

Bankacılık Sırlarının Korunmasında Risk Temelli Yaklaşım: Türk Hukukunda Fiilen İşleyen Bir Regülasyon Çerçevesi

Kaan KARAMANLI*

Öz

Düzenleyici otoriteler tarafından gerçekleştirilen düzenleme faaliyetlerinde, kural oluşturma, kurallara uyum ve aykırılığa yaptırım uygulama şeklindeki geleneksel kural temelli yaklaşımın yerini, uygulayıcıya takdir alanı tanıyan risk temelli düzenleme yaklaşımına bıraktığı görülmektedir. Bu yaklaşım, düzenlemeye konu faaliyetlerin doğurabileceği risklerin önceden değerlendirilmesini, bu risklere uygun önlemlerin alınmasını ve yapılan değerlendirmelerin hesap verebilirlik ilkesi çerçevesinde denetlenebilir olmasını esas almaktadır.

Bu çalışmada, risk temelli düzenleme yaklaşımı kavramsal açıdan ele alınmakta ve bu yaklaşımın bankacılık mevzuatındaki görünümü değerlendirilmektedir. Bu kapsamda, Avrupa Birliği veri koruma hukukunda risk temelli yaklaşımın açık ve sistematik bir şekilde benimsendiği, buna karşılık Türk hukukunda KVKK'da sınırlı düzeyde karşılık bulduğu görülmektedir.

Bankacılık sırrının korunmasına ilişkin Türk mevzuatı ise farklı bir görünüm sunmaktadır. Bu mevzuat risk temelli yaklaşımı sistematik biçimde ortaya koymamakla birlikte gerek genel risk yönetimi düzenlemeleri gerek veri paylaşımına ilişkin kararların bankalarca risk değerlendirmesine ve hesap verebilirliğe dayalı olarak alınmasını öngören yapı fiilen işleyen bir risk temelli yaklaşıma işaret etmektedir.

Bu yönüyle çalışma, risk temelli yaklaşımın Türk hukukunda yalnızca normatif düzenlemelerde açıkça zikredilerek değil, sektörel düzenlemeler ve uygulama pratikleri aracılığıyla da geliştiğini ortaya koyarak literatüre katkı sunmayı amaçlamaktadır.

Anahtar Kelimeler: Bankacılık Sırrı, Risk Temelli Yaklaşım, Regülasyon, Veri Koruma Hukuku, Risk Yönetimi

Jel Sınıflaması: K10, K20, G21, G28, G32

* Grup Başkanı (Bankacılık Başuzmanı), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Düzenleme Daire Başkanlığı; Doktora Öğrencisi, Türk-Alman Üniversitesi, Özel Hukuk Doktora Programı; e248109002@stud.tau.edu.tr, ORCID: 0000-0001-8258-3243.

Atıf: Karamanlı, K. (2026). Bankacılık Sırlarının Korunmasında Risk Temelli Yaklaşım: Türk Hukukunda Fiilen İşleyen Bir Regülasyon Çerçevesi. BDDK Bankacılık ve Finansal Piyasalar Dergisi, 20(1), 71-93.
<https://doi.org/10.46520/bddkdergisi.1972891>

Bu çalışmada belirtilen görüşler yazarına ait olup, Bankacılık Düzenleme ve Denetleme Kurumu'nun görüşlerini yansıtmamaktadır.

Makale Gönderim Tarihi: 11.05.2026

Makale Kabul Tarihi: 12.06.2026

Abstract- A Risk-Based Approach to The Protection of Banking Secrecy: A Functioning Regulatory Framework in Turkish Law

In regulatory activities carried out by regulatory authorities, the traditional rule-based approach characterized by rule-making, ensuring compliance with rules, and imposing sanctions for violations appears to have been replaced by a risk-based regulatory approach that grants discretion to the implementing authority. This approach is based on the prior assessment of the risks arising from activities subject to regulation, the adoption of measures appropriate to such risks, and the auditability of the assessments made within the framework of the principle of accountability.

This study examines the risk-based regulatory approach from a conceptual perspective and evaluates its manifestation in banking legislation. In this context, it is observed that the risk-based approach has been explicitly and systematically adopted in European Union data protection law, whereas it has found only limited reflection in the Turkish Personal Data Protection Law (KVKK).

Turkish legislation on the protection of banking secrecy, however, presents a different picture. Although this legislation does not set forth the risk-based approach systematically, the structure requiring data-sharing decisions to be made by banks on the basis of risk assessment and accountability -together with the general risk management regulations -points to a de facto functioning risk-based approach. In this respect, the study aims to contribute to the literature by demonstrating that the risk-based approach in Turkish law has developed not only through explicit reference in normative regulations but also through sectoral regulations and implementation practices.

Keywords: Banking Secrecy, Risk-Based Approach, Regulation, Data Protection Law, Risk Management
JEL Classification: K10, K20, G21, G28, G32

1. Giriş

Günümüzde düzenleme faaliyetlerinde risk kavramı daha fazla önem kazanmakta, düzenlemelerin risk temelli bir perspektifle oluşturulması öne çıkan bir yaklaşım haline gelmektedir. Ayrıntılı kurallar aracılığıyla istenilen eylem veya işlemleri önceden belirlemeye dayanan kural temelli yaklaşımın yanında, düzenleme konusu faaliyetlerin doğurabileceği risklerin değerlendirilmesini esas alan risk temelli düzenlemeler özellikle Avrupa Birliği hukukunda son dönemde görülmektedir. Bu yaklaşım, risklerin önceden değerlendirilmesini, niteliğine göre farklılaştırılmış yükümlülükler öngörülmesini ve düzenleme öznesine belirli ölçüde takdir alanı tanınmasını esas almaktadır. Bu yönüyle risk temelli yaklaşım, getirilen kurallara salt uyumu ele alan geleneksel kural temelli düzenlemelerden ayrılarak, daha esnek, dinamik ve hesap verebilirlik ilkesiyle bütünlüklü düzenleme perspektifini ifade etmektedir.

Kişisel verilerin korunmasına ilişkin Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), söz konusu yaklaşımın en belirgin örneklerinden birini teşkil etmektedir (Çekin, Berktaş, v.d., 2023). Zira, GDPR veri sorumlularına, veri işleme faaliyetlerinin niteliği, kapsamı ve ilgililerin hak ve özgürlükleri bakımından doğurabileceği riskler çerçevesinde değerlendirme yapma ve buna uygun teknik ve idari tedbirleri belirleme sorumluluğu yüklenmiştir. Bu yaklaşımda risk kavramı, veri koruma hukukunun merkezine yerleştirilmekte, düzenleyici otoritenin rolü, önleyici ve yönlendirici bir çerçeveye sınırlandırılmakta, riski değerlendirme ve uygun önemleri alma yükümlülüğü veri sorumlularıyla veri işleyenlere bırakılmaktadır.

Türk hukukunda ise, temel düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) büyük ölçüde 95/46/EC sayılı AB Direktifi esas alınarak hazırlanmış, sonraki değişikliklerle GDPR'la

uyumlaştırılmaya çalışılmıştır. Bununla birlikte, KVKK'nın sistematigi incelendiğinde, GDPR'da açık ve sistematik biçimde yer bulan risk temelli yaklaşımın ve buna bağlı araçların -özellikle risk değerlendirmesi, farklılaşan yükümlülükler ve hesap verebilirlik mekanizmalarının- aynı açıklıkta düzenlenmediği görülmektedir.

Öte yandan, bankacılık sektörü, doğası gereği risk yönetimi üzerine kurulu bir faaliyet alanıdır. Bankalar, faaliyetlerinde kredi riski, piyasa riski, likidite riski ve operasyonel risk farklı risk türlerini tanımlamak, ölçmek ve yönetmekle yükümlüdür. Bu risk kategorileri, veri koruma hukukunda esas alınan, ilgililerin hak ve özgürlüklerine yönelik risklerden farklılık arz etmektedir. Ancak, bankacılık sırrı niteliğindeki bilgilerin korunmasına ilişkin düzenlemeler, bir yandan ilgililerin hak ve özgürlüklerini korurken, öte yandan bankacılık faaliyetine özgü risklerle de ilişkilidir. Bu açıdan, sektörün risk yönetimi anlayışı, sır niteliğindeki verilerin paylaşımına ilişkin kararların da risk değerlendirmesine dayalı alınmasına zemin hazırlamaktadır. Nitekim, bankacılık mevzuatının genel yapısında, risklerin sınıflandırılması, ölçülmesi ve yönetilmesine ilişkin yükümlülüklerin açıkça düzenlenmekte olup bu yönüyle sektörün, risk temelli bir düzenleme yaklaşımına yabancı olmadığı görülmektedir.

Bu çalışmanın hareket noktasını, kişisel verilerin korunmasına ilişkin genel mevzuatta risk temelli yaklaşımın sınırlı düzeyde yer bulmasına karşın, bankacılık sektörüne özgü düzenlemelerde, özellikle bankacılık sırlarının korunmasına ilişkin rejimde, risk temelli yaklaşımın ne ölçüde yer bulduğunun değerlendirilmesi ve tespitlerin ortaya konulması oluşturmaktadır.

Ülkemizde bankacılık sırlarının korunmasına ilişkin temel düzenleme 5411 sayılı Bankacılık Kanunu'nun (Kanun) 73'üncü maddesidir. Bu maddeye dayanılarak çıkarılan Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik (Sır Yönetmeliği) ve uygulanmasına ilişkin ek açıklamalar getiren 2022/1 sayılı Genelge (Sır Genelgesi) doğrudan bankacılık sırlarının korunmasına yönelik düzenlemelerdir. Söz konusu düzenlemeler incelendiğinde, müşteri sırrı niteliğindeki bilgilerin paylaşımının kural olarak müşterinin talep ve talimatına, banka sırrı niteliğindeki bilgilerin paylaşımının ise kural olarak yönetim kurulunun iradesine bağlı olduğu görülmektedir. Bununla birlikte, paylaşımına ilişkin somut olay bazında değerlendirme veya karar alma süreçleri önemli ölçüde bankaların uhdesine bırakılmış olup bu süreçler bankaların maruz kaldıkları riskler çerçevesinde şekillenmektedir. Ayrıca, bankacılık sektörüne ilişkin risk yönetimi düzenlemeleri de veri güvenliği ve gizliliği ihlallerini operasyonel ve uyum riski kapsamında ele alarak, bu risklerin yönetimini bankaların sorumluluğuna bırakmaktadır.

Bu çerçevede çalışmada öncelikle risk kavramı, bankacılık verilerinin risk boyutu ve risk temelli düzenleme yaklaşımı ele alınmakta; ardından kişisel verilerin korunmasına ilişkin düzenlemelerde risk temelli yaklaşımın görünümü GDPR ve KVKK bağlamında değerlendirilerek, Türk bankacılık mevzuatında bankacılık sırlarının korunmasına ilişkin düzenlemeler incelenmektedir. Bu doğrultuda, bankacılık sırrının korunmasına ilişkin düzenlemeler tek başına ele alındığında, risk temelli yaklaşımı açık ve sistematik bir model olarak ortaya koymamaktadır. Ancak bu düzenlemeler, bankacılık faaliyetinin tabi olduğu genel risk yönetimi çerçevesiyle birlikte değerlendirildiğinde, risk değerlendirmesini karar alma süreçlerinin merkezine yerleştiren kümülatif bir yapı ortaya çıkmaktadır. Başka bir ifadeyle, bu alandaki risk temelli nitelik, salt bir düzenlemenin açık ifadesinden değil; sır düzenlemeleriyle sektörel risk yönetimi düzenlemelerinin birlikte oluşturduğu bütünden kaynaklanmaktadır. Çalışma, bu kümülatif yapıyı ortaya koyarak, risk temelli yaklaşımın Türk hukukunda yalnızca açık normatif ifadeler yoluyla değil, sektörel düzenlemelerin birlikte işleyişi aracılığıyla da gelişebileceğini göstermeyi amaçlamaktadır.

Bu noktada belirtmek gerekir ki bazı düzenlemelerde risk değerlendirmesi, "risk" kavramının açıkça zikredilmesinden ziyade, uygulama yapısı, karar alma mekanizmaları ve yükümlülüklerin dağılımı aracılığıyla işlevsel olarak düzenlemenin merkezine yerleşebilmektedir. Bu açıdan çalışmada, bankacılık sırlarının korunmasına yönelik mevzuatta "risk" kavramının açıkça yer alıp almamasından ziyade, gerek bu hükümlerin uygulanması ve karar alma mekanizmaları gerek bankacılık faaliyetine yönelik risk yönetimi düzenlemeleri birlikte ele alındığında ortaya çıkan, risk değerlendirmesine dayalı işleyiş dikkate alınmıştır. Bu nedenle, regülasyonun değerlendirilmesinde "fiilen işleyen bir yaklaşım" ifadesinin kullanımı tercih edilmiştir.

2. Risk Kavramı ve Kavramsal Çerçevesi

2.1. Risk Kavramı

Risk, bir sonucun, olayın veya kaybın yarattığı belirsizlik; yaralanma, hasar, kayıp veya zarar olasılığının varlığı olarak nitelendirilmektedir (Black's Law Dictionary, 2004). Belirsizliğin hâkim olduğu durumlarda risk kavramı ön plana çıkmakta, belirsizliğin doğurabileceği sonuçların değerlendirilmesi için, planlanan işlem ve eylemlerin gerçekleştirilmesi halinde yol açabileceği ihtimallerin ortaya konulması önem kazanmaktadır.

Risk kavramı kullanıldığı yerlerde, olumsuz bir durumu çağırırsa da bu nitelendirme temel olarak doğru değildir. Zira risk, doğrudan bir kaybı, zararı veya gerçekleşmiş bir tehlikeyi değil kimi durumda kazanca kimi durumda ise kayba götürebilecek bir ihtimalin varlığını ifade eder. Dolayısıyla, asıl önemli olan ortaya çıkabilecek tehlike veya zararın kendisi değil; bu olasılığın önceden değerlendirilmesine, azaltılmasına veya ortadan kaldırılmasına yönelik adımların atılması ve risk tahmin yöntemlerinin geliştirilmesidir (Babuşçu, Hazar, v.d., 2021). Bu açıdan, risk temelli regülasyon yaklaşımının da merkezinde yer alan "risk" kavramını "zarar" kavramından ayırmak, regülasyona ilişkin yaklaşımların belirlenmesi açısından önem taşımaktadır.

2.2. Verilerin Korunması Bakımından Bankacılıkta "Risk"

Bankacılık en temel anlamıyla, halktan istenildiğinde veya önceden belirlenmiş bir zamanda geri verilmek üzere toplanan parasal kıt kaynağın, ihtiyaç duyanlara ödünç verilmesi ve bu yolla kazanç sağlaması esasına dayanan bir faaliyettir. Doğası gereği bu faaliyet itibar, kredi, likidite, piyasa veya uyum riski gibi birçok riski bünyesinde barındırmaktadır. Bu nedenle risk ve riskin yönetimi bankacılıkta önemli bir yere sahip olup bankacılık esasen bir risk yönetme faaliyeti olarak nitelendirilmektedir (Babuşçu, Hazar, v.d., 2021). Nitekim, yüksek getiri arzusu eş anlamlı olarak yüksek riski de beraberinde getireceğinden, finansal krizlerin kaynağının da yüksek riskle ilişkilendirilmesine yol açmaktadır (Tunay, 2010).

Risk yönetiminin amacı ise, bankacılık faaliyetlerinin niteliğini ve düzeyini izlemek, kontrol altında tutmak ve gerektiğinde değiştirmek üzere belirlenen politika ve usullerle risklerin tanımlanmasını, ölçülmesini, raporlanmasını, izlenmesini, kontrolünü sağlamaktır (İSEDES², m. 35). Hızla değişen ekonomik koşullar, piyasa hareketleri ve teknolojik gelişmeler karşısında, risklerin daha iyi ölçülebilmesi ve yönetilebilmesi için bankaların güçlü bir risk yönetim sistemine sahip olması büyük önem taşımaktadır. Bu nedenle gerek kanun gerek ikincil düzenlemelerle güçlü risk yönetimi oluşturulması için yükümlülükler getirilmiştir. Örneğin, İSEDES uyarınca bankalar etkin, risk doğuran faaliyetlerin yoğunluk ve karmaşıklık düzeyiyle orantılı bir risk yönetim sistemini tesis etmekle yükümlüdür. Risk yönetim sisteminin kapsamlılık düzeyi, bankaların büyüklüğü ve faaliyetlerinin karmaşıklığıyla orantılı olarak oluşturulur. Bu açıdan bankacılık sektörü, faaliyetlerinin ölçeği ve karmaşıklığı da dikkate alındığında diğer sektörlerden pozitif yönde ayrışmakta ve bu alanda konusunda önemli tecrübeye sahip bulunmaktadır.

Çalışma konumuz bakımından bankacılık sırları hem müşterilerinin finansal hareketlerine hem de bankanın varlığına ilişkin önemli bilgiler içerdiğinden, bunların korunmasına ilişkin de birtakım

² Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik

risklerin ortaya çıkabilmektedir. Bu açıdan, bankacılığa özgü diğer risklerin yanında özellikle mevzuata uyumsuzluktan doğabilecek "uyum riski" ile düzenlemelere aykırılık halinde ortaya çıkabilecek "itibar riski" ön plana çıkmaktadır. Bankalar nezdinde müşteri sırrı veya banka sırrı olarak oluşan veriler, özellikle saklanması ve paylaşımı konusunda özel hükümlere tabi kılınmıştır.

Bankaların faaliyetleri çerçevesinde oluşan verilerin toplanması, işlenmesi ve bunlar üzerinden finansal değerlendirme yapılması bankacılık faaliyetinin doğal bir sonucudur. Bankaların müşterilerini tanıması (know your customer), kredi başvurusunda bulunan müşterinin kredibilitesinin tespiti ve bireysel müşteriler risklilik durumlarının takibi gibi birçok süreç, bankayla müşteri arasındaki ilişkide kullanılacak verilerin varlığına bağlıdır (Arslanhan, 2024). Nitekim, müşterinin tanınmasına ilişkin bu gereklilikten kaynaklı, müşteri kimlik verilerinin elde edilmesi ve saklanması, Basel Bankacılık Denetim Komitesi'nin (BCBS)³ "Consolidated KYC Risk Management" (BCBS, 2004) ve "Sound Management Of Risks Related To Money Laundering And Financing Of Terrorism" (BCBS, 2014) dokümanlarında da ele alınmaktadır. Söz konusu dokümanlarda, bankaların finansal suçların işlenmesine aracı olmasının engellenmesinin, bankaların itibarını ve bankacılık sisteminin koruyacağı, itibardan kaynaklanan zararları engelleyeceği, dolayısıyla risk yönetimi bakımından müşteri verilerine erişilebilirliğin önem taşıdığı vurgulanmaktadır (BCBS, 2001). Bu açıdan, bankalarla müşterileri arasında gerçekleştirilen bankacılık faaliyetinin sürdürülebilirliği, elde edilen verilerin işlenmesini de zorunlu kılmaktadır (Karamustafaoğlu, Ünsal Özden, v.d. (2021). Dolayısıyla, bankacılık verilerine ilişkin eksiklikler bankaları başta itibar, operasyonel, hukuki, yoğunlaşma gibi riskler olmak üzere ciddi risklere maruz bırakabilir.

Bankanın finansal risklerinin yönetiminde kullandığı müşteri sırrı niteliğindeki verilerin gereği gibi saklanmaması, kişilerin gizliliklerinin zedelenmesine ve bu verilerin kişilerin zararına olacak şekilde kullanılmasına kapı açmak suretiyle risk doğurabilir. Zira, bankanın faaliyetlerinin veya çalışanlarının eylemlerinin mevzuata uygun olmaması finansal veya itibari kayıplara ilişkin *operasyonel riski*, *uyum riskini* veya toplumsal algı bakımından ise *itibar riskini* gündeme getirir.

Bu çerçevede bankacılık sırlarının korunması, saklanması ve esaslar dahilinde paylaşılması belirli kurallara tabidir. Kurallara aykırılık ise, banka açısından idari yaptırımla karşılanması ve verilerine izinsiz erişilen kişilerin bankaya olan güvenlerinin zedelenmesi sonucunu doğurabilir. Dolayısıyla bu tür zararların önlenmesi, bankanın ilgili riskleri doğru şekilde yönetilmesini gerektirir.

3. Risk Temelli Düzenleme Yaklaşımı (Risk-Based Regulation)

3.1. Genel Olarak "Düzenleme Faaliyeti"

Düzenleme kavramı, en temel anlamıyla, bir konuya ilişkin getirilen kuralların bütünü olarak ifade edilebilir. Daha geniş anlamda ise düzenleme, bir kamusal yetki ve gücün kullanımıyla bağlayıcı kuralların belirlenmesini, bu kuralların uygulanmasını, uygulamanın izlenmesini ve aykırılık halinde gerekli yaptırımın tesis edilmesini kapsayan, bu süreçlerin özellikle bir kamu kurumunun görevli ve yetkili olarak eşlik ettiği faaliyetler bütünüdür (Baldwin, Scott, v.d., 1998).

Kamusal yetkinin kullanılmasıyla yürütülen düzenleme faaliyetleri, muhataplarının işlem ve eylemlerine yön veren farklı amaçlar taşıyabilmektedir. Bu faaliyetler, kimi zaman mevcut düzenlemelerin genişletilmesine, kimi zaman da bir faaliyet alanının çerçevesinin çizilmesine, izne tabi kılınmasına veya sınırlandırılması yönelik olabilir. Örneğin, bankacılık sırrı niteliğindeki verilerinin korunmasına ilişkin Sır Yönetmeliği ve Sır Genelgesi 2022 yılından önce halihazırda kanun düzeyinde düzenlenmiş olan banka ve müşteri sırrına ilişkin paylaşımların ilişkin kapsam, şekil, usul ve esasları belirleyen ikincil nitelikli bir düzenleme faaliyeti olarak karşımıza çıkmaktadır.

³ Basel Bankacılık Denetim Komitesi, Türkiye Cumhuriyet Merkez Bankası'nın da üyeleri arasında bulunduğu Uluslararası Ödemeler Bankası'nın (BIS), ülkemizin de aralarında bulunduğu 45 üye ülkeden oluşan, bankaların Basel Bankacılık Denetim Komitesi, Türkiye Cumhuriyet Merkez Bankası'nın da üyeleri arasında bulunduğu Uluslararası Ödemeler Bankası'nın (BIS), ülkemizin de aralarında bulunduğu 45 üye ülkeden oluşan, bankaların ihtiyati düzenlemesi için birincil küresel standartların belirleyicisi ve bankacılık denetim konularında düzenli iş birliği sağlanmasına katkı sunan, finansal istikrarın artırılması amacıyla dünya genelinde bankaların düzenlenmesini, gözetimini ve uygulamalarının güçlendirilmesini amaçlayan bir komitesidir.

Bir başka örnekte, 2021 yılından önce de ülkemizde çeşitli kuruluşlarca yürütülen tasarruf finansman faaliyeti, 2021 yılında getirilen yasal düzenlemelerle çerçevesi belirli, kurallara tabi, yürütülmesi kamusal izne bağlı, regüle bir alana dönüştürülmüştür. Dolayısıyla, düzenleme faaliyetleri kimi zaman halihazırda regüle edilen bir alanın yeni unsurlarla geliştirilmesi, kimi zaman da hiç regüle olmayan bir alanın kurallara bağlanması amacıyla yürütülebilmektedir.

Bu çerçevede, regülasyon, belirli bir faaliyet alanına girişten faaliyetlerin sürdürmesine ve hatta sona erdirilmesine kadar uzanan sürece ilişkin kuralların oluşturulmasını ifade etmektedir. Söz konusu kurallar, kanun koyucu veya düzenleyici otorite tarafından çıkarılan bağlayıcı normatif düzenlemelerle şekillenir ve faaliyetlerin hangi şartlar altında, hangi yükümlülüklerle tabi olarak yürütüleceğini belirler. Regülasyon, yalnızca kuralların konulmasını değil, bu kuralların değişen ihtiyaçlar doğrultusunda güncellenmesini, uygulamanın denetlenmesini ve aykırılık halinde yaptırımlar uygulanmasını da kapsayan dinamik bir çerçeve ortaya koyar (Altay, 2019).

3.2. Risk Temelli Yaklaşımın Tanımı ve Kapsamı

Düzenleyici amaçların gerçekleştirilmesi bakımından, düzenleme sürecinde tercih edilen yaklaşım, düzenleme çerçevesinin yapısını doğrudan belirlemektedir. Zira düzenlemenin neyi esas aldığı ve nasıl uygulanmasını öngördüğü, düzenlemeye tabi olanların davranışlarını da şekillendirmektedir. Bu kapsamda düzenlemeler; ayrıntılı kurallar içeren ve bu kurallara sıkı bağlılık öngören kural temelli bir yaklaşımla hazırlanabileceği gibi, daha esnek, yönlendirici ve risklere odaklanan bir yaklaşımla da oluşturulabilir.

Anılan farklı yaklaşımlar, düzenleme sonucu ortaya çıkan davranış biçimlerini ve hedeflere ulaşma yöntemlerini belirlemeleri bakımından birbirinden ayrılmaktadır. Bununla birlikte, düzenlemeler çoğu zaman biden fazla yaklaşım unsurlarını bir arada içerebilir (Burgemeestre, Hulstijn, v.d., 2009). Kural temelli yaklaşım; uyulması gereken kuralların ayrıntılı biçimde belirlendiği ve ihlal halinde uygulanacak yaptırımların açıkça ortaya konulduğu bir modeldir (Decker, 2018). İlkeler temelli yaklaşım ise kesin kurallar yerine genel prensipler ortaya koyarak uygulayıcıya ulaşılması gereken sonuçlar bakımından belirli bir hareket alanı tanıır (Black, Hopper, v.d., 2007).

Bu kapsamda, bu yaklaşımların bankacılık mevzuatındaki yansımalarına bakıldığında örneğin, kurumsal yönetim yapılarını belirlemelerine yönelik ilkeler içeren *"Bankaların Kurumsal Yönetim İlkelerine İlişkin Yönetmelik"*in ilkeler temelli bir yaklaşımı yansıttığı, buna karşılık bankaların kuruluş şartları ve izin süreçlerini ayrıntılı şekilde düzenleyen hükümler içeren *"Bankaların İzne Tabi İşlemleri İle Dolaylı Pay Sahipliğine İlişkin Yönetmelik"*in ise kural temelli yaklaşımı yansıttığı görülmektedir.

Risk temelli yaklaşım ise, düzenleyici otoritenin ayrıntılı kurallar koymasından ziyade, düzenlemeye tabi olanların risk değerlendirmesine dayalı hareket etmesini esas alan daha esnek bir yaklaşımdır (Burgemeestre, Hulstijn, v.d., 2009). Bu yaklaşımın temelini yönetilmesi gereken riskler oluşturur. Tabi olanlara getirdiği esneklik bakımından ilkeler temelli yaklaşıma benzerse de ondan farklı olarak ilkelerin uygulanmasında tam bir serbesti tanımayı değil, çizilen sınırlar içerisinde faaliyetin risk değerlendirmesine tabi kılınmasını, bu değerlendirmenin tabi olanlar tarafından yapılmasını ve gerektiğinde hesap verilebilir olmasını öngörür. Bu kapsamda hazırlanan düzenlemeler, risk düzeyine bağlı olarak faaliyetlerin önceliklendirilmesini ve denetim-gözetim mekanizmalarının buna göre şekillendirilmesini içerir (Black, 2010). Veri koruma alanında bu yaklaşım, tüm durumlar için tek tip kurallar uygulanmasını değil, karşılaşılabilecek risklerin değerlendirilerek uygun tedbirlerin alınmasını ifade eder (Gellert, 2020).

Bu çerçevede risk temelli yaklaşım, düzenlemenin odağına düzenlenen alanda ortaya çıkabilecek risklerin yerleştirildiği; risklerin belirlenmesi, analiz edilmesi ve yönetilmesini içeren bir süreç öngörür

(Gellert, 2018). Bu çerçevede düzenlemenin muhatapları, faaliyetlerin doğurabileceği riskleri öngörerek riske ilişkin gerekli değerlendirmeleri yapmak, tedbirleri almak ve riskin gerçekleşmesi halinde gerekli adımların atıldığı konusunda gerektiğinde otoriteye hesap verebilmekle yükümlüdür (Çekin, 2025). Bu süreç sonucunda elde edilen bulgular, özellikle veri güvenliğine ilişkin alınacak tedbirlerin belirlenmesi bakımından yol gösterici nitelik taşımaktadır (Tokmakçı, 2023). Zararlı bir sonucun meydana gelmesinden önce risk değerlendirmesi yapılmasına imkân veren bu yaklaşım, önleyiciliği güçlendirmekte ve kurallara uyumun yüksek düzeyde tutulmasına imkân sağlanmaktadır (Yan, 2023).

3.3. Risk Temelli Yaklaşım Dayalı Düzenlemelerin Özellikleri

Düzenlemelerin risk temelli yaklaşım çerçevesinde hazırlanmasının temel amacı, faaliyetlerde ortaya çıkabilecek risklerin, *ex ante*⁴ (önceden) değerlendirilmesini ve bu değerlendirme sonucunda gerekli önlemlerin ilgili tabi olanlarca alınmasını sağlamaktır. Bu kapsamda, riskli işlemlerde sorumluluk, riski yönetene ait olmakta, denetim işlevini üstlenmekte, gerekli önlemlerin alınmaması halinde doğacak sonuçlara düzenlemeye tabi olanların katlanması beklenmektedir. Bu yönüyle yaklaşım, kaynakların riskin olasılık ve etkisine göre tahsis edilmesini ve karar süreçlerinin düzenlemeye tabi olanların hakimiyet alanına bırakılmasını öngörmektedir (Gonçalves, 2019).

Risk temelli yaklaşımı diğer düzenleme yaklaşımlarından ayıran temel unsur, risk analizi, aksiyon alma ve hesap verebilirlik arasında kurulan ilişkiyle düzenlemeye tabi olanlara tanınan değerlendirme ve hareket alanıdır. Bu çerçevede risk temelli düzenlemelerin genel olarak şu özellikleri içerdiği söylenebilir:

- Düzenlemeye konu faaliyet alanındaki risklerin ve bu risklerle birlikte ortaya çıkabilecek faydaların belirlenmesi (Ebers, 2025),
- Risklerin önlenmesine veya azaltılmasına yönelik genel bir çerçevenin oluşturulması,
- Faaliyete ilişkin aksiyon alma kararının düzenlemeye tabi olan aktörlere bırakılması,
- Faaliyet öncesi izin, onay veya uygunluk mekanizmalarının sınırlı tutulması,
- Uyum sorumluluğunun esas itibarıyla düzenlemeye tabi olanlara ait olması (Gellert, 2021),
- Düzenleyici otoritenin doğrudan müdahaleci bir rol üstlenmekten ziyade faaliyet öncesinde değil faaliyet sırasında *ex post* denetim fonksiyonuna odaklanması (Çekin, Berktaş, v.d., 2023),
- Düzenlemelerin esnek ve değişen koşullara uyarlanabilir olması, risk değerlendirmeleri neticesindeki değişen risk durumlarına göre gerekli değişikliklerin yapılabilmesi (Kaya, 2020),
- Alınan kararların hesap verebilir nitelikte olması ve gerektiğinde otoriteye sunulabilmesi (Çekin, Berktaş, v.d., 2023).

Bu yönüyle risk temelli yaklaşım, düzenlemelerin uyulması gereken kurallardan ziyade yönetilmesi gereken risklere odaklanmasını gerektirir (Black, 2010). Kural temelli düzenlemelerin ayrıntılı ve katı yapısının karmaşıklığa yol açması ve değişen koşullara uyum sağlamakta yetersiz kalması risk temelli yaklaşımlara yönelimin nedenlerindedir (Gellert, 2020). Bununla birlikte, risk temelli yaklaşımın uygulanmasının zorlukları da söz konusu olabilecektir. Özellikle risklerin doğru şekilde belirlenebilmesi için yeterli veri bulunması, risk değerlendirme yöntemlerinin sağlıklı sonuçlar üretmesini ve otoritenin denetim-yönlendirme kapasitesinin güçlü olmasını gerektir (Black, 2010).

Bununla birlikte, yukarıda sıralanan bu özelliklerin salt bir düzenlemede ne ölçüde yer aldığının tespiti, her zaman "risk" kavramının yer aldığı açık normatif ifadelerle bağlı olmayıp düzenlemenin yapısal işleyişinin yahut ilişkili düzenlemelerin birlikte incelenmesini gerektirebilmektedir. Bu husus, hesap verebilirlik ilkesiyle doğrudan bağlantılı olduğundan hesap verebilirlik ilişkisiyle birlikte değerlendirilmelidir.

Öte yandan, risk temelli yaklaşımın, salt bir düzenlemenin hükümlerinden değil, birbiriyle işlevsel bütünlük içindeki birden fazla düzenleyici işlemin birlikte (kümülatif) etkisinden de kaynaklanabileceği

⁴ *Ex ante* yaklaşım; geleceğe yönelik bir durumun gerçekleşmesinden önce tahmin edilmesine yönelik varsayımsal olarak ileriye dönük yaklaşımdır (Black's Law Dictionary, 8th ed. 2004).

değerlendirilmektedir. Bu durum, özellikle bankacılık gibi risk yönetiminin faaliyetin özüne içkin olduğu sektörlerde yer bulabilmektedir. Zira bu tür sektörlerde, kendine özgü düzenlemenin -somut olayda bankacılık sırrına ilişkin hükümlerin- risk temelli yaklaşımı tek başına salt bir düzenlemede açık biçimde ortaya koymadığı durumlarda dahi, bu düzenlemenin içine yerleştiği genel risk yönetimi çerçevesinin katkısıyla fiilen risk temelli bir yapının kümülatif olarak ortaya çıkması mümkün olabilecektir.

3.4. Risk Temelli Yaklaşım ve Hesap Verebilirlik İlişkisi

Risk temelli yaklaşımla yakından ilişkili olan ve düzenlemelerde önemli bir yer tutan bir diğer ilke hesap verebilirliktir. Özellikle düzenleyici otoriteler tarafından getirilen kurallara uyumun sağlanıp sağlanmadığının etkin şekilde denetlenebilmesi ve gerçekleştirilen işlemlerin düzenlemelere uygunluğunun ortaya konulabilmesi bakımından hesap verebilirlik yaklaşımına ihtiyaç duyulmaktadır (Kaya, 2020). Bu ilkenin mevzuatta somutlaşması, düzenlemelerin muhataplarının sorumluluğunun belirlenmesi bakımından da önem taşımaktadır (Gellert, 2020).

Sırların niteliğindeki verilerin korunması bakımından hesap verebilirlik ilkesi, verilerin korunmasına ilişkin yükümlülüklerin yerine getirilip getirilmediğine ilişkin ispat yükünün veri sorumlusuna ve/veya veri işleyenlere ait olmasını ifade etmektedir (Tokmakçı, 2023). Bu durum, veri sorumlularının veri işleme faaliyetlerinin ilgili ilkelere uygunluğunu izlemelerini, bu uyuma ilişkin kayıtları tutmalarını ve gerektiğinde bu kayıtları ortaya koyabilmelerini gerektirmektedir. Bu yönüyle hesap verebilirlik, ihlallerin ortaya çıkmasını önlemeye veya risklerin gerçekleşme ihtimalini azaltmaya hizmet eden bir mekanizma olarak değerlendirilebilir (Kaya, 2020). Bu nedenle, risklerin belirlenmesi, analiz edilmesi ve buna uygun tedbirlerin ortaya konulmasıyla bu süreçle ilişkin araçların açık şekilde belirlenmesi, hesap verebilirliğin etkin şekilde işletilebilmesi bakımından önemlidir.

Nitekim, son dönemde AB nezdinde çıkarılan düzenlemelerde, riskin ilgili aktörler tarafından değerlendirilmesi ve buna bağlı olarak sorumluluğun da bu aktörlere yüklenmesi yaklaşımının benimsenerek yer bulduğu görülmektedir. Örneğin, GDPR m.5/f.2 hükmü uyarınca veri sorumluları kişisel verilerin işlenmesine ilişkin ilkelere uyumdan sorumlu tutulmakta, m.35 hükmü uyarınca yüksek riskli bir işleme faaliyeti için veri koruma etki değerlendirmesinin yapılması öngörülmekte; benzer şekilde örneğin Artificial Intelligence Act (AI Act) m.21 hükmü kapsamında, yapay zeka sistemlerine ilişkin yükümlülükler uyumun gösterilebilmesi amacıyla gerekli bilgi ve belgelerin saklanması öngörülmektedir.

Diğer taraftan, Madde 29 Veri Koruma Çalışma Grubunun 2014 yılında yayınladığı veri koruma yasal çerçevelerinde risk temelli yaklaşımın rolüne ilişkin açıklamada (Art. 29 WP 218, 2014), veri işleme faaliyetinin yarattığı risk düzeyine bağlı olarak farklı seviyelerde hesap verebilirlik yükümlülükleri öngörülebileceği ifade edilmiştir. Bu yaklaşım, risk temelli düzenleme anlayışı çerçevesinde, farklı risk seviyeleri için farklı yoğunlukta yükümlülükler getirilmesini mümkün kılmaktadır. Bu yönüyle, risk temelli yaklaşımla hesap verebilirlik arasında doğrudan ve tamamlayıcı ilişki bulunmaktadır.

Bu noktada ifade etmek gerekir ki, bir düzenleme çerçevesinin risk temelli nitelik taşıyıp taşımadığının belirlenmesi, yalnızca mevzuatta "risk" kavramının açıkça zikredilmesine bağlı değildir. Zira, risk temelli yaklaşımın temel unsurunu "kuralların değil risklerin" oluşturduğu, risk temelli bir düzenlemenin çıkış noktasının, uyulması gereken kurallar değil yönetilmesi gereken riskler olduğu (Black, 2010) dikkate alındığında; düzenlemenin risk temelli olup olmadığı değerlendirmesinde getirilen hükümlerin uygulama alanı ve varsa diğer ilişkili düzenlemelerle birlikte değerlendirme yapılması faydalı olacaktır. Nitekim, GDPR bakımından "risk temelli yaklaşım" kavramının tamamen yer almadığı, bununla birlikte söz konusu yaklaşımın, hesap verebilirlik ilkesi ve bu ilkeye bağlı mekanizmalar aracılığıyla düzenlemenin bünyesinde somutlaştığı ifade edilmektedir (Gellert, 2020).

Bu çerçevede, düzenlemenin risk temelli nitelik taşıyıp taşımadığının tespitinde belirleyici olanın, kavramsal etiketinin varlığı değil, düzenlemenin işleyiş yapısı ve içerdiği mekanizmalar olduğu değerlendirilmektedir. Risk değerlendirme yetkisinin düzenleyici otoritenin ön iznine değil, düzenlemeye tabi aktörün somut olay bazındaki değerlendirmesine bırakılması; ölçülülük ve gereklilik ilkelerinin önceden belirlenmiş bir kuralın mekanik uygulanması olarak değil, her olayda yeniden yapılması gereken bir risk değerlendirmesi olarak işlev görmesi bu kapsamda birer ölçüt olabilecektir. Yine, risk değerlendirmesinin kurumsal olarak risk yönetiminin parçası olarak sistematik olarak gerçekleştirilmesi ve alınan kararların kayıt altına alınarak gerektiğinde yetkili otoriteye sunulabilir, yani hesap verebilir nitelikte olması da düzenleme çerçevesinin fiilen işleyen risk temelli bir yapının söz konusu olup olmadığının tespitinde ölçüt olarak değerlendirilebilecektir. Bundan hareketle, söz konusu ölçütlerin varlığı durumunda risk temelli yaklaşım kavramını açıkça içermese dahi işlevsel açıdan risk temelli bir yapı sergilediği kabul edilebilecektir.

4. Risk Temelli Regülasyon Yaklaşımı Çerçevesinde Veri Koruma Düzenlemelerine Bakış

4.1. Genel Çerçevede Kişisel Verilerin Korunması Düzenlemelerinin Yaklaşımı

Kişisel verilerin korunmasına ilişkin düzenlemelerin temel amacı, veri sahibinin korunmasıdır (Çekin, Berktaş, v.d., 2023; Aşıkoğlu, 2018). Bilgiye erişimin artmasıyla bireylerin menfaatlerinin ve kişilik hakkının zarar görmemesi ihtiyacı, kişisel verilerin korunmasını düzenlemelere konu hale getirmiştir (Ayözger Öngün, 2018). Bu kapsamda, veri işleme ilkeleri, işleme şartları, veri aktarımı ve ilgili kişi hakları gibi hususlar düzenleme altına alınmakta (Bilir, 2023), veri sorumlularının veri işleme faaliyetlerinden kaynaklanabilecek riskleri değerlendirmesi, bu risklere göre karar alması ve riski en aza indirecek şekilde gerekli tedbirleri uygulaması öngörülmektedir.

Bununla birlikte, veri işleme faaliyetlerinde riskin tamamen ortadan kaldırılması her zaman mümkün olmayabilir. Özellikle verilerin yurt dışına aktarılması gibi durumlarda, farklı hukuk sistemleri nedeniyle verinin sonraki kullanımına ilişkin risklerin tümüyle bertaraf edilmesi güçtür. Veri işleme faaliyetinin tamamen sonlandırılması bir seçenek olsa da ciddi aksaklıklara yol açabileceğinden, uygulamada daha çok riskin makul ölçüde azaltılması ve kontrol altına alınması hedeflenmektedir (Bilir, 2023). Zira, riskin varlığını faaliyetin engeli kabul etmek, faaliyetin hiç gerçekleştirilememesi anlamına gelecektir. Bu açıdan kişisel verilerin korunması, veri işlemenin yasaklamayı değil (Başar, 2020), belirli esaslar dahilinde olası zarardan korunmayı amaçlar.

Bu açıdan, risk temelli yaklaşımın esasen bu ihtiyaca cevap verdiği değerlendirilmektedir. Zira söz konusu yaklaşım, düzenlemeye konu faaliyetlerin doğurabileceği risklerin önceden değerlendirilmesine, bu değerlendirme sonucuna göre önceliklerin belirlenerek hareket edilmesine imkân sağlayacağından, netlik sağlamakla birlikte katı yahut keskin sonuçlar doğuracak şekilde kural temelli düzenleme yaklaşımının olumsuzlukları da bertaraf edilebilecektir.

Veri koruma mevzuatı bakımından GDPR, risk temelli regülasyon örneğini oluşturmaktadır (Çekin, Berktaş, v.d., 2023). GDPR'da veri sorumlularının, veri işlem faaliyetinin niteliği, kapsamı ve doğabilecek riskleri dikkate alarak hareket etmesi öngörülmüştür. GDPR m. 24 "*Responsibility of the controller*" hükmü uyarınca, uygun teknik ve organizasyonel tedbirleri alınması, GDPR m. 35 "*Data protection impact assessment*" hükmü kapsamında yüksek riskli işlemler için veri koruma etki değerlendirmesi yapılması, işlem güvenliği kapsamında farklı risklerin dikkate alınması ve riske uygun güvenlik düzeyinin sağlanmasına ilişkin m. 32 hükmü uyarınca ise, risk düzeyine uygun güvenlik tedbirlerinin uygulanması gerekmektedir. Bu düzenlemeler, veri koruma hukukunda risklerin tespiti ve bunlara uygun tedbirlerin alınmasının esas alındığını göstermektedir.

Bu noktada, GDPR'daki risk kavramının yalnızca veri sahiplerinin hak ve özgürlüklerine yönelik riskleri değil, aynı zamanda düzenlemeye uyumsuzluk ihtimalini de kapsadığı ifade edilmektedir (Gellert, 2018). Uyumsuzluk düzeyinin artması, veri sahiplerinin maruz kalabileceği riskleri de artıracığından, uyumsuzluk ihtimalinin ortadan kaldırılması açısından verinin işlenmesi sırasında gerekli risk değerlendirmelerinin yapılması önemlidir. Bu açıdan, veri işleme faaliyetlerinin nasıl yürütüleceğine ilişkin değerlendirme sorumluluğunun veri sorumlularına bırakılması ve düzenleyici otoritelerin rolünün daha çok gözetimle sınırlı tutulması GDPR'ın önemli özelliklerinden biridir (Gonçalves, 2019; Kaya, 2020).

Diğer taraftan, veri sorumlularının işlenen verilerden dolayı sorumluluğunun ortaya konulması hesap verebilirlik ilkesi çerçevesinde şekillenmekte ve veri koruma yükümlülüklerinin etkin şekilde uygulanmasını sağlamaktadır (Gellert, 2020). GDPR m. 5 ve m. 30 hükümleri uyarınca veri sorumluları tarafından veri işleme faaliyetlerine ilişkin ilkelere uyum sağlanması, veri işleme faaliyetine ilişkin tüm kayıtların tutulması ve talep edildiğinde denetim merciine bunların sunulması gerekmektedir. Bu yönüyle sorumluluk ilkesi olarak yer bulan hesap verebilirlik ilkesinin (Oğuz, 2018) risk temelli düzenlemenin ayrılmaz bir parçası olduğu görülmektedir.

Türk hukukundaki temel düzenleme olan KVKK, kişisel verilerin işlenmesinde bireylerin temel hak ve özgürlüklerini korumayı amaçlamakta ve bu alandaki temel hukuki çerçeveyi belirlemektedir (Taştan, 2017). Ancak KVKK'da risk temelli yaklaşım ve hesap verebilirlik ilkesi, GDPR'da olduğu gibi açık ve sistematik bir şekilde düzenlenmemiştir. KVKK'da kişisel verilerin işlenmesine ilişkin gelen ilkeler (hukuka uygunluk, doğruluk ve güncellik, amaçla sınırlılık ve ölçülülük, sınırlı süreyle muhafaza) belirlenmiş olmakla birlikte, veri sorumlularının risk değerlendirmesi yapmasına yönelik açık araçlar ve mekanizmalar sınırlı düzeydedir.

Söz konusu hükümlerin uygulanmasına yönelik uyumun gösterilmesi ve veri güvenliğinin sağlanması veri sorumlusu ve veri işleyenin sorumluluğuna bırakılmış olmakla birlikte yukarıda GDPR bağlamında anılan mekanizmalara KVKK'da yer verilmemiştir (Karatay, 2023). Nitekim, temel hesap verebilirlik araçlarından olan ve hak ve hürriyetlerin ihlal edilme riskinin tanımlanarak azaltılması amacıyla yapılması zorunlu tutulan veri koruma etki değerlendirmesiyle (Taştan, 2017), veri koruma görevlisine ve davranış kurallarına ve buna ilişkin taahhütlerin belirlenmesine ilişkin düzenlemelere KVKK'da yer verilmemiştir (Kaya, 2020; Oğuz, 2018).

Aynı zamanda, KVKK tarafından Veri Sorumluları Sicili'nin (VERBİS) hesap verebilirlikle ilişkilendirilmesine rağmen, VERBİS'in kapsam ve içerik itibarıyla veri işleme faaliyetlerinin risk temelli değerlendirmesini bütüncül şekilde yansıtmaması, bu sistemin tam anlamıyla bir hesap verebilirlik aracı olarak değerlendirilmesini güçleştirmektedir (Kaya, 2020). Bu açıdan KVKK hükümleri incelendiğinde KVKK'nın, risk temelli yaklaşımın temel araçları bakımından sınırlı bir yapı düzenlediği görülmektedir. Özellikle GDPR'da açıkça düzenlenen veri koruma etki değerlendirmesi, risk temelli güvenlik yükümlülükleri ve risk düzeyine göre farklılaştırılmış yükümlülük mekanizmalarının KVKK'da sistematik bir bütünlük içerisinde yer almaması bu durumu ortaya koymaktadır.

Ayrıca, veri sorumlularının risk değerlendirmelerini belgeleme ve bu değerlendirmeleri denetime hazır bulundurma yükümlülüğünün KVKK'da açık bir şekilde düzenlenmemiş olması da hesap verebilirlik ilkesinin uygulama araçları bakımından sınırlı kalmasına neden olmaktadır. Bununla birlikte, Veri Sorumluları Sicili Hakkında Yönetmelik uyarınca, VERBİS'e kayıtlı veri sorumluları, gerçekleştirmekte oldukları veri işleme faaliyetlerini, kişisel veri işleme amaçları, veri kategorisi ve alıcı gruplarıyla ilişkilendirilmiş bir kişisel veri işleme envanteri hazırlamakla yükümlüdür. Bu yönüyle KVKK, risk temelli yaklaşımın sonuçlarını dolaylı olarak içermekle birlikte, bu yaklaşımın araçlarının tümünü açık ve sistematik bir şekilde düzenleyen bir model ortaya koyamamaktadır.

Ancak, yasal düzenleme söz konusu olmamakla birlikte Kişisel Verileri Koruma Kurumu tarafından, hesap verebilirlik ilkesine yönelik yaklaşıma ilişkin bağlayıcı şirket kuralları ve açıklamalarında, veri sorumlularının söz konusu kurallara uyum sağlanması noktasında yükümlü ve sorumlu olduğundan bahisle, veri işleme faaliyetlerinin kaydının tutulması ve KVKK tarafından istenildiğinde kayıtların sunulması, kişilerin temel hak ve özgürlükleri bakımından yüksek riskin söz konusu olduğu işleme faaliyetleri için risk analizinin gerektiğini ifade etmesi, bu analiz sonucunda yüksek risk tespiti ve gerekli tedbirlerin alınmamış olması halinde KVKK'ya başvurulmasını vurgulaması dolayısıyla, KVKK'nın da hesap verebilirliği GDPR yaklaşımıyla yorumladığı görülmektedir (Kaya, 2020).

Bu çerçevede, KVKK'da risk temelli yaklaşımın benimsenmesine yönelik araçların bütüncül şekilde düzenlenmediği, ancak uygulama ve ikincil düzenlemeler aracılığıyla bu yaklaşımın giderek güçlendiği değerlendirilmektedir. Bu nedenle, risk temelli yaklaşımın açık normatif araçlarla desteklenmesi, verilerin korunması bakımından risk kültürünün yerleştirilmesi, oluşabilecek ihlalin önlenmesi bakımından bilinçlendirme açısından önem arz etmektedir (Bayram, 2022). Bu durum, risk temelli yaklaşımın genel veri koruma rejiminde sınırlı kalmasına karşın, sektörel düzenlemelerde daha belirgin şekilde ortaya çıkabileceğini göstermektedir.

4.2. Türkiye’de Bankacılık Verilerinin Korunmasına Yönelik Regülasyon Yaklaşımı

4.2.1. Kavramsal Açıdan Bankacılık Sırları

Sır, genel olarak herkes tarafından bilinmeyen, ancak açıklanması halinde sahibinin hak ve menfaatlerine zarar getirebilecek nitelikte olan bilgidir (Alıcı, 2017). Bankacılık sırrı hem banka sırrı ve hem müşteri sırrını kapsayıcı nitelikte oluşan bir üst kavram olarak değerlendirilmektedir.

Kanunda kavramsal tanımlamasına yer verilmemiş ise de banka sırrı, bankanın kendi faaliyetleri kapsamında oluşan ve açıklanması halinde banka açısından olumsuz sonuçlar doğurabilecek bilgileri ifade etmektedir. Bu kapsamda bankanın mali durumu, hizmetleri, kurumsal yönetim yapısı, politikaları ve stratejilerine ilişkin bilgilerin banka sırrı kapsamında değerlendirildiği kabul edilmektedir (Sözügüzel, 2023; Alıcı, 2017). Müşteri sırrı ise, Kanunda 2020’de yapılan değişiklikte, bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler olarak tanımlanmış olup bu yönüyle müşteri sırrı, esas itibarıyla bankacılık faaliyetlerinden doğan müşteri verilerini kapsamaktadır.

Bu noktada ifade etmek gerekir ki, kimliği belirli veya belirlenebilir gerçek kişi müşteriye ait bankacılık verileri elbette ki müşteri sırrı niteliğinde bir kişisel veri olmakla birlikte, bankacılık sırrı kapsamında tüzel kişi müşterilere ait veriler kişisel veri olarak nitelendirilmemekte ise de (Özcan, 2020) müşteri sırrı niteliğindedir (Arslanhan, 2024). Bu kapsamda, müşteri sırrının tüzel kişilere ait bilgileri de kapsamı nedeniyle, kişisel veri kavramına kıyasla daha geniş bir içeriğe sahip olduğu kabul edilmektedir (Güven, Irmak, v.d., 2023).

Diğer taraftan, bankaların faaliyetlerini emin bir şekilde sürdürebilmesi, yalnızca mali yapılarının sağlamlığına değil, güven ve itibar kurumu olarak algılanmalarına da bağlıdır (Altay, 2019). Bankayla kurulan ilişki çerçevesinde paylaşılan bilgilerin korunacağına dair güven önemli bir unsurlardan birini oluşturmaktadır. Bu nedenle, müşteriye ait bilgilerin korunması, bankaların temel davranış yükümlülüklerinden biri olarak kabul edilmektedir (Güven, Irmak, v.d., 2023).

Bu bağlamda, bankacılık sırrının korunması, bankacılık faaliyetlerinde güven ve istikrarın sağlanması açısından merkezi bir rol oynamakta ve bu nedenle ilgili düzenlemelerin bankacılık mevzuatı

içerisinde yer alması kaçınılmaz görülmektedir (Kaya, 2024). Bununla birlikte, bu düzenlemelerde, risk temelli yaklaşım kavramsal açıdan açık bir şekilde ifade edilmese de gerek bankacılık sisteminin risk yönetimi düzenlemeleri, gerek sırların paylaşım usullerinin ve karar alma mekanizmalarının riskin değerlendirilmesine göre kurgulanması, bankacılık sırlarının korunmasında riskin ön planda tutulduğunu göstermektedir.

4.2.2. Bankacılık Sırlarına İlişkin Düzenlemelerin Genel Çerçevesi

4.2.2.1. 5411 Sayılı Bankacılık Kanunu

Risk temelli düzenleme yaklaşımı çerçevesinde bankacılık sırlarının korunmasına ilişkin ulusal mevzuatın değerlendirilebilmesi için, konuya ilişkin bankacılık mevzuatında yer alan düzenlemelerin genel hatlarıyla ele alınmasında fayda görülmektedir. Bu doğrultuda, ülkemiz mevzuatı bakımından bankacılık faaliyetinin ana düzenlemesini Kanun ve alt düzenlemeleri oluşturmaktadır. Kanunun sırların saklanmasıyla ilişkin hükümleri ise, esas itibarıyla sırların paylaşımına ilişkin genel sınırlamalara ve bunların istisnalarına ilişkin çerçeveyi düzenlemekte olup, paylaşım dışındaki veri işleme faaliyetleri bakımından özel bir hüküm içermemektedir. Bu nedenle verilerin paylaşılması dışındaki işleme faaliyetleri bakımından genel düzenleme niteliğindeki KVKK'nın uygulama alanı bulması söz konusu olacaktır (Dülger, 2021). Kişisel verilerin korunmasına ilişkin genel rejimi KVKK oluştururken, Kanunun 73'üncü maddesi, bankacılık sırrı niteliğindeki kişisel veriler bakımından özel hüküm niteliği taşımakta ve genel rejime kıyasla bankacılığa özgü olarak daha özel bir koruma düzeni sağlamaktadır. Nitekim 2020'de gerçekleştirilen değişikliğin gerekçesinde de sır kapsamındaki müşteri bilgileri için Kanun hükümlerinin özel nitelikli kanun hükümleri olarak ele alınması gerektiğinin netleştirildiği belirtilmiştir.

KVKK kapsamında açık rıza kuralı olarak bir işleme/aktarma sebebi sayılırken, Kanunun 73'üncü maddesinde sır niteliğindeki bilgilerin "açık rıza alınsa dahi, müşteriden gelen bir talep/talimat olmaksızın" yurt içinde veya yurt dışındaki kişilerle paylaşılacakları düzenlenmiştir. Dolayısıyla, KVKK'da öngörülen yurt içi ve yurt dışı aktarıma ilişkin hükümler etkisiz hale gelerek (Taştan ve Saruhan, 2020) KVKK'da yer alan açık rızadan daha aktif bir irade beyanı aramaktadır. KVKK'da 2024 yılında yurt dışına veri aktarımı bakımından yapılan değişikliklerle açık rızanın istisnai bir aktarım şartına dönüştürülmesi, açık rızaya dayalı modelin tek başına yeterli görülmediği bir anlayışa işaret etmekle birlikte; gerek 6698 sayılı Kanun uyarınca kişisel verilerin yurtiçi/yurtdışı aktarımına ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulması gerek 73'üncü madde düzenlemesi, bankacılık sırrının kişisel verilerin paylaşımı bakımından KVKK'nın genel sistematüğinden bilinçli biçimde ayrıldığını göstermektedir.

Bankacılık sırlarına ilişkin temel düzenleme ise, Kanunun 73'üncü maddesinde yer almakta olup, sır niteliğindeki bilgilerin kapsamı, paylaşım koşulları, bu bilgilerin korunması yükümlülüğünün kapsamı ve istisnalar bu maddede düzenlenmiştir. Buna göre, bankacılık sırlarının korunmasına ilişkin genel düzenleme, sıfat ve görevleri dolayısıyla bankalara veya müşterilere ait sırları öğrenenlerin, bu sırların bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklanamaması olup 2020 yılında anılan maddede yapılan değişiklikle birlikte müşteri sırrı bakımından ise, yapılan değişikliğe ilişkin eleştiriler bulunmakla birlikte (Taştan ve Saruhan, 2020; Dülger ve Bakdur, 2021), istisnalar dışında müşterinin talep veya talimatının bu bilgilerin paylaşımı için gerekli olduğu düzenlenmiştir. Bu düzenleme KVKK'nın açık rızaya yönelik yaklaşımından farklılık arz etmekte ise de söz konusu farklılık bankacılık sektörüne yönelik genel-özel hüküm ilişkisi bağlamında değerlendirilmektedir (Çatakoğlu Aydın, 2024). Dolayısıyla, müşterinin talep veya talimatı dışında, ancak kanuni istisnalarda ve kanunen yetkili kılınan mercilerle paylaşım mümkün olabilecek olup bilgilerin paylaşımı, amaçla sınırlı olma ve amacın gerektirdiği kadar veriyi içerecek şekilde ölçülü olma ilkeleri çerçevesinde gerçekleştirilmek zorundadır.

Öte yandan, anılan Kanun'un 73'üncü maddesinin dördüncü fıkrasında ise, müşteri talebi veya kanuni yetki halleri dışında, belirli şartlar altında istisnai veri paylaşımlarına da izin verilmektedir. Bu kapsamda, yalnızca belirli amaçlarla sınırlı olmak ve gizlilik sözleşmesi yapılması kaydıyla, hizmet alımları gibi bazı hususlara yönelik veri paylaşımları sır saklama yükümlülüğünün dışında tutulmuştur.

Bu çerçevede, bankacılık sırlarının paylaşımı Kurul'un ön iznine tabi bir işlem olarak düzenlenmemiştir. Paylaşımın hukuka uygun olup olmadığına ilişkin değerlendirme, doğrudan banka tarafından yapılmakta olup banka, paylaşımın kapsamını, amacını ve doğurabileceği riskleri somut olay bazında değerlendirerek paylaşıma karar verebilecektir. Bu düzenleme, veri paylaşımına ilişkin karar alma süreçlerinin merkezi bir otoritenin ön iznine tabi kılınmaması ve değerlendirme yetkisinin doğrudan düzenlemeye tabi aktörlerden olan bankalara bırakılması nedeniyle, risk temelli yaklaşımın temel unsurlarından biri olan merkezi olmayan risk değerlendirmesine işaret etmektedir. Bu yönüyle bankacılık sırrı rejiminde veri paylaşımı, önceden belirlenmiş kuralların mekanik uygulanmasından ziyade, her bir somut olay bakımından gerçekleştirilen bir risk değerlendirme sürecine dayanmaktadır.

Ancak belirtmek gerekir ki, Kanun'un 73'üncü maddesi uyarınca, ekonomik güvenliğe ilişkin yapılacak değerlendirmeler sonucunda müşteri veya banka sırrı niteliğindeki verilerin yurt dışına aktarımı Kurul tarafından sınırlandırılabilir. Bu kapsamda, sırların aktarımına ilişkin usul ve esasların belirlenmesi ve gerektiğinde sınırlandırılması konusunda Kurul'a yetki tanınmış olup özellikle ülke ekonomisine veya finansal piyasaların güven ve istikrarına, kredi sisteminin etkin çalışmasına tehlike teşkil edebilecek hallerde bu yetkinin kullanılabilmesi mümkündür.

4.2.2.2. Sır Yönetmeliği ve 2022/1 Sayılı Genelge: Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmeliğin Uygulanmasına İlişkin Açıklamalar

Kanunun 73'üncü maddesine dayanılarak 2021'de çıkarılan Sır Yönetmeliğiyle, bankacılık sırlarının saklanması ve özellikle sır niteliğindeki bilgilerin paylaşımına ilişkin usul ve esaslar ikincil mevzuat düzeyinde ayrıntılı olarak düzenlenmiştir (Dülger, 2021). Yönetmelik hükümleri, genel itibarıyla Kanunla paralel olmakla birlikte, uygulamaya yönelik daha somut düzenlemeler içermektedir.

Sır Yönetmeliği incelendiğinde, sır niteliğindeki bilgilerin paylaşımına ilişkin yaklaşımın birtakım hususlar üzerinden genel çerçevede şekillendiği görülmektedir. Bu kapsamda, sırların paylaşımına ilişkin temel kural olarak müşteri talep veya talimatı aranmakta ve müşteriden gelen bir talep veya talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılması ve bunlara aktarılması mümkün bulunmamaktadır. Bu kural dışında ise gerek Kanunda gerek diğer kanunlarda açıkça paylaşıma yetkilendirilen hallerde sır niteliğindeki bilgilerin paylaşımı söz konusu olabilmektedir.

Diğer taraftan, sır niteliğindeki bilgilerin paylaşımının mümkün olduğu hallerde ise; veri minimizasyonu ilkesine uygun hareket edilmesi, mümkün olduğu ölçüde verinin ilgili kişiyle ilişkilendirilemeyecek hale getirilmesi, istisnai paylaşımlar bakımından gizlilik sözleşmesi yapılması, paylaşımın belirli ve sınırlı amaçlarla gerçekleştirilmesi, gerekli teknik ve idari tedbirlerin alınması⁵, sadece banka sırrı içeren bilgilerin yönetim kurulu kararıyla paylaşılabilmesi ve bu yetkinin belirli çerçevede devredilebilmesi şeklindeki esaslara uygun hareket edilmesi gerekmektedir.

Bu unsurlar dikkate alındığında, verilerin korunmasına yönelik riskleri minimize etmek amacıyla yalnızca amaca odaklı, mümkün olduğu kadarıyla en az veri kopyası oluşturularak ve amacın gerektirdiği kadar verinin paylaşımının mümkün kılındığı, veri paylaşımına ilişkin değerlendirme ve karar alma sürecinin doğrudan bankaların sorumluluğuna bırakıldığı ve paylaşımın merkezi bir otoritenin ön iznine tabi kılınmadığı görülmektedir. Bu yapı, veri paylaşımına ilişkin riske dikkate edilerek kararların

paylaşımına konu edilebilecek somut olay bazında değerlendirilmesini gerektirmesi ve değerlendirme yetkisinin düzenlemeye tabi aktörlere bırakılması nedeniyle, sır niteliğindeki bilgilerin paylaşılması düzenlemesinin çerçevesinin risk temelli yaklaşımın temel unsurlarıyla örtüştüğü değerlendirilmektedir. Bu çerçevede, Sır Yönetmeliği kapsamında sır niteliğindeki bilgilerin paylaşılması, önceden belirlenmiş katı kuralların uygulanmasına dayalı olmaktan ziyade, her bir işlem bakımından gerçekleştirilen bir risk değerlendirmesine dayalı olarak şekillenmektedir.

Bunun yanında, sır niteliğindeki bilgilerin paylaşımına ilişkin olarak; gizlilik sözleşmesi, paylaşım amacı, alınan teknik ve idari tedbirlerle aktarım yapılan taraflara ilişkin bilgilerin belirli dönemlerde BDDK'ya raporlanması ve müşteri kimliğini belirli veya belirlenebilir kılan paylaşımların banka nezdinde denetime hazır şekilde bulundurulması zorunluluğu getirilmiş olup gerçekleştirilen paylaşımların hesap verilebilir olması gerektiği ön plana alınmıştır. Ayrıca, veri paylaşımlarını koordine etmek ve gelen talepleri değerlendirmek üzere bankalar bünyesinde Bilgi Paylaşım Komitesi kurulması öngörülmüş; bu komitenin değerlendirmelerinin kayıt altına alınması ve gerektiğinde BDDK'yla paylaşılması düzenlenmiştir (Güven, Irmak, v.d., 2023).

Sır Yönetmeliği sonrasında uygulamada ortaya çıkabilecek tereddütlerin giderilmesi amacıyla 2022/1 sayılı Sır Genelgesi yayımlanmıştır. Genelge, uygulamada karşılaşılan sorunlara konu bazı açıklamalar getirmekte ve özellikle bankaların risk yönetimi kapsamında ana ortakları veya grup şirketleriyle yapacakları veri paylaşımlarının kapsamının bankalar tarafından değerlendirilmesine yönelik önemli yönlendirmeler içermektedir. Bu kapsamda, veri paylaşımına ilişkin risklerin belirlenmesi ve bu risklerin gerekçelendirilmesi yükümlülüğünün bankalara bırakıldığı görülmekte olup, bu durum risk temelli yaklaşımın uygulama düzeyinde de benimsendiğini göstermektedir.

4.2.3. Bankacılık Mevzuatında Yer Alan Bazı Diğer İkincil Düzenlemeler

Bankacılık sırlarının korunmasına ilişkin düzenlemeler yalnızca Kanunun 73'üncü maddesi ve buna ilişkin alt düzenlemelerle sınırlı olmayıp, bankacılık mevzuatında yer alan diğer ikincil düzenlemelerle de desteklenmektedir. Bu kapsamda özellikle risk yönetimine ilişkin düzenlemeler, bankacılık verilerinin korunması bakımından dolaylı ancak önemli bir çerçeve sunmaktadır.

Örneğin, *Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik* ve risk yönetimiyle ilgili iyi uygulamaları ortaya koymak üzere BDDK tarafından yayımlanan *Operasyonel Riskin Yönetimine İlişkin Rehber* hükümleri uyarınca bankalar, faaliyetlerinden kaynaklanan riskleri tanımlamak, ölçmek, izlemek ve yönetmekle yükümlüdür. Bu kapsamda operasyonel risk; yetersiz veya başarısız iç süreçler, insan unsuru, sistemler veya harici olaylardan kaynaklanan ve hukuki riskleri de kapsayan zarar ihtimalini ifade etmektedir. Bu çerçevede kişisel ve ticari verilerin korunmasına ilişkin yükümlülüklerle uyumsuzluk, bankalar açısından operasyonel risk kapsamında değerlendirilmekte ve veri güvenliği ihlalleri doğrudan risk yönetimi sisteminin konusu haline gelmektedir.

Bu bağlamda, bankacılık sırlarının korunmasına ilişkin yükümlülüklerin ihlali yalnızca veri güvenliği açısından bir risk doğurmamakta; aynı zamanda bankalar bakımından uyum riski, operasyonel risk ve itibar riski gibi birden fazla risk kategorisiyle ilişkilendirilecektir. Bu nedenle bankalar, veri paylaşımına ilişkin kararlarında yalnızca mevzuat uyumunu değil, aynı zamanda bu risklerin yönetimini de dikkate almak durumundadır. Özellikle büyük ve karmaşık yapıya sahip bankalar, geçmiş ihlal vakalarından doğan zararları da dikkate alarak risk ölçüm ve değerlendirmeleri yapmakta ve buna göre risk iştahlarını belirlemektedir. Bu çerçevede, veri koruma yükümlülüklerine aykırı işlem veya paylaşımlar, bankaların kabul edebileceği risk sınırlarının dışında kalacaktır.

⁵ 2022/1 sayılı Sır Genelgesi'nin "2.7." başlığı altındaki açıklamada, "gerekli teknik ve idari tedbirler" ifadelerinden, genel anlamda veri konusunda genel kabul görmüş standart ve çerçeveler esas alınarak karşı tarafta alınabilecek teknik ve idari tedbirlerle de bu konulardaki BSEBY hükümlerinin karşılanması mümkün olduğu belirtilmiştir.

Bankacılık faaliyetlerinde kullanılan veriler, bankaların temel bilgi varlığını oluşturmakta olup bu verilerin korunması faaliyetin ayrılmaz bir unsurudur. Bu nedenle veri güvenliğine ilişkin risklerin yönetimi, bankacılık faaliyetlerinin sürdürülebilirliği açısından kritik öneme sahiptir. Bankaların, birer güven müessesesi oldukları da göz önüne alındığında, diğer tacirlere kıyasla ağırlaştırılmış bir özen yükümlülüğü içerisinde bulunduğu kabul edilmekte (Çatakoğlu Aydın, 2024) ve bu ağır özen sorumluluğu hali bankaların bilgi güvenliğinin sağlanması bakımından önem arz etmektedir (Arslanhan, 2024; Alımcı, 2022). Bu kapsamda Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (BSEBY), bilgi sistemlerinin yönetimi ve bu sistemlere ilişkin risklerin kontrolüne yönelik kapsamlı düzenlemeler içermektedir.

Söz konusu düzenlemeler uyarınca bankalar, verilerin işlendiği, saklandığı ve iletildiği ortamlarda gerekli güvenlik önlemlerini almak, bu önlemleri verinin gizlilik derecesine uygun belirlemek ve veri içeren ortamların kullanım dışı kalması halinde güvenli imhasını sağlamakla yükümlüdür (BSEBY m.9). Ayrıca, veri varlıklarının sınıflandırılması, envanter oluşturulması, güvenlik gereksinimlerinin belirlenmesi ve uygun kontrol mekanizmalarının tesisi de bankaların sorumluluğundadır (Sözügüzel, 2023). Bu yönüyle veri güvenliğinin sağlanamaması banka özelinde güvenin zedelenmesinden, bankacılık sisteminin güven ve istikrarına yönelik olabilecek kadar ciddi sorunlara yol açabilecek olup (Çatakoğlu Aydın, 2024; Alımcı, 2022) veri güvenliğinin sağlanmasına özellikle ağırlık verildiği görülmektedir.

Tüm bu düzenlemeler birlikte değerlendirildiğinde, bankacılık sırrının korunmasına ilişkin çerçevenin, verinin korunması amacının doğası gereği sınırlandırıcı bir yapıda olduğu değerlendirilse de veri paylaşımına ilişkin kararların önceden belirlenmiş katı kuralların mekanik uygulanmasına dayanmaktan ziyade, her somut olayın taşıdığı risklerin değerlendirilmesini esas alacağı görülmektedir. Bu yönüyle bankacılık mevzuatı, bilgi sistemlerine ilişkin risklerin yönetilmesi de dahil risk değerlendirmesini doğrudan düzenlemeye tabi aktörlere bırakan ve bu aktörlerin kararlarını çok boyutlu risk analizine dayandırmasını gerektiren yapısı itibarıyla, risk temelli yaklaşımın açık normatif bir model olarak değil, sektörel düzenlemelerin birlikte işleyişi aracılığıyla fiilen ortaya çıktığı bir alan olarak değerlendirilmektedir.

5. Bankacılık Sırlarının Korunması Düzenlemelerinin Risk Temelli Düzenleme Yaklaşımı Çerçevesinde Değerlendirilmesi

5.1. Risk Değerlendirme Yetkisinin Dağılımı: Düzenleyici Otorite ile Banka İlişkisi

Bankalar, faaliyetlerinin doğası gereği güven ve itibar temeline dayanan, yoğun bir risk yönetimi fonksiyonu üzerine kurulu kurumlardır. Bu nedenle, oluşturulan faaliyet yapısı bankacılık sektörüne ilişkin düzenlemelerin de kaçınılmaz olarak risk perspektifiyle şekillenmesini gerektirmektedir.

Risk temelli düzenleme yaklaşımının varlığı için, risk değerlendirme yetkisinin düzenleyici otoriteyle düzenlemeye tabi aktörler arasında ne şekilde dağıtıldığı önem arz etmektedir. Bu yaklaşımda, düzenleyici otoritenin tüm ihtimalleri önceden belirleyerek ayrıntılı kurallar koyması ve bunlara sonuç bağlamasından ziyade, düzenlemeye tabi aktörlere risk değerlendirmesi yapılabilmesine ilişkin belirli bir takdir alanı tanınmakta ve risk değerlendirmesi bu alan içerisinde ilgili aktörler tarafından gerçekleştirilmektedir. Bu çerçevede, bankacılık düzenlemelerinde bankaların risk değerlendirme yetkisi bakımından nasıl konumlandığının ortaya konulması önem taşımaktadır.

Kanunun 73'üncü maddesiyle buna dayanılarak çıkarılan ikincil düzenlemeler incelendiğinde, sır niteliğindeki bilgilerin paylaşımına ilişkin karar alma süreçlerinde doğrudan izin veya ön denetim mekanizmasının öngörülmediği; aksine, paylaşım esasları çizilerek değerlendirme yetkisinin büyük ölçüde bankalara bırakıldığı anlaşılmaktadır. Düzenlemeyi ilke temelinden ayırarak risk temelli kılan

unsur, bu takdir yetkisinin soyut ilkelere uygunluk değil, somut risk değerlendirmesi esas alınarak kullanılmasının öngörülmesidir. Nitekim bankalardan beklenen, paylaşımın yalnızca mevzuata şeklen uygunluğunu değil, amacını, kapsamını ve doğurabileceği riskleri somut olay bazında değerlendirerek hesap verebilir şekilde karar vermesidir.

Bu yapı, BDDK'nın ex ante kontrolüne dayalı klasik bir kural temelli sistemden ziyade, paylaşımın çerçevesi bakımından düzenlemeye tabi aktörlerin ex ante risk değerlendirmesine dayanan bir modelin benimsendiğini göstermektedir. Dolayısıyla bankacılık sırlarının korunmasına ilişkin düzenleme çerçevesi, risk değerlendirme yetkisinin ağırlıklı olarak bankalara bırakılması yönüyle, risk temelli düzenleme yaklaşımının temel unsurlarından birini açık biçimde yansıtmaktadır.

5.2. Bankacılık Sırlarının Korunmasına Yönelik Düzenlemelerde Fiilen Risk Temelli Yaklaşım Unsurları

Bir düzenlemenin çerçevesinin risk temelli nitelik taşıyıp taşımadığının belirlenmesi, yalnızca "risk" kavramının düzenleme metinlerinde açıkça yer almasına bağlı olmayıp düzenlemenin risk esaslı olup olmadığının değerlendirilmesini gerektirebilmektedir. Bu açıdan, 3.4. başlığı altında değerlendirildiği üzere, risk değerlendirme yetkisinin düzenlemeye tabi aktöre bırakılması, ölçülülük ve gerekliliğin somut olay bazında değerlendirilmesi, risk değerlendirmesinin genel risk yönetimi sistemi içerisinde sistematik olarak ele alınması ve alınan kararların hesap verebilir nitelikte olması, düzenlemenin risk esaslı niteliğinin belirlenmesinde ölçüt olarak esas alınmalıdır.

Bankacılık mevzuatında sırların saklanması ve paylaşımına ilişkin çerçeve çizilmekte, bu kapsamda KVKK'da yer alan veri işleme ilkelerine benzer şekilde, amaçla sınırlılık, ölçülülük ve gerekli kadar veriyle sınırlı paylaşım gibi ilkeler benimsenmektedir. Bu ilkeler, ilk bakışta kural temelli bir yapı izlenimi vermekte ise de bankaların her somut olay bakımından ayrı bir uygunluk değerlendirmesi yapmasını zorunlu kılması nedeniyle risk temelli yaklaşımın unsurlarını örtülü şekilde içermektedir.

Özellikle sır niteliğindeki bilgilerin paylaşımına ilişkin olarak getirilen "amaçla sınırlılık", "ölçülülük" ve "gerekli olan veriyle sınırlı paylaşım" ilkeleri, otomatik ve mekanik şekilde uygulanabilecek kurallar olmayıp, her paylaşımda kriterlerin sağlanıp sağlanmadığı değerlendirilmek durumundadır. Zira, örneğin bir paylaşım talebi bakımından kişilerin muhtelif bilgilerinin yanında müşteri kimliğinin belirli veya belirlenebilir kılınması gerekebilecek iken, bir başka paylaşımda müşteri bilgisinin her bileşenine ihtiyaç duyulmayabilmektedir. Keza, sır niteliğindeki bilginin paylaşılacağı tarafın niteliği de risklilik değerlendirmesini doğrudan etkilemektedir. Nitekim bir kamusal otoriteyle yapılacak paylaşım, hizmet alımı amacıyla yapılacak paylaşımın risklilik değerlendirmesi birbirinden farklıdır. Bu açıdan, her somut olay bazında paylaşımlara ayrı değerlendirme yapılmasını ve ilkelerin yansımalarının değerlendirilmesi gerekmektedir. Nitekim Sır Yönetmeliği'nin 6'ncı maddesi uyarınca, paylaşımın belirli bir amaca dayanması, bu amaçla sınırlı olması ve paylaşılan veri setinin tamamının bu amacın gerçekleştirilmesi için gerekli olduğunun gösterilebilir olması zorunlu tutulmuş olup her paylaşımın taşınması gereken şartların değerlendirilebilir ve hesap verilebilir olmasını gerekli kılmıştır.

Bu çerçeve, veri paylaşımına ilişkin kararların somut olay bazında değerlendirme yapılmasını gerektirmesi, risk temelli yaklaşımın temel unsurlarından biri olan duruma özgü değerlendirme ilkesini açık şekilde yansıtmaktadır. Ayrıca, Sır Genelgesi'nde de paylaşımın amacına hizmet eden veri setinin gerçekten gerekli olduğunun somut şekilde ortaya konulması gerektiği vurgulanarak, bu değerlendirmelerin gerekçelendirilmesi zorunlu tutulmuştur. Bu durum, yalnızca risk değerlendirmesini değil, aynı zamanda bu değerlendirmenin hesap verebilirliğini de gerekli kılmaktadır.

Bunun yanında, paylaşımın anonimleştirme veya toplulaştırma yöntemleriyle gerçekleştirilip gerçekleştirilemeyeceğinin değerlendirilmesi, paylaşım kapsamının belirlenmesi ve gerekli teknik ve

İdari tedbirlerin alınması gibi yükümlülükler de bankaların risk değerlendirmesi yapmasını gerektiren unsurlar arasında yer almaktadır.

Öte yandan, Sır Yönetmeliğiyle birlikte veri paylaşım süreçlerinin değerlendirilmesi ve kaydedilmesi amacıyla bankalar bünyesinde Bilgi Paylaşım Komitesi kurulması zorunlu tutulmuştur. Bu komitenin; asgari olarak, iç kontrol, uyum ve hukuk gibi farklı fonksiyonları temsil eden iş birimlerinden oluşması öngörülerek, veri paylaşımına ilişkin kararların farklı çalışma alanları bulunan banka birimleri tarafından çok boyutlu bir değerlendirme sürecine tabi tutulması amaçlanmıştır. Dolayısıyla düzenlemeler, risklerin yalnızca hukuki değil, operasyonel ve uyum boyutlarıyla birlikte değerlendirilmesini sağlayarak, risk temelli yaklaşımın kurumsal düzeyde içselleştirildiğini göstermektedir.

Bu yönüyle bankacılık sırrının korunmasına ilişkin düzenlemeler, her ne kadar "risk temelli yaklaşım" kavramını açıkça zikretmese de uygulamada bankaların somut olay bazında risk analizi yapmasını zorunlu kılmaktadır. Dolayısıyla bu düzenlemeler, risk temelli yaklaşımın açık bir normatif ifadeyle değil, sektörel bazda getirilen farklı mekanizmalar aracılığıyla hayata geçirildiği bir model olarak değerlendirilebilir.

5.3. Bankacılık Sektörüne İlişkin Risk Yönetimi Düzenlemeleriyle Bankacılık Sırlarının Korunmasına Yönelik Düzenlemeler Arasındaki İlişki

Bankacılık sırrının korunmasına ilişkin düzenlemelerin risk temelli yaklaşım bakımından değerlendirilmesinde, bu düzenlemelerin yalnızca kendi içeriğiyle değil, bankacılık sektörüne özgü genel risk yönetimi çerçevesiyle birlikte ele alınması gerekmektedir. Zira bankacılık faaliyetlerinde risk yönetimi, yalnızca finansal risklerle sınırlı olmayıp operasyonel ve uyum risklerini de kapsayan çok sayıda risk türlerini içerisinde barındıran geniş bir alanı ifade etmektedir.

Bu noktada, bankacılık faaliyetine özgü risk anlayışıyla verilerin korunmasına özgü risk anlayışı arasındaki kavramsal farklılığa değinmek gerekmektedir. Bu iki risk anlayışı koruma konusu menfaat bakımından değerlendirildiğinde; bankacılıkta risk yönetiminin esas aldığı finansal riskler makro bakış açısıyla öncelikle bankanın ve dolayısıyla finansal sistemin istikrarını hedeflerken, veri koruma hukukundaki risk temelli yaklaşım ilgili kişilerin temel hak ve özgürlüklerini esas almaktadır. Bu açıdan müşteri sırrına yönelik düzenlemeler de esasen müşteri menfaatinin korunmasına yönelik olup (Bağrıaçık, 2017) söz konusu farklılık göz ardı edilmemekte; aksine, bankacılık sırrı rejiminin risk temelli yapısı değerlendirilirken doğrudan dikkate alınmalıdır.

Bununla birlikte, bu kavramsal ayrımın varlığı, iki risk anlayışının bankacılık uygulamasında birbirinden farklı olduğu veya kopukluk gösterdiği anlamına gelmemektedir. Aksine, Türk bankacılık mevzuatında veri güvenliği ve gizliliğine ilişkin riskler operasyonel risk, uyum riski ve itibar riski kategorileri içinde değerlendirilerek, esasen bireyin korunmasına yönelik bir menfaati bankanın kurumsal risk yönetimi perspektifine dahil etmektedir. Başka bir ifadeyle, bankacılık sırrının gerektiği şekilde korunmaması, ilgili kişinin hak ve özgürlükleri bakımından doğurduğu sonuçtan bağımsız olarak, banka açısından da somut bir uyum ve itibar riski olarak ortaya çıkarmaktadır.

Nitekim, 2020'de Kanunun 73'üncü maddesinde yapılan değişiklikle, kural olarak, "6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteri sırrı niteliğindeki bilgilerin müşteriden gelen bir talep veya talimat olmaksızın" yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamayacağı açıkça düzenlenmiştir. Bu hüküm, açık rıza ilkesini işlevsiz hale getiren uygulamaların da bir sonucu olarak (Çatakoğlu Aydın, 2024), veri koruma rejiminin bireysel irade aracı olan açık rızayı bankacılık sırrı bakımından tek başına yeterli görmeyerek, müşterinin daha aktif bir irade ortaya koyan talep veya talimatla sürece dahil olmasını gerekli kılmaktadır. Bu yönüyle düzenleme, sır niteliğindeki bilgilerin korunmasında hem müşterinin hak ve özgürlüklerini hem de bankacılık

faaliyetine özgü risklilik değerlendirmesini birlikte gözeten bir kapsam ortaya koymaktadır. Dolayısıyla, kaynağı veri koruma menfaatinde olan bir risk, bankanın halihazırda işleyen risk yönetimi sistemi içinde değerlendirilebilir hale gelmektedir.

Bu açıdan bankacılık sırrı rejiminin risk temelli niteliği, iki risk anlayışının özdeşleştirilmesine değil; veri korumaya özgü riskin, bankacılığa özgü risk yönetimi kategorileri aracılığıyla operasyonelleştirilmesine dayanmaktadır. Bu yönüyle bankacılık mevzuatı, farklı menfaatleri esas alan iki risk anlayışı arasında işlevsel bir köprü kurmakta ve veri korumaya ilişkin riskleri bankanın bütüncül risk yönetimi çerçevesine dahil etmektedir.

Nitekim Sır Yönetmeliği'nde, risk yönetimi amacıyla yapılabilecek paylaşımların yalnızca finansal risklerle sınırlı olmadığı; uyum, kredi ve itibar riskleri dâhil tüm risk kategorilerini kapsadığı açıkça düzenlenmiştir. Bu durum gerek paylaşım ihtiyacında gerek paylaşım amacında bankacılık risklerinin göz ardı edilemeyeceği ortaya koymakta ve veri paylaşımı kararlarını doğrudan risk kategorileriyle ilişkilendirmektedir.

Bankacılık verilerinin korunmasına ilişkin yükümlülükler aykırılık oluşabilmesi ihtimali, bankalar açısından öncelikle bir uyum riski doğurmakta, bununla bağlantılı olarak operasyonel risk kapsamında da değerlendirilmektedir. Özellikle sır niteliğindeki bilgilerin hukuka aykırı şekilde paylaşılması veya korunamaması durumunda ortaya çıkabilecek idari ve adli yaptırımlar, tazmin sorumluluğu ve itibar kaybı, bu risklerin somut görünümünü oluşturmaktadır. Ayrıca, Sır Genelgesi'nde de uyum riski kapsamında yapılacak paylaşımların geçerli bir mevzuat hükmünden kaynaklanmasının ve bu durumun somut olarak ortaya konulmasının gerektiği ifade edilerek veri paylaşımına ilişkin risk değerlendirmesinin yalnızca bankanın içsel takdirine bırakılmadığını, aynı zamanda bir düzenleyici çerçeveye temellendirilmesi gerektiğini göstermektedir.

Bankaların iç sistemlerine ve risk yönetimine ilişkin düzenlemeler incelendiğinde, bankaların faaliyetlerinden kaynaklanan riskleri tanımlamak, ölçmek, izlemek ve kontrol etmekle yükümlü olduğu açıkça düzenlenmiştir. Aynı zamanda, veri güvenliği ve gizliliğine ilişkin ihlallerin de operasyonel risk kapsamında ele alınması ve buna uygun risk yönetim mekanizmalarının tesis edilmesi gerekmektedir. Benzer şekilde, Bankaların Bilgi Sistemleri ve *Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik* kapsamında da bilgi sistemlerine ilişkin risklerin analizi, sınıflandırılması, izlenmesi ve raporlanması yükümlülüğünün doğrudan bankalara bırakılması, risk temelli yaklaşımın somut bir yansıması olarak kabul edilebilecektir.

Bu doğrultuda, bankacılık sırrına ilişkin düzenlemelerle sektörel risk yönetimi düzenlemelerinin birlikte değerlendirildiğinde, veri güvenliği ve gizliliğine ilişkin risklerin bankaların genel risk yönetim sistemi içerisinde bütüncül şekilde ele alındığı ve bu risklerin yönetiminin doğrudan bankaların sorumluluğuna bırakıldığı görülmektedir. Bu durum, bankacılık sırrı rejiminin yalnızca sır niteliğindeki bilgilerin korunmasına ilişkin düzenlemeler üzerinden değil, aynı zamanda risk yönetimi mekanizmaları aracılığıyla da risk temelli bir yapıya sahip olduğunu ortaya koymaktadır. Başka bir ifadeyle sır niteliğindeki bilgilerin korunması, yalnızca bir veri koruma meselesi olmayıp, bankanın risk durumunu doğrudan etkileyen ve risk yönetimi faaliyetleri içerisinde yer alması zorunlu bir değerlendirme başlığı olarak ortaya çıkmaktadır.

5.4. Bankacılık Sırlarının Korunmasına Yönelik Düzenlemelerin Genel Veri Koruma Mevzuatıyla Karşılaştırılması

Türk hukukunda kişisel verilerin korunmasına ilişkin genel düzenleme olan KVKK'yla bankacılık sırrı düzenlemeleri karşılaştırıldığında, risk temelli yaklaşım bakımından yapısal bir farklılık ortaya çıktığı değerlendirilmektedir. Zira, KVKK'da kişisel verilerin işlenmesine ilişkin genel ilkeler ve işleme şartları ayrıntılı şekilde düzenlenmiş olmakla birlikte, risk temelli yaklaşımın temel unsurlarının –özellikle

veri işleme faaliyetinin doğurabileceği risklerin sistematik olarak değerlendirilmesi, risk seviyesine göre farklılaştırılmış yükümlülüklerin öngörülmesi ve buna bağlı hesap verebilirlik mekanizmalarının oluşturulması– kanun düzeyinde açık ve bütüncül bir şekilde yer almadığı görülmektedir. Bu yönüyle KVKK'nın yapısal olarak daha kural temelli bir karakter taşıdığı değerlendirilebilir (Kaya, 2020).

Buna karşılık, bankacılık sırrına ilişkin düzenlemelerde, risk temelli yaklaşım açıkça ifade edilmemiş ise de yükümlülüklerin yerine getirilmesi bakımından uygulamada bankaların risk üzerinden değerlendirmesi yapmasını gerekli kılan bir yapı söz konusu olmaktadır. Özellikle veri paylaşımına ilişkin karar alma süreçlerinin bankalara bırakılması, paylaşımın kapsam ve yönteminin somut olay bazında belirlenmesi ve bu süreçlerin kayıt altına alınarak denetime açık tutulması gibi unsurlar, risk temelli yaklaşımın fiilen uygulandığını göstermektedir.

Bu çerçevede, Türk hukukunda genel veri koruma rejimiyle bankacılık sırrı rejimi arasında risk temelli yaklaşım bakımından açık bir ayrışma bulunduğu söylenebilir. Genel veri koruma rejiminde sınırlı ve dolaylı şekilde yer alan risk temelli unsurların, bankacılık faaliyetinin doğası gereği risk yönetimine dayanması nedeniyle, sektörel düzenlemelerde daha belirgin ve işlevsel bir nitelik kazandığı görülmektedir. Bu bakımdan KVKK'yla bankacılık mevzuatı arasındaki ayrım risk temelli yaklaşımın kanun lafzında açıkça yer alıp almamasıyla değil, riskliliğe ilişkin hususların çevresindeki düzenleyici yapı tarafından doldurulup doldurulmadığıyla ilişkilidir. Bankacılık mevzuatı bakımından gerek sır düzenlemelerinin çerçevesi gerek mevcut risk yönetimi düzenlemelerinin kümülatif katkısıyla karşılanması bu işlevi sağlamaktadır.

5.5. Genel Değerlendirme: Bankacılık Sırlarının Korunmasına Yönelik Düzenlemelerin Parçalı Ancak İşlevsel Bir Risk Temelli Yaklaşımı Yansıtmaması

Yapılan değerlendirmeler birlikte ele alındığında, Türk bankacılık sektöründe sırların korunmasına ilişkin regülasyonun iki yönlü bir görünüm sergilediği sonucuna ulaşılmaktadır. Bankacılık sırrının korunmasına ilişkin düzenleme çerçevesi, bir yandan risk temelli yaklaşımı açıkça zikretmemekte, öte yandan içerdiği yapısal unsurlar itibarıyla risk temelli yaklaşımın temel bileşenlerini barındırmaktadır. Bu iki tespit birbiriyle çelişmemekte; aksine, çalışmanın temel iddiasını oluşturan fiili yapının birbirini tamamlayan iki kaynağına işaret etmektedir. Zira, bir yandan, bankacılık sırrının korunmasına ilişkin düzenlemelerde risk temelli yaklaşım bu adla anılmasa dahi, paylaşım kararlarının somut olay bazında değerlendirilmesi, paylaşım kararların BDDK'nın ön iznine değil bankanın kendi takdirine bırakılması, paylaşımına ilişkin kayıtların tutularak denetime hazır biçimde saklanması, paylaşımın amaç sınırlı ve ölçülü yapılmasıyla bu yaklaşımın somut unsurlarını barındırmaktadır. Öte yandan bu düzenlemeler, bankacılık faaliyetine özgü genel risk yönetimi çerçevesiyle birlikte işlediğinde, unsurlar bakımından operasyonel, uyum ve itibar riski kategorileri aracılığıyla daha geniş bir sistemle bütünleşmektedir. Bir başka deyişle, sır düzenlemeleri veya genel risk yönetimi çerçevesinin tek başına değil, ikisinin bütüncül yaklaşımla dikkate alındıklarında, regülasyonun risk temelli yaklaşımı yansıttığı görülmektedir.

Özellikle risk değerlendirme yetkisinin bankalara bırakılması, veri paylaşımına ilişkin kararların somut olay bazında alınması, veri güvenliği ihlallerinin bankaların risk yönetimi süreçleri içerisinde denetime açık bir şekilde ele alınması gibi unsurlar, söz konusu rejimin bir risk temelli yapı içerdiğini göstermektedir.

Nitekim Sır Yönetmeliği'nde, müşteri sırrı kapsamındaki paylaşımların kayıt altına alınması, belirli periyotlarla raporlanması ve denetime hazır şekilde saklanmasına yönelik yükümlülükler öngörülerek, risk değerlendirmesinin yalnızca karar alma aşamasıyla sınırlı kalmadığı, aynı zamanda gerektiğinde izlenebilir ve denetlenebilir hale getirildiği ortaya konulmaktadır. Bu yönüyle bankacılık sırrı rejimi, genel veri koruma mevzuatından farklı olarak, risk temelli düzenleme yaklaşımının açıkça zikredilmese de fiilen işlediği bir alan olarak karşımıza çıkmaktadır.

Bu çerçeve, veri paylaşımına ilişkin kararların önceden belirlenmiş katı kurallara değil, her somut olayın taşıdığı risklerin değerlendirilmesine dayandığını ve bankacılık sırrı rejimini işlevsel bir risk temelli düzenleme yaklaşımı yansıttığı ortaya koymaktadır. Dolayısıyla Türk hukukunda risk temelli yaklaşımın, genel veri koruma rejiminden ziyade, özellikle riskin yönetiminin ön planda olduğu bankacılık gibi sektörel düzenlemelerde daha belirgin ve işlevsel bir biçimde ortaya çıkabileceği değerlendirilmektedir.

6.Sonuç

Düzenleme faaliyetlerine ilişkin yaklaşımlarda zaman içerisinde meydana gelen dönüşümle birlikte, ayrıntılı kurallarla uygulamayı önceden belirleyen ve düzenleyici otoritenin *ex ante* kontrolüne dayanan kural temelli yaklaşımın yerini, düzenleme öznesine takdir alanı tanıyan yaklaşımlar almaktadır. Bu çerçevede, risk temelli yaklaşım, düzenlemelerin muhataplarına, faaliyetlerinden kaynaklı riskleri önceden analiz etme, uygun önlemleri alma ve buna göre karar verme imkânı tanırken; yapılan değerlendirmelerin gerektiğinde açıklanabilir ve denetlenebilir olmasını zorunlu kılarak hesap verebilirlik ilkesini de beraberinde getirmektedir. Dolayısıyla bu yaklaşım, yalnızca bir esneklik aracı değil, sorumluluğun düzenleme öznesine kaydırıldığı düzenleme modeli olarak ortaya çıkmaktadır.

Veri koruma hukuku bakımından, GDPR, risk temelli yaklaşımı açık ve sistematik şekilde benimsemektedir. Buna karşılık KVKK, temel ilkeleri düzenlemekle birlikte risk temelli yaklaşımının araçlarını aynı açıklıkta içermemekte olup, bu durum KVKK'nın daha kural temelli karakter taşıdığına işaret etmektedir.

Buna karşılık bankacılık sektörü özelinde yapılan değerlendirme ise farklı bir tablo sunmaktadır. Bankacılık faaliyetlerinin doğası gereği risk yönetimi üzerine kurulu olması bankacılık sırrının korunmasına ilişkin düzenlemelerin de bu çerçeveden bağımsız değerlendirilemeyeceğini göstermektedir. Her ne kadar Kanun ve sır düzenlemelerinde risk temelli yaklaşım açık bir kavram olarak yer almasa da bu rejimin risk temelli niteliği iki kaynağın birlikte işlemlerinden doğmaktadır. Bir yandan sır düzenlemeleri, paylaşım kararlarının somut olay bazında ve bankanın takdiriyle alınması, bu kararların kayıt altına alınarak denetime açık tutulması ve ölçülülükle gereklilik ilkelerinin gözetilmesi gibi unsurları kendi içinde barındırmakta; öte yandan bu unsurlar, bankacılığın genel risk yönetimi çerçevesiyle birlikte işlediğinde, veri güvenliği ve gizliliğine ilişkin riskler uyum, operasyonel ve itibar riski kategorileri aracılığıyla daha geniş bir sistemle bütünleşmektedir.

Bu itibarla, Türk hukukunda risk temelli yaklaşımın genel veri koruma düzenlemelerinde sınırlı bir görünüm sergilemesine karşın, bankacılık gibi sektörel düzenlemelerde daha belirgin ve işlevsel biçimde ortaya çıktığı sonucuna ulaşılmaktadır. Başka bir deyişle bankacılık sırrı rejimi, risk temelli yaklaşımın açıkça zikredilmese dahi fiilen işlediği bir alan olarak öne çıkmaktadır. Bu çalışma, söz konusu yaklaşımın Türk hukukunda yalnızca açık normatif düzenlemeler yoluyla değil; düzenlemelerin yapısal özellikleri, karar alma mekanizmaları ve sorumluluk dağılımının birlikte oluşturduğu kümülatif yapı aracılığıyla da var olabileceğini göstermektedir.

Son olarak, bankacılık sırrının korunmasında gözlemlenen bu fiili yaklaşımın, özellikle bankacılık dışı alanlarda da "sır" kavramının "risk" perspektifiyle ele alınması bakımından dikkate değer bir örnek olabileceği değerlendirilmektedir.

Kaynakça

1. Alıcı, Y. (2017). *Bankacılık Kanunu Şerhi*. İstanbul: On İki Levha Yayıncılık.
2. Alımcı, E. (2022). Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi. *Ankara Barosu Dergisi*, 80(1): 47-76.
3. Altay, S. A. (2019). *Hukuki Açıdan Banka Anonim Ortaklığı*. İstanbul: Vedat Kitapçılık.
4. Arslanhan, M. (2024). Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması. *Kişisel Verileri Koruma Dergisi*, 6(2): 33-53.
5. Article 29 Data Protection Working Party. (2014). *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks*, European Commission, 14/EN WP 218.
6. Artificial Intelligence Act (AI Act). (2024). *Official Journal of the European Union*, L 2024/1689, 12 Temmuz 2024.
7. Aşıkoğlu, Ş. İ. (2018). *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*. İstanbul: On İki Levha Yayıncılık.
8. Ayözger Öngün, A. Ç. (2018). İlgili Kişinin Kişisel Verilerin Korunması Kanunu'ndan Doğan Hakları. Prof. Dr. Hüseyin Hatemi'ye 80. Yıl Armağanı (80. Yıl Sempozyumu Tebliğleri), (Ed.) Yasemin Güllüoğlu Altun. İstanbul: On İki Levha Yayıncılık.
9. Babuşçu, Ş., Hazar, A., İskender, A. (2021). *Banka Risk Yönetimi: Basel I-II-III-IV Düzenlemeleri*. Ankara: Bankacılık Akademisi Yayınları.
10. Bağrıaçık, S. N. (2017). *Üretim ve İş Sırlarının Korunması*. İstanbul: On İki Levha Yayıncılık.
11. Baldwin, R., Scott, C., Hood, C. (1998). *A Reader on Regulation*. Oxford: Oxford University Press.
12. Bankacılık Düzenleme ve Denetleme Kurumu. (2016). *Operasyonel Riskin Yönetimine İlişkin Rehber*, Kurul Kararı No. 6827, 31 Mart 2016.
13. Bankacılık Düzenleme ve Denetleme Kurumu. (2022). 2022/1 sayılı Genelge: *Sır Niteliğindeki Bilgilerin Paylaşılması Hk. Yönetmeliğin Uygulanmasına İlişkin Açıklamalar*. Kurul Kararı No. 10295, 11 Ağustos 2022.
14. Bankacılık Kanunu. (2005). *T.C. Resmî Gazete*, 25983, 1 Kasım 2005.
15. Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik. (2014). *T.C. Resmî Gazete*, 29057, 11 Temmuz 2014.
16. Başar, C. (2020). *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayıncılık.
17. Bayram, Ö. B. (2022). Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi. *Kişisel Verileri Koruma Dergisi*, 4(1): 38-53.
18. Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik. (2020). *T.C. Resmî Gazete*, 31069, 15 Mart 2020.
19. Bilir, F. (2023). Kişisel Verilerin Korunması Yönündeki Uygulama ve Hukuki Düzenlemelerin Ortaya Çıkışı. *Adalet Dergisi*, 71: 631-651.
20. Black, J. (2010). Risk-based Regulation: Choices, Practices and Lessons Being Learnt. Risk and Regulatory Policy: Improving the Governance of Risk. Paris: *OECD Publishing*.
21. Black, J., Hopper, M., Band, C. (2007). Making a success of Principles-based regulation. *Law and Financial Markets Review*, 1(3): 191-206.
22. Burgemeestre, B., Hulstijn, J., Tan, Y. H. (2009). Rule-based versus Principle-based Regulatory Compliance, *Frontiers in Artificial Intelligence and Applications*, 205: 37-46.

23. BCBS. (2001). *Customer Due Diligence For Banks (Consultative Document)*. BIS.
24. BCBS. (2004). *Consolidated KYC Risk Management*. BIS.
25. BCBS. (2014). *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*. BIS.
26. Çatakoğlu Aydın, B. (2024). Bankacılıkta Dijital Yoldan Edinilen Kişisel Verilerin Korunması. *Banka ve Ticaret Hukuku Dergisi*, 40(4): 1027-1073.
27. Çekin, M. S. (2025). Dijital Çağda Anayasa Yargısı: Özel Hukuk Perspektifinden Bir İnceleme. *Anayasa Yargısı*, 42 (1), 583-609.
28. Çekin, M. S., Berktaş, A. E., Akıncı, M. F. (2023). *Veri Hukuku*. İstanbul: On İki Levha Yayıncılık.
29. Decker, C. (2018). Goals-based and Rules-based Approaches to Regulation. *BEIS Research Paper*, No8.
30. Dülger, M. V. (2021). Bankaları Doğrudan İlgilendiren Yeni ve Karmaşık Bir Düzenleme Üzerine: Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik Neler Getiriyor?. *SSRN*, <https://ssrn.com/abstract=3863276>.
31. Dülger, M. V. ve Bakdur, M. (2021). 7222 Sayılı Kanun ile 5411 Sayılı Bankacılık Kanunu'nda Yapılan Düzenlemenin KVK Hukuku Açısından Değerlendirilmesi. *SSRN*, <https://ssrn.com/abstract=3792361>.
32. Ebers, M. (2025). Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act. *European Journal of Risk Regulation*. 16: 684-703.
33. Gellert, R. (2018). Understanding the Notion of Risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2): 279-288.
34. Gellert, R. (2020). *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press.
35. Gellert, R. (2021). The Role of the Risk-Based Approach in the GDPR and in the AI Act. *Journal of Ethics and Legal Technologies*, 3(2): 15-33.
36. General Data Protection Regulation (GDPR). (2016). *Official Journal of the European Union*, L 119/1, 4 Mayıs 2016.
37. Gonçalves, M. E. (Online: 2019). The Risk-Based Approach under the New EU Data Protection Regulation. *Journal of Risk Research*, 23: 139-152.
38. Güven, Ç., Irmak, O., Eren, E. (2023). 5411 sayılı Bankacılık Kanununda Müşteri Sırlarının Tabi Olduğu Hukuki Çerçeve. *Bankacılar Dergisi*, 124: 18-45.
39. Karamustafaoğlu, M., Ünsal Özden, S., Uz, İ. (2021). Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği. *Kişisel Verileri Koruma Dergisi*, 3(1), 17-40.
40. Karatay, R. (2023). Kolluğun Önleyici Faaliyetler Kapsamında Kişisel Veri İşlemesi. *Kişisel Verilerin Korunmasına Uzman Bakış*, (Ed.) Pınar Çağlayan Aksoy ve Hüseyin Can AKSOY. Ankara: KVKK Yayınları.
41. Kaya, İ. (2024). *Banka Hukukunda Müşteri Sırrını Saklama Yükümlülüğü (Fransız, İsviçre ve Türk Hukukunda)*. Ankara: Seçkin Yayıncılık.
42. Kaya, M. B. (2020). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. *İstanbul Hukuk Mecmuası*, 78(4): 1859-1897.
43. Kişisel Verilerin Korunması Kanunu. (2016). *T.C. Resmî Gazete*, 29677, 24 Mart 2016.
44. Oğuz, S. (2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 13(2):121-138.
45. Özcan, G. (2020). *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*. İstanbul: On iki Levha Yayıncılık.

46. Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik. (2021). *T.C. Resmî Gazete*, 31501, 4 Nisan 2021.
47. Sözüğüzel, İ. (2023). *Banka Anonim Ortaklığında Müşteri Sırrının Korunması*. İstanbul: On İki Levha Yayıncılık.
48. Taştan, F. G. (2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayıncılık.
49. Taştan, F. G. ve Saruhan, U. (2020) Açık Bankacılık: Kişisel Verilerin Korunmasına Bir Tehdit Mi?. *academia.edu*, 1-44.
50. Tokmakçı, U. (2023). Kişisel Verilerin Korunmasında Risk Temelli Yaklaşım. Kişisel Verilerin Korunmasına Uzman Bakış, (Ed.) Pınar Çağlayan Aksoy ve Hüseyin Can AKSOY. Ankara: KVKK Yayınları.
51. Tunay, K. B. (2010). Bankacılık Krizleri ve Erken Uyarı Sistemleri: Türk Bankacılık Sektörü İçin Bir Model Önerisi. *BDDK Bankacılık ve Finansal Piyasalar Dergisi*, 4(1): 9-46.
52. Yan, Y. (2023). The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law. *Beijing Law Review*, 14:1250-1270.