avrupa Parlamentosu ve Konsey, (AB) 2015/849 sayılı Direktif (4. Kara Paranın Aklanmasının Önlenmesi Direktifi – 4AMLD), OJ L 141, 5 Haziran 2015 https://eur-lex.europa.eu/eli/dir/2015/849/oj/eng (E.T.: 01.08.2025)

zamanda finansal sistemin istikrarı ve Risk Merkezi'nin meşruiyeti açısından da gereklidir. Mevzuatın işlevsel olarak da uygulanabilir hâle getirilmesi, sürdürülebilir temelli bir veri yönetimi için önemli bir koşuldur. Bu nedenle, Risk Merkezi faaliyetleri şeffaflık, ölçülülük ve denetlenebilirlik ilkeleri çerçevesinde yeniden ele alınmalıdır ve sadece yasal çerçeveyle değil, aynı zamanda kurumsal etik ve birey hakları eksenine dayalı bir yapı inşa edilmelidir.

SONUÇ

Bankacılık hukukunda müşteri sırrı kavramı, bireysel bir mahremiyet unsuru olmanın ötesinde anayasal değerler ve kamu yararı boyutlarıyla yorumlanması gereken bir kavramdır. Bankaların müşterilerinden edindikleri bilgi ve belgeler, başlangıçta sözleşmesel güven ilkesine dayalı bir yükümlülük niteliği taşısa da zaman içinde temel hakların ayrılmaz bir parçası hâline dönüşmüştür. Müşteri sırrının korunması, bireylerin malî bilgilerinin gizliliğini güvence altına alarak bankacılık sistemine duyulan güveni tesis etmeyi sağlar. Dolayısıyla, müşteri sırrının ihlali yalnızca bireysel hak kaybı doğurmakla kalmaz, aynı zamanda finansal sistemin bütünlüğü ve istikrarı açısından kamu düzenine ilişkin bir sorun olarak karşımıza çıkar.

Gelinen noktada dijitalleşme ve veriye dayalı finansal uygulamalar, müşteri sırrı kavramını yeni bir bakış açısıyla ele almayı zorunlu kılmaktadır. Kredi kayıt ve paylaşım sistemleri yaygınlaştıkça, bankaların sır saklama yükümlülüğü ile şeffaflık ihtiyacı arasında daha hassas bir denge kurulması ihtiyacı ortaya çıkmıştır. Kamu yararının gerektirdiği finansal istikrarın sağlanması ve piyasada bilgi asimetrisinin azaltılması adına belirli veri paylaşımı mekanizmalarının varlığı elzemdir.

Türkiye Bankalar Birliği bünyesinde faaliyet gösteren Risk Merkezi, müşterilere ait kredi bilgilerinin merkezi bir yapıda toplanarak finansal kuruluşlarla paylaşılması görevini üstlenen bir yapıdır. Risk Merkezi'nin temel görevi, finansal kuruluşlara kredi tahsis süreçlerinde objektif ve güncel bilgiler sunmaktır. Günümüzde ulaştığı kapsam göz önünde bulundurulduğunda, Risk Merkezi'nin veri yoğunluğu finansal istikrarın sağlanmasında önemli bir araç niteliği taşımaktadır. Bununla beraber, sahip olduğu geniş yetki ve veri akışı, etkin denetim ve gözetim mekanizmalarıyla desteklenmediği takdirde çeşitli riskleri ve denetim eksikliklerini de beraberinde getirmektedir.

Mevcut hukukî altyapıya bakıldığında, Risk Merkezi'nin veri toplama ve paylaşma yetkisi yalnızca genel ifadelerle tanımlanmaktadır ve bu yetkinin sınırlarına ve denetimine dair belirsizlikler mevcuttur. Verilerinin Risk Merkezi'ne aktarılması sürecinde bireylerin hangi verilerinin kimler tarafından ve hangi amaçla işlendiğini tam olarak bilememesi, kendi verileri üzerindeki denetim ve hak arama imkânlarını zayıflatmakta ve veri sorumluluğunun sınırlarını belirsizleştirmektedir. Dolayısıyla Bankacılık Kanunu'nda müşteri sırrının korunmasına ilişkin temel düzenlemeler mevcut olsa da, Risk Merkezi kapsamındaki veri

paylaşımının sınırları net değildir. Aynı şekilde Kişisel Verilerin Korunması Kanunu kapsamında finansal verilerin işlenmesi belirli ilkelerle sınırlandırılmış olsa da Risk Merkezi uygulamalarında bu ilkelerin ne derece gözetildiği tartışmalı bir konudur.

Türkiye'deki finans sistemi, yasal zorunluluk temelinde tek merkezli bir risk kayıt modeli öngörerek kapsamlı bir veri paylaşım mekanizması kurmuştur. Bu yönüyle, birçok AB ülkesinin merkez bankası bünyesinde tuttuğu kredi sicil kayıtlarına benzer şekilde, Türkiye'de de kamusal bir veri havuzu yaklaşımı bulunmaktadır. Ancak uygulamada şeffaflık, hesap verebilirlik, veri minimizasyonu, otomatik kararların denetimi gibi GDPR ile somutlaşan ilkelerle tam anlamıyla uyumlu olduğunu gösterememektedir.

Çalışma kapsamında elde edilen önemli diğer bir bulgu Risk Merkezi'nin şu anki hâliyle bir kayıt tutucu rolü oynadığıdır. Merkez sahip olduğu veri havuzuna rağmen, proaktif bir karar destek sistemine dönüşememektedir. Örneğin, kredi borçlularının temerrüde düşme ihtimalini önceden tahmin eden yapay zekâ destekli modeller geliştirebilir ve bu kullanımın hesap verebilirlik prensibiyle desteklenmesi sağlanabilir. Bu eksiklik, teknolojik kapasite anlamında büyük bir potansiyelin kullanılmadığını ortaya koymaktadır.

Bununla beraber, Risk Merkezi teknoloji ve veri çeşitliliği bakımından büyüme potansiyeline sahiptir. Ancak bu potansiyelin hayata geçirilmesinde merkeze alınması gerekli unsur veri güvenliği ve kişisel hakların korunması olmalıdır. Teknolojik kapasite arttıkça, beraberinde getirilecek olan denetim ve şeffaflık mekanizmaları da güçlendirilmelidir ki sistem hem etkin hem de adil bir faaliyet gösterebilsin.

Risk Merkezi'nin gerek birey haklarıyla uyumlu gerekse denetlenebilir ve hesap verebilir bir yapıya kavuşması için kısa, orta ve uzun vadeli çeşitli reform adımlarına ihtiyaç duyduğu açıktır. Bu adımların başında, mevcut hukukî çerçevenin netleştirilmesi ve uygulamadaki boşlukların giderilmesi gelmektedir. Kısa vadede atılabilecek en somut adımlardan biri, mevzuatın daha ayrıntılı hâle getirilmesidir. Bankacılık Kanunu ve ilgili yönetmeliklerde, müşteri verilerinin Risk Merkezi'ne aktarım koşulları, saklama süreleri, paylaşım sınırları ve ihlal durumunda uygulanacak yaptırımlar ayrıntılı ve kesin hükümlerle düzenlenmelidir. Mevzuatın bu şekilde netliğe kavuşturulması, Risk Merkezi'ne veri bildiriminde bulunan kuruluşların sorumluluk alanlarını da belirginleştirecek ve olası hukukî ihtilafların önüne geçecektir.

Hukukî altyapının güçlendirilmesine yönelik bu adımlar, yönetmelik değişiklikleri veya BDDK ile KVKK tarafından yayımlanacak rehberler vasıtasıyla kısa vadede hayata geçirilebilir. Böylelikle açık rıza, uygulamada bireyin veri üzerindeki söz hakkını gerçek anlamda yansıtan etkin bir unsur hâline gelecektir. Orta vadede ise denetim ve şeffaflık mekanizmalarının tesisi öncelik taşımalıdır. Bu kapsamda, Risk Merkezi nezdinde dijital bir itiraz ve düzeltme platformu kurulması önerilmektedir. Merkezi bir itiraz mekanizması, hem şikâyetlerin sistematik izlenmesine imkân verecek hem de her bankanın ayrı ayrı prosedürleriyle uğraşma zorunluluğunu ortadan kaldıracaktır. Kişisel Verileri Koruma Kurumu ve BDDK iş birliğiyle böyle bir altyapının kurulması önemli yapısal bir eksikliği giderecek ve Risk Merkezi'nin hesap verebilirlik düzeyini artıracaktır. Uzun vadede ise, Risk Merkezi'nin küresel finansal sistemle entegrasyonu hedeflenmelidir. Türk finansal kurumlarının yurt dışı kredi ilişkilerinde ve yatırımlarında, Risk Merkezi verilerinin uluslararası geçerliliği önemli hâle gelecektir. Bu kapsamda GDPR ile uyumlu veri işleme prensiplerinin tam olarak benimsenmesi ve uluslararası uyumun sağlanması Merkez'in itibarını küresel düzeyde destekleyecektir.

KAYNAKLAR

Acharya, Viral, Douglas Gale ve Tanju Yorulmazer, "*Yenileme Riski ve Piyasa Donmaları* (Rollover Risk and Market Freezes)", *The Journal of Finance*, Cilt 66, Sayı 4, 2011, s. 1177-1209.

Akçalı Gür, Berna, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt 25, Sayı 2, Aralık 2019, s. 850-872.

Aksoy, Hüseyin Can, *Medenî Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Ankara, Çakmak, 2010.

Alıcı, Yaşar, *Bankacılık Kanunu Şerhi*, İstanbul, On İki Levha Yayıncılık, 2. Baskı, 2017.

Alımcı, Ezgi, "Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi", *Ankara Barosu Dergisi*, Cilt 80, Sayı 1, 2021, s. 47-76.

Amerika Birleşik Devletleri Federal Ticaret Komisyonu (Federal Trade Commission– FTC), Adil Kredi Raporlama Yasası (Fair Credit Reporting Act– FCRA), 2023. https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf (E.T.: 01.08.2025)

Amerika Birleşik Devletleri Kanunu (United States Code), Finansal Mahremiyet Hakkı Yasası (Right to Financial Privacy Act), 12 U.S.C. § 3409, 1978. https://www.govinfo.gov/content/pkg/USCODE-2021-title12/html/USCODE-2021-title12-chap35.htm (E.T.: 01.08.2025)

APEC, "APEC Gizlilik Çerçevesi (APEC Privacy Framework)", APEC, 2005. https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1 (E.T.: 01.08.2025)

APEC, "Sınır Ötesi Gizlilik Kuralları (CBPR) Sistemi: Politikalar, Kurallar ve Rehberler (Cross-Border Privacy Rules (CBPR) System: Policies, Rules and Guidelines)", 2019. https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf (E.T.: 01.08.2025)

Arslanhan, Merve, "Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması", *Kişisel Verileri Koruma Dergisi*, Cilt 6, Sayı 2, 2024, s. 33-53.

Avrupa Birliği Adalet Divanı (Court of Justice of the European Union– CJEU), Google v. CNIL, C-507/17, 2019. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17 (E.T.: 01.08.2025)

Avrupa Birliği Adalet Divanı (Court of Justice of the European Union– CJEU), Veri Koruma Hukuku Bağlamında Karar (Judgment on Data Protection Law), C-319/22, 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=EN (E.T.: 01.08.2025)

Avrupa İnsan Hakları Mahkemesi (AİHM), S. ve Marper v. Birleşik Krallık, Başvuru No. 30562/04 ve 30566/04, 04.12.2008. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]} (E.T.: 01.08.2025)

Avrupa Komisyonu, AB Dışı Ülkeler İçin Veri Koruma Yeterliliği Kararları (Data Protection Adequacy For Non-EU Countries), 2025. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?utm_source (E.T.: 01.08.2025)

Avrupa Konseyi (Council of Europe), Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunmasına İlişkin Sözleşme (Sözleşme 108) (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data– Convention 108), 1981. https://rm.coe.int/1680078b37 (E.T.: 01.08.2025)

Avrupa Konseyi, "Kişisel Verilerin Otomatik İşlenmesine İlişkin Sözleşmeyi Değiştiren Protokol (Sözleşme 108+) (Protocol Amending the Convention for the Protection of

Individuals with Regard to Automatic Processing of Personal Data)", CETS No. 223, 2018, s. 6. https://rm.coe.int/16808ac918 (E.T.: 01.08.2025)

Avrupa Parlamentosu ve Konsey, (AB) 2015/849 sayılı Direktif (4. Kara Paranın Aklanmasının Önlenmesi Direktifi – 4AMLD), OJ L 141, 5 Haziran 2015 https://eur-lex.europa.eu/eli/dir/2015/849/oj/eng (E.T.: 01.08.2025)

Avrupa Parlamentosu ve Konsey, Gerçek Kişilerin Kişisel Verilerinin İşlenmesine ve Bu Verilerin Serbest Dolaşımına İlişkin Koruma Hakkında Avrupa Parlamentosu ve Konsey Tüzüğü (AB) 2016/679 (Genel Veri Koruma Tüzüğü– GDPR), 27 Nisan 2016, Avrupa Birliği Resmî Gazetesi, L119, 4 Mayıs 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (E.T.: 01.08.2025)

Avrupa Veri Koruma Kurulu (European Data Protection Board - EDPB), "Romanya Denetim Kurumu Tarafından Verilen İlk Para Cezası (First Fine By The Romanian Supervisory Authority)", 2019. https://www.edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_en (E.T.: 01.08.2025)

Başel, Burak, *Banka Sırrının Açıklanması Suçu (BankK. m. 159)*, Ankara, Seçkin Yayıncılık, 2021.

BCBS, "Kredi Riskinin Yönetimine İlişkin Prensipler (Principles for the Management of Credit Risk)", BIS, 2000. https://www.bis.org/publ/bcbs75.pdf (E.T.: 01.08.2025)

BCBS, "Basel III: Likidite Riski Ölçümü, Standartları ve İzlenmesine İlişkin Uluslararası Çerçeve (Basel III: International Framework for Liquidity Risk Measurement, Standards and Monitoring)", BIS, 2010. https://www.bis.org/publ/bcbs188.pdf (E.T.: 01.08.2025)

BCBS, "Basel III: Likidite Karşılama Oranı ve Likidite Riski İzleme Araçları (Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools)", BIS, 2013. https://www.bis.org/publ/bcbs238.pdf (E.T.: 01.08.2025)

BCBS, *Etkili Risk Verisi Toplama ve Risk Raporlaması İlkeleri (Principles for Effective Risk Data Aggregation and Risk Reporting)*, BIS, 2013. https://www.bis.org/publ/bcbs239.pdf (E.T.: 01.08.2025)

BCBS, "Piyasa Riski İçin Asgari Sermaye Gereklilikleri (Minimum Capital Requirements for Market Risk)", 2016. https://www.bis.org/bcbs/publ/d352.pdf (E.T.: 01.08.2025)

BCBS, "Bankacılık Portföyünde Faiz Oranı Riski (IRRBB) (Interest Rate Risk in the Banking Book (IRRBB))", BIS, 2016. https://www.bis.org/bcbs/publ/d368.pdf (E.T.: 01.08.2025)

BCBS, "Operasyonel Risk için Standartlaştırılmış Yaklaşım– Giriş (The Standardised Approach for Operational Risk– Introduction)", BIS, 2017. https://www.bis.org/basel_framework/chapter/OPE/25.htm (E.T.: 01.08.2025)

BCBS, "MAR31– İçsel Model Yaklaşımı: Model Gereklilikleri (MAR31– Internal Models Approach: Model Requirements)", BIS, 2023. https://www.bis.org/basel_framework/chapter/MAR/31.htm (E.T.: 01.08.2025)

BDDK, Bankaların Özkaynaklarına İlişkin Yönetmelik, Resmî Gazete, Sayı 28756, 5 Eylül 2013. https://www.lexpera.com.tr/resmi-gazete/metin/bankalarin-ozkaynaklarina-iliskin-yonetmelik-28756-1 (E.T.: 01.08.2025)

BDDK, Likidite Karşılama Oranı Hakkında Tebliğ, Resmî Gazete, Sayı: 29294, 21 Mart 2014. . https://resmigazete.gov.tr/eskiler/2014/03/20140321-7.htm (E.T.: 01.08.2025)

BDDK, Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, 2014. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19864&MevzuatTur=7&MevzuatTertip=5. (E.T.: 01.08.2025)

BDDK, Faiz Oranı Riski Yönetimi Rehberi, 2016. https://www.bddk.org.tr/Mevzuat/DokumanGetir/957 (E.T.: 01.08.2025)

BDDK, Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik, 4 Haziran 2021. https://www.resmigazete.gov.tr/eskiler/2021/06/20210604-6.htm (E.T.: 01.08.2025)

BDDK, Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik, 2022. https://www.bddk.org.tr/Mevzuat/DokumanGetir/1290 (E.T.: 01.08.2025)

BDDK, Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Uygulama Tebliği, Resmî Gazete, Sayı 32044, 25.03.2022. https://www.mevzuat.gov.tr/mevzuat?mevzuatno=39442&mevzuattur=9&mevzuattertip=5 (E.T.: 01.08.2025)

BDDK, "2022-2025 Sürdürülebilir Bankacılık Strateji Belgesi", 2022. https://www.bddk.org.tr/KurumHakkinda/EkGetir/18?ekId=360 (E.T.: 01.08.2025)

Bernstein, Peter L., *Tanrılara Karşı: Riskin Olağanüstü Tarihi (Against the Gods: The Remarkable Story of Risk)*, New York, Wiley, 1996.

Bessis, Joël, *Bankacılıkta Risk Yönetimi* (*Risk Management in Banking)*, Hoboken, Wiley, 3. Baskı, 2010.

Bilge, Mehmet Emin, *Ticarî Sırrın Korunması,* Ankara, Seçkin Yayıncılık, 2. Baskı, 2005.

BIS, Sermaye Ölçümünün ve Standartlarının Uluslararası Uyumlaştırılması: Gözden Geçirilmiş Çerçeve (International Convergence of Capital Measurement and Capital Standards: A Revised Framework), 2004. https://www.bis.org/publ/bcbs107.pdf (E.T.: 01.08.2025)

BIS, Risk Yönetiminde Merkez Bankalarının Rolü (The Role of Central Banks in Risk Management), 2007. https://www.bis.org/review/r071026g.pdf (E.T.: 01.08.2025)

BIS, *Yeşil Kuğu: İklim Değişikliği Çağında Merkez Bankacılığı ve Finansal İstikrar* (*The Green Swan: Central Banking and Financial Stability in the Age of Climate Change*), 2020. https://www.bis.org/publ/othp31.pdf (E.T.: 01.08.2025)

BM, İnsan Hakları Evrensel Beyannamesi (Universal Declaration of Human Rights), 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights (E.T.: 01.08.2025)

BM, Medenî ve Siyasal Haklara İlişkin Uluslararası Sözleşme (International Covenant on Civil and Political Rights (ICCPR)), 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (E.T.: 01.08.2025)

Bygrave, Lee Andrew, *Uluslararası Perspektifle Veri Koruma Hukuku* (*Data Privacy Law: An International Perspective),* Oxford, Oxford University Press, 2014.

Candoğan, Mehmet Ali, "Ticarî Bankalarda İtibar Riski Yönetimi ve İtibar Riski Hesaplama Model Önerisi: Borsa İstanbul Bankacılık Endeksinde Ampirik Bir Uygulama", Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2023.

Cicoğlu, Şükrü ve Celal Gökhan Çil, "Türkiye'de Uygulanan Basel Kriterleri ve Basel III Kriterlerinin Türk Finans Sistemine Etkileri", *Politik Ekonomik Kuram*, *Cilt 3, Sayı 1,* 2019, s. 83-104.

Coelho, Rodrigo ve Jermy Prenio, "Covid-19 ve Operasyonel Dayanıklılık: Pandemi Sürecinde Finansal Kurumların Operasyonel Zorluklarının Ele Alınması *(*Covid-19 and Operational Resilience: Addressing Financial Institutions Operational Challenges in a Pandemic)", FSI Briefs No. 2, BIS, 2020. https://www.bis.org/fsi/fsibriefs2.pdf (E.T.: 01.08.2025)

Çiftçioğlu, Cengiz T., *Ticarî Sır, Bankacılık Sırrı veya Müşteri Sırrının Açıklanması Suçu.* Ankara, Seçkin Yayıncılık, 2017.

Dellinger, Andrew James, "533 Milyon Facebook Kullanıcısının Kişisel Verisi Çevrimiçi Sızdırıldı (Personal Data of 533 Million Facebook Users Leaks Online)", Forbes, 2021. https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/ (E.T.: 01.08.2025)

Donay, Süheyl, *Meslek Sırrının Açıklanması Suçu*, İÜHF Yayınları, 1978.

Dünya Fikri Mülkiyet Teşkilatı (WIPO), "Ticarî Sırlar (Trade Secrets)". https://www.wipo.int/en/web/trade-secrets (E.T.: 01.08.2025)

Dünya Fikri Mülkiyet Teşkilatı (WIPO), "Ticarî *Sırların Korunması: Uluslararası ve Ulusal Yaklaşımlara Genel Bakış* (Protection of Trade Secrets: An Overview of International and National Approaches)", 2020. https://www.wipo.int/publications/en/details.jsp?id=4528 (E.T.: 01.08.2025)

Eamon, William, *Bilim ve Doğanın Gizleri: Ortaçağ ve Erken Modern Kültürde Sır Kitapları (Science and the Secrets of Nature: Books of Secrets in Medieval and Early Modern Culture)*, Princeton, Princeton University Press, 1994.

EBA, "Bilgi ve İletişim Teknolojileri ile Güvenlik Risklerinin Yönetimine İlişkin Rehber (Guidelines on ICT and Security Risk Management)", 2020. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf (E.T.: 01.08.2025)

EBRD, "Finansal Aracı Kuruluşlar için İklim Riski Yönetimi (Climate Risk Management for Financial Intermediaries)", 2024.

ECB, "Bankacılık Denetimine İlişkin Kılavuz (Guide to Banking Supervision)", Kasım 2014. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssmguidebankingsupervision201411.en.pdf (E.T.: 01.08.2025)

ECB, "AnaCredit Raporlama Kılavuzu– Bölüm I: Genel Metodoloji (AnaCredit Reporting Manual– Part I)", 2019. https://www.ecb.europa.eu/pub/pdf/other/AnaCredit_Manual_Part_I_General_Methodology_201905~e4b471a87e.en.pdf (E.T.: 01.08.2025)

ECB, "İklimle İlgili ve Çevresel Risklere İlişkin Rehber (Guide on Climate-Related and Environmental Risks)", 2020. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf (E.T.: 01.08.2025)

ECB, "Yönetişim ve Risk Kültürüne İlişkin Taslak Kılavuz (Draft Guide on Governance and Risk Culture)", 2024. https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon202407_draftguide.en.pdf (E.T.: 01.08.2025)

ECB, "2022 Euro Sisteminin Bilançosuna Yönelik İklim Riski Stres Testi Sonuçları (Results of the 2022 Climate Risk Stress Test of the Eurosystem Balance Sheet)", 2023. https://www.ecb.europa.eu/press/economic-bulletin/focus/2023/html/ecb.ebbox202302_06~0e721fa2e8.en.html (E.T.: 01.08.2025)

EDPB, "CNIL Kısıtlı Komitesi, Google LLC'ye 50 Milyon Avro Para Cezası Uyguladı" (CNIL's Restricted Committee Imposes Financial Penalty of 50 Million Euros Against Google LLC), 2019. https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (E.T.: 01.08.2025)

EDPB, "Hamburg Veri Koruma Komiseri, H&M'e 35,3 Milyon Avro Para Cezası Verdi (Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations)", 2020. https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en (E.T.: 01.08.2025)

EDPB, "Erişim Hakkına İlişkin Rehber 01/2022" (Guidelines 01/2022 on Right of Access), 2022. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (E.T.: 01.08.2025)

Eiteman, David, Arthur Stonehill ve Michael Moffett, *Çok Uluslu İşletme Finansmanı* (*Multinational Business Finance)*, Pearson, 15. Baskı, 2021.

Erem, Faruk, Akın Altınok ve Haluk Tandoğan, *Bankalar Kanunu Şerhi*, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, 1989.

Erem, Faruk, *Ceza Hukuk Genel Hükümler,* Ankara, Sevinç Matbaası, 1997.

Eren, Fikret, *Borçlar Hukuku Genel Hükümler,* Ankara, Yetkin Yayınları, 24. Baskı, 2022.

Eren, Fikret ve İpek Yücer, *Borçlar Hukuku Özel Hükümler,* Ankara, Legem Yayınevi, 12. Baskı, 2024.

Ersöyleyen, Fatma Özge, "Veri Madenciliği Yöntemleri Kullanılarak Kredi Kartı Müşterilerinin Ayrılma Analizi (Credit Cardholders Churn Analysis Using Data Mining Methods)", Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi, 2017.

Eulerich, Marc, "Kurumsal Yönetişimin Yapılandırılması İçin Yeni Üç Hat Modeli (The New Three Lines Model for Structuring Corporate Governance)", *SSRN Elektronik Dergisi (SSRN Electronic Journal)*, 2021. https://doi.org/10.2139/ssrn.3777392 (E.T.: 01.08.2025)

FATF, "Özel Sektörde Bilgi Paylaşımına İlişkin Rehber (Guidance on Private Sector Information Sharing)", 2017. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf (E.T.: 01.08.2025)

FATF, "Kara Paranın Aklanması ve Terörizmin ve Kitle İmha Silahlarının Finansmanıyla Mücadeleye İlişkin Uluslararası Standartlar– FATF Tavsiyeleri (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation– The FATF Recommendations)", 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (E.T.: 01.08.2025)

FATF, *2023–2024 Yılı Faaliyet Raporu (Annual Report 2023–2024)*, Paris, 2024. https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html (E.T.: 01.08.2025)

FINRA, "Menkul Kıymetler Sektöründe Yapay Zekâ (Artificial Intelligence in the Securities Industry)", 2020. https://www.finra.org/rules-guidance/key-topics/fintech/report-artificial-intelligence-financial-services-industry (E.T.: 01.08.2025)

Güven, Çiğdem, Onur Irmak ve Erkan Eren, "5411 Sayılı Bankacılık Kanununda Müşteri Sırlarının Tâbi Olduğu Hukukî Rejim ve Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik Üzerine Değerlendirmeler", *Bankacılar Dergisi, Sayı 122*, 2023, s. 18-45.

Greenleaf, Graham, "2013 Küresel Veri Mahremiyeti Yasaları (Global Data Privacy Laws 2013)", *Privacy Laws & Business International Report*, Sayı 122, 2014. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034 (E.T.: 01.08.2025)

"Hammurabi Kanunları", çeviri: L.W. King, *The Avalon Project*, Yale Law School, https://avalon.law.yale.edu/ancient/hamframe.asp (E.T.: 01.08.2025)

Hazar, Adalet ve Şenol Babuşçu, *Banka Hukuku*, Ankara, Seçkin Yayıncılık, 4. Baskı, 2025.

Hazine ve Maliye Bakanlığı, "Kişisel Verilerin Korunması, Muhafazası ve Paylaşımı Rehberi", 2015. https://ms.hmb.gov.tr/uploads/sites/12/2021/02/kisisel_verilerin_korunmasi_ve_paylsim_rehberi.pdf (E.T.: 01.08.2025)

Hazine ve Maliye Bakanlığı Malî Suçları Araştırma Kurulu (MASAK), *Şüpheli İşlem Bildirim Rehberi*, 2024. https://ms.hmb.gov.tr/uploads/sites/12/2024/05/MSK-RHB-SIB-001-2.pdf (E.T.: 01.08.2025)

"Hipokrat Yemini", çeviri: W.H.S. Jones. *Loeb Classical Library*, Harvard University Press, 1923. https://www.loebclassics.com/view/hippocrates_cos-oath/1923/pb_LCL147.295.xml (E.T.: 01.08.2025)

Hull, John C., *Risk Yönetimi ve Finansal Kurumlar* (*Risk Management and Financial Institutions)*, New Jersey, Wiley, 3. Baskı, 2012.

Ibish, Yusuf, "Çarşıların Loncaları (Brotherhoods of the Bazaars)", *The UNESCO Courier*, Cilt 30, Sayı 12, 1977. https://unesdoc.unesco.org/ark:/48223/pf0000074817

İç Denetçiler Enstitüsü (Institute of Internal Auditors - IIA), “Etkili Risk Yönetimi ve Kontrolde Üç Hatlı Savunma Modeli (The Three Lines of Defense in Effective Risk Management and Control)”, 2013. https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf (E.T.: 01.08.2025)

İngiltere Merkez Bankası, "2021 İki Yıllık İklim Senaryosu (CBES) Sonuçları *İ*klim Değişikliğinden Kaynaklanan Finansal Riskler *(*Boe Publishes Results Of The 2021 Biennial Exploratory Scenario: Financial Risks From Climate Change)", 2022. https://www.bankofengland.co.uk/news/2022/may/boe-publishes-results-of-the-2021-biennial-exploratory-scenario-financial-risks-from-climate-change (E.T.: 01.08.2025)

İngiltere Merkez Bankası, "2021 İklim İki Yıllık Araştırma Senaryosu Sonuçları *(*Results of the 2021 Climate Biennial Exploratory Scenario)", 2022. https://www.bankofengland.co.uk/stress-testing/2022/results-of-the-2021-climate-biennial-exploratory-scenario (E.T.: 01.08.2025)

İnsan Hakları Komitesi (Human Rights Committee), "Toonen v. Australia kararı", *Başvuru* No. 488/1992, 1994. http://hrlibrary.umn.edu/undocs/html/vws488.htm (E.T.: 01.08.2025)

İsviçre Bankalar ve Tasarruf Bankaları Federal Yasası (Bankengesetz– BankG / Federal Act on Banks and Savings Banks). https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en (E.T.: 01.08.2025)

İsviçre Federal Mahkemesi, "Banka Sırrı ve Kamu Yararı Hakkında Karar (Decision on Bank Secrecy and Public Interest)", 2017, Karar No: 4A_83/2016, BGE 143 II 506. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F143-II-506%3Ade&lang=de&type=show_document (E.T.: 01.08.2025)

Kandıralıoğlu, Pınar Çağla, "Türk Hukukunda Bankaların Sır Saklama Yükümlülüğü", Doktora Tezi, İstanbul Kültür Üniversitesi, 2010.

Kaplan, Robert S. ve Anette Mikes, "Risklerin Yönetimi: Yeni Bir Çerçeve" (Managing Risks: A New Framework), *Harvard Business Review*, Haziran 2012. https://hbr.org/2012/06/managing-risks-a-new-framework (E.T.: 01.08.2025)

Kara Para Aklanmasının Önlenmesine İlişkin Federal Yasa (Geldwäschereigesetz– AMLA / Anti-Money Laundering Act), 2015. https://www.fedlex.admin.ch/eli/cc/2015/791/en (E.T.: 01.08.2025)

Kaya, İlknur, *Banka Hukukunda Müşteri Sırrını Saklama Yükümlülüğü (Fransız, İsviçre ve Türk Hukukunda)*, Ankara, Seçkin Yayıncılık, 2024.

KKB, *Tarihçe*. https://www.kkb.com.tr/hakkimizda (E.T.: 01.08.2025)

KKB, "2021 Faaliyet Raporu". https://www.kkb.com.tr/faaliyetraporu2021/tr/m-1-1.html (E.T.: 01.08.2025)

KKB, *TBB Risk Merkezi Hizmetleri*, 2025. https://www.kkb.com.tr/urunler/tbb-risk-merkezi-hizmetleri (E.T.: 01.08.2025)

Kunz, Peter V., *İsviçre'de Banka (Müşteri) Sırrı*, çeviren: Erhan Seyfi Moroğlu, Banka ve Tüketici Hukuku Sorunları Sempozyumu, İstanbul Üniversitesi, On İki Levha Yayıncılık, 2010, s. 137-141.

Kurt, Selin, *Ticarî Sır, Bankacılık Sırrı Veya Müşteri Sırrı Niteliğindeki Bilgi Veya Belgelerin Açıklanması Suçu*, Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2019.

Mazıbaş, Murat, *Operasyonel Riske Basel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme*, BDDK Araştırma Raporu No: 2005/1, 2005. https://www.bddk.org.tr/ContentBddk/dokuman/duyuru_basel_0001_44.pdf (E.T.: 01.08.2025)

McKinsey & Company, *Bankacılıkta Risk Yönetiminin Geleceği* (*The Future of Risk Management in Banking*), 2022. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.pdf (E.T.: 01.08.2025)

Metin, Bilgin, "Sürdürülebilir Kişisel Veri Güvenliği Yönetişimi", *KVKK Akademik Derleme Çalışması* içinde, Kişisel Verileri Koruma Kurumu Yayınları, 2021, s. 345-366.

NGFS, "Eylem Çağrısı: Finansal Risk Kaynağı Olarak İklim Değişikliği *(*A Call for Action: Climate Change as a Source of Financial Risk)*"*, 2019.

OECD, "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımı Hakkında Rehber İlkeler (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)", 1980. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf (E.T.: 01.08.2025)

OECD, *Açık Kamu Verisi Raporu: Sürdürülebilir Etki İçin Politika Olgunluğunu Geliştirme* (*Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*), 2018. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/09/open-government-data-report_g1g94eac/9789264305847-en.pdf (E.T.: 01.08.2025)

OECD, "Finansal Hesap Bilgilerinin Otomatik Değişimi Standardının Uygulanması– 2019 (Implementation of the Standard for Automatic Exchange of Financial Account Information)", 2019. https://www.cbr.ru/Content/Document/File/84568/OECD_AEOI-Implementation-Report-2018.pdf (E.T.: 01.08.2025)

OECD, *Gizlilik ve Bilgi Güvenliği Yönetimi Araç Seti (Confidentiality and Information Security Management Toolkit)*, Küresel Şeffaflık ve Vergi Konularında Bilgi Değişimi Forumu, 2020. https://www.oecd.org/content/dam/oecd/en/networks/global-forum-tax-transparency/confidentiality-ism-toolkit-en.pdf (E.T.: 01.08.2025)

OECD, *Finansal Hesap Bilgilerinin Otomatik Değişimine İlişkin Akran Değerlendirme Rapor*u *(Peer Review of the Automatic Exchange of Financial Account Information)*, 2020. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/peer-review-of-the-automatic-exchange-of-financial-account-information-2020_845ac93f/175eeff4-en.pdf (E.T.: 01.08.2025)

Öcal, Talha, "Bankacılıkta Kredi Riski Yönetimi, Kredi Riski Ölçüm Modelleri Ve Türkiye Uygulaması", Doktora Tezi, İstanbul Üniversitesi, 2022.

Özbilger, Halil İbrahim, "İç Denetime Yeni Bir Bakış: Üçlü Hat Modelinin Değerlendirilmesi", *Denetişim Dergisi*, Sayı 22, 2020, s. 40-54.

Özen, Okan, *Ticarî Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu (TCK m. 239)*, Ankara, Seçkin Yayıncılık, 2024.

Reisoğlu, Seza, *Bankacılık Kanunu Şerhi*, Ankara, Yaklaşım Yayınları, Cilt 2, 2. Baskı, 2015.

Rochberg, Francesca, *Göksel Yazı: Mezopotamya Kültüründe Kehanet, Horoskopi ve Astronomi* (*The Heavenly Writing: Divination, Horoscopy, and Astronomy in Mesopotamian Culture)*, Cambridge, Cambridge University Press, 2004.

Saraç, Mehmet ve Mehmet Burak Kahyaoğlu, "Risk Algısının Tarihsel Gelişimi", *Finans Politik ve Ekonomik Yorumlar*, Cilt 48, Sayı 556, 2011, s. 31-43.

Schulz, Fritz, *Klasik Roma Hukuku* (*Classical Roman Law)*, Oxford, Clarendon Press, 1951.

Selimler, Hüseyin ve Süleyman Kale, "Türk Bankacılık Sektöründe Yabancı Para İşlemler", *Maliye ve Finans Yazıları, Sayı 96*, Temmuz 2012, s. 35-65.

Solove, Daniel J., "Bir Mahremiyet Sınıflandırması (A Taxonomy of Privacy)", *University of Pennsylvania Law Review*, Cilt 154, Sayı 3, 2006, s. 477–559.

Straumann, Tobias, *Zürih ve Cenevre: Altın Çağın Sonu* (*Zurich and Geneva: The End of the Golden Age)*, International Financial Centres after the Global Financial Crisis and Brexit içinde, Oxford, Oxford University Press, 2018, s. 106-125.

Şener, Mert Mehmet, "Kurumsal Risk Yönetimi Üzerine Bir Yazın Taraması", *Akademik Sosyal Araştırmalar Dergisi,* Sayı 71, 2018, s. 459-494.

Taş, Caner, "Şimdi Al Sonra Öde Müşterilerinin Kredi Risk Skorlamasında Makine Öğrenmesi ve Standart Kredi Risk Modellerinin Performanslarının Karşılaştırılması

(Comparison of Machine Learning and Standard Credit Risk Models Performances in Credit Risk Scoring of Buy Now Pay Later Customers)", Yayımlanmamış Yüksek Lisans Tezi, ODTÜ, 2023.

Taşdelen, Servet, *Bankacılık Kanunu Şerhi,* Ankara, Adalet Yayınevi, Cilt 2, 2. Baskı, 2015.

TBB, "Risk Merkezi Yönetmeliği", 2014. https://www.tbb.org.tr/pdf/faaliyetler/71/784 (E.T.: 01.08.2025)

TBB, "Bankacılık Etik İlkeleri", 2014. https://www.tbb.org.tr/pdf/faaliyetler/89/702 (E.T.: 01.08.2025)

"TBB Risk Merkezi, Türkiye Bankalar Birliği Risk Merkezi Raporlarının E-Devlet Kapısından Sunulmasına İlişkin Kamuoyu Duyurusu", 2019. https://www.tbb.org.tr/duyurular/pdf/2816 (E.T.: 01.08.2025)

TBB, Risk Merkezi Aylık Bültenler (Ocak, Mart, Haziran, Eylül, Aralık 2024).

TBB, *Risk Merkezi 2023-2024 Faaliyet Raporu*, 2024.

TBB, *Risk Merkezi 2024-2025 Faaliyet Raporu*, 2025.

TCMB, "Risk Merkezi Duyurusu (DUY-2013/48)", 2013. https://www.tcmb.gov.tr/wps/wcm/connect/8064278a-fe74-4add-acc5-d4b9b40d0ca3/DUY2013-48.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-8064278a-fe74-4add-acc5-d4b9b40d0ca3-m3fC8mf (E.T.: 01.08.2025)

TCMB, *2018 Yılı Faaliyet Raporu*, s. 23. https://www3.tcmb.gov.tr/yillikrapor/2018/files/tr-full.pdf (E.T.: 01.08.2025)

TCMB, *2022 Yılı Para ve Kur Politikası*, 2021. https://www.tcmb.gov.tr/wps/wcm/connect/e9d73d1f-1523-46ea-a307-bb74fe366389/2022+Para+ve+Kur+Politikas%C4%B1.pdf?MOD=AJPERES&CACHEID

=ROOTWORKSPACE-e9d73d1f-1523-46ea-a307-bb74fe366389-nU4.h6f (E.T.: 01.08.2025)

TCMB, *Yıllık Faaliyet Raporu*, 2023. https://www3.tcmb.gov.tr/yillikrapor/2023/pdf/TCMB-Faaliyet-Raporu-2023.pdf (E.T.: 01.08.2025)

TCMB, *Finansal İstikrar Raporu*, Sayı 38, 2024. https://www.tcmb.gov.tr/wps/wcm/connect/tr/tcmb+tr/main+menu/yayinlar/raporlar/finansal+istikrar+raporu/2024/sayi+38 (E.T.: 01.08.2025)

Tekin, Kemal Doruk, *Banka Sırrı Kavramı Yönünden Bankalarda Sır Saklama Yükümlülüğü*, Ankara, Adalet, 2010.

Tekinalp, Ünal, *Banka Hukukunun Esasları*, İstanbul, Vedat Kitapçılık, 2. Baskı, 2009.

U.S. Department of Justice, "Yaşamı ve Özgürlüğü Korumak (Amerika'yı Terörizmi Önlemek İçin Gerekli Araçlarla Birleştirme ve Güçlendirme Yasası) (PATRIOT Act– Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)", 2001. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (E.T.: 01.08.2025)

Westin, Alan Furman, *Mahremiyet ve Özgürlük* (*Privacy and Freedom)*, New York, Atheneum, 1967.

Yıldırım, Gurbet Arife, "Banka Çalışanlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Müşteri Sırlarını Koruma Yükümlülükleri", Yüksek Lisans Tezi, Ufuk Üniversitesi, Ankara, 2021.

Zuboff, Shoshana, *Gözetim Kapitalizmi Çağı: İktidarın Yeni Sınırında İnsanlığın Geleceği İçin Mücadele* (*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power)*, New York, PublicAffairs, 2019.

İnternet Kaynakları:

www.anayasa.gov.tr
www.danistay.gov.tr
www.kazanci.com.tr
www.kvkk.gov.tr
www.lexpera.com.tr
www.rekabet.gov.tr
www.yargitay.gov.tr