Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr Cilt:6 Sayı:2 Geliş:27.10.2024
Kabul:20.12.2024

Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması

Merve, ARSLANHAN
Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü Yüksek Lisans Öğrencisi
mervearslanhan2@gmail.com
ORCID ID: 0009-0001-9184-7690

ÖZ
Teknolojinin finans sektöründeki konumunun güçlenmesi ve bu sektörde dijital sistemlerin kullanımının yaygınlaşması ile kişisel verilerin korunması hukuku, birçok alanda olduğu gibi, müşteri verilerinin güvenliğinin sağlanması noktasında da önemini arttırmıştır. Günümüzde bankacılık sektöründe faaliyet gösteren finansal kuruluşların finansal işlemlerde kullandığı verilerden, müşteri ilişkilerinin kurulması süreçlerinde toplanan verilere kadar birçok farklı süreçte kişisel veri işlediklerini görmekteyiz. Bu çalışmada bankaların, kişisel veri işleme süreçlerindeki kişisel veri güvenliği ihlallerinden doğan sorumluluğu, Kişisel Verilerin Korunması Kurulu tarafından bankalardaki kişisel veri güvenliği ihlallerine ilişkin verilen kurul kararları ekseninde ve mevzuat kapsamındaki yükümlülükleri ile incelenmektedir. Bu çalışmanın amacı bankaların kişisel veri güvenliğinden kaynaklanan sorumluluğun incelenmesi yoluyla bankaların kişisel veri güvenliğine ilişkin yükümlülüklerinin değerlendirilmesidir.

Anahtar Kelimeler: Kişisel Veri, Bankacılık Sektörü, Bankalar, Müşteri Sırrı, Kişisel Veri Güvenliği

Protection of Bank Customer's Personal Data Within Information Security Governance of Banks

ABSTRACT
Personal data protection law raised its importance in providing security of the customers' data, due to strengthening place of technology in finance and extending use of digital systems in this sector, as in all other sectors. Today we see that, personal data are processed in many ways including from data used in financial transactions of financial institutions in banking sector to personal data collected in customer relation procedures. In this article, liability arising from misdemeanor on personal data security breach of the banks shall be evaluated with inspecting decisions given by the Personal Data Protection Board on the personal data security breaches of the Banks and banks' responsibilities arising from legislation. The aim of this study is to evaluate the banks liability arising from personal data security by evaluating their responsibility thereof.

Keywords: Personal Data, Banking Sector, Banks, Customer Secret, Personal Data Security

Atıf Gösterme Arslanhan, M., (2024). Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması, *Kişisel Verileri Koruma Dergisi*. *6*(2), 33-53.

GİRİŞ

Teknolojinin hızlı ilerleyişi iş hayatının tüm yönlerini etkilemekte, birçok alanda yeni altyapılar gerektirmekte, ortaya çıkabilecek muhtemel sorunlar için hız kazandıran çözüm arayışlarına sebep olmakta ve yine buna yönelik çözümler sunmaktadır. Finansal hizmetler açısından da birçok uygulama ve yeni kanalların kullanımına imkân veren bu ilerleyiş; dijital bankacılık, internet bankacılığı ve mobil bankacılık dahil birçok yeni bankacılık kanalının kullanımının önünü açmıştır. Ancak dijitalleşme bilginin erişilebilirliğini arttırmış olmakla beraber; sistemlere yönelik saldırıların ve ihlallerin de artışına sebep olmuştur. Bu açıdan sistemlerin güvenliğinin sağlanması, verilerin güvenliğinin sağlanması ile mümkün olacaktır. Bankalar faaliyetlerini gerçekleştirirken işledikleri bilgilerin, verilerin ve belgelerin güvenliğini sağlamalıdır.

Dijital sistemlerin kullanımın yaygınlaşması veriye erişimi kolaylaştırmıştır. Bu sebeple ilgili kişiler belirli bir amaca yönelik olarak paylaştıkları verilerinin; özel sektöre, kamuya veya talep etmediği kişilere açıklanmıyor olmasını beklemekte, birçok işlem özelinde bu beklenti ile verilerini veri sorumluları ile paylaşmaktadırlar. Kişilerin verilerinin toplanması ve kullanımı, bu veriler üzerinde 3. Kişilerin sahip olacağı hakimiyetin sınırlarının belirlenmesi gerekliliğini de beraberinde getirmiştir. Dijital dağıtım kanallarının kullanımı büyük miktarda verinin toplanmasını gerektirir, bu durum da çoğunlukla ilgili kişilerin kişisel verilerinin toplanmasına ve muhtemel bir ihlal durumunda bu verilere 3. kişiler tarafından ulaşılabilmesine neden olur.

Her geçen gün yeni alternatif dağıtım kanallarının ortaya çıkmasının bir sonucu olarak; elektronik bankacılık kanalları mevzuatımızda sınırlı sayı prensibi uygulanmadan belirlenmiştir. Bankaların yeni çözümler üretmek amacıyla oluşturdukları yeni kanallar; bu kanalları kullanan müşterilerin sayısında da artışa yol açmıştır. İnternet bankacılığını ve mobil bankacılığı (*dijital bankacılık*) kullanan bireysel ve kurumsal müşterilerin sayısı; dijital bankacılık kanallarının kullanımındaki artış sonucunda Aralık 2019'da 53 milyonken yaklaşık 4 yıllık bir sürede iki katını aşarak, Aralık 2023'te 111 milyona ulaşmıştır. Haziran 2024 itibariyle ise toplam 115 milyon kişi aktif olarak dijital bankacılık kanallarını kullanmaktadır (Türkiye Bankalar Birliği ("**TBB**") Aralık 2023, 2024; TBB Haziran 2024, 2024).

5411 sayılı Bankacılık Kanunu ("**Bankacılık Kanunu**") bilgi güvenliğine ilişkin doğrudan bir hüküm içermemektedir ancak Bankacılık Düzenleme ve Denetleme Kurumu ("**BDDK**") tarafından bilgi güvenliğinin sağlanmasına yönelik çeşitli ikincil düzenlemeler ihdas edilmiştir. Bankacılıkta bilgi güvenliğini düzenleyen ilk kapsamlı düzenleme Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'dir ("**Mülga Tebliğ**"). Mülga Tebliğ esas olarak bankaların faaliyetlerinde kullandıkları bilgi sistemlerinin yönetimine ilişkin asgari esas ve usulleri düzenlemekteydi. Ayrıca internet bankacılığını ve ATM'leri özellik arz eden işlemlerden kabul etmekte ancak; telefon bankacılığı, mobil bankacılık ve açık bankacılık gibi alternatif kanallara yer vermemekteydi. Mülga Tebliğ kayıtların/işlemlerin/verilerin bütünlüğünün ve gizliliğinin sağlanmasına yönelikti ve verinin iletimi, işlenmesi ve bilginin doğruluğunun, tamlığının ve güvenilirliğinin sağlanmasını kapsamaktaydı. Ayrıca verilerin gizlilik derecesine göre sınıflandırılması ve zorunlu ise ek birtakım kontrollerin tesisi edilmesini öngörmekteydi. Belirtmek gerekir ki, Mülga Tebliğ'de gizlilik derecelerine ilişkin ek bir açıklamaya yer verilmemekteydi.

Yürürlükteki düzenleme olan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ("**Bilgi Sistemleri Hakkında Yönetmelik**") ise 31069 sayılı ve 15 Mart 2020 tarihli Resmî Gazete'de yayınlanması akabinde yürürlüğe girmiştir. Aynı sayı ve tarihli Resmî Gazete ile BDDK tarafından Mülga Tebliğin Yürürlükten Kaldırılmasına Dair Tebliğ yayınlanmış ve Bilgi Sistemleri Hakkında Yönetmeliğin belirli hükümlerinin ilk yürürlük tarihi olan 1 Temmuz 2020 tarihi itibarıyla yürürlüğe gireceği belirtilmiştir. Bilgi Sistemleri Hakkında Yönetmelik, bilgi güvenliğinin sadece mevcut elektronik bankacılık sistemlerinde değil; sonrasında ortaya çıkması muhtemel alternatif dağıtım

kanallarını da kapsayacak şekilde elektronik bankacılık hizmetleri için ortak hükümler ve bilgi sistemlerinin risk yönetimine ilişkin asgari esas ve usuller belirlemektedir. Mülga Tebliğ'den ayrışan bir diğer nokta ise Bilgi Sistemleri Hakkında Yönetmeliğin amacı ve kapsamı elektronik bankacılık hizmetlerinin sunulmasına ilişkin risklerin yönetimi ve bilgi sistemlerinin yönetimine ek olarak, bu sistemlerin kontrollerinin tesisini de düzenlemektir. Bütünsel bakıldığında, sistemin asgari esas ve usuller ile mümkün olacak en güvenli ve kontrollü hale getirilmesi amaçlanmıştır. Bunun sağlanması adına, sistemlerin güvenliğine ve muhtemel ihlallerde alınması gerekecek önlemlere ilişkin teknik ve idari tedbirler belirlenmiştir. Belirtmek gerekir ki, idari tedbirler insan kaynaklı risklerin minimizasyonu ve süreç yönetiminin kontrolü ile iş sürekliliğinin sağlanmasına yönelik iken; teknik tedbirler sistem kayıtlarının tutulmasına, muhtemel açıkların tespitine ve sistemlerde etkin mekanizmaların tesisine yöneliktir. Bankacılık mevzuatında veri paylaşımına, sır niteliğindeki bilgilerin paylaşılmasına, dış hizmet alınmasına ve destek hizmetlerin sağlanmasına ilişkin yönetmelikler de mevcuttur. Çalışma kapsamında bu düzenlemelere gerektiği ölçüde yer verilecektir.

Kişisel verilerin işlenmesinden kasıt; tamamen veya kısmen otomatik yollarla veya otomatik olmayan yollarla ancak bir veri kayıt sisteminin parçası olarak kişisel veriler üzerinde gerçekleştirilen tüm işlemlerdir (6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**") m.3/1(e)). Sistemsel aksaklıklar ve/veya eksiklikler sebebiyle, ya da çalışanlardan kaynaklanan nedenlerle veya üçüncü kişilerin müdahaleleri sonucunda veri güvenliği ihlalleri meydana gelebileceğinden; basiretli tacir olan bankaların bu verilerin güvenliği hususunda aldığı tedbirlerin kişisel veri işleme süreçlerinin her kademesinde bir yansıması olacağı kuşkusuzdur. Bu sebeple öncelikle, bu çalışma kapsamında açıklanmasında yarar görüldüğü ölçüde, kişisel veri işleme süreçlerinin temel aktörlerine ve bankacılık mevzuatından örneklerle kişisel veri işleme süreçlerine yer verilecektir. Sonrasında ise bankalardaki diğer veri kategorileri açıklanacak, müşteri sırrı ve kişisel veri tanımı birlikte değerlendirilecek, bilgi güvenliğinin tanımı yapılacak, bilgi sistemlerinin güvenliği ve yönetimi için gerekli tedbirler açıklanacak ve son olarak Kişisel Verileri Koruma Kurulu ("**Kurul**") tarafından alınan kararlar bu bilgiler ışığında incelenecektir. Belirtmek gerekir ki, banka çalışanlarının kişisel verilerinin işlenmesi çalışma kapsamı dışında tutulmuştur. Ayrıca çalışma kapsamında bankacılık sektöründen kasıt, Bankacılık Kanunu uyarınca yetkilendirilen ve faaliyete başlayan bankaları kapsamakta olup; genel olarak Bankacılık Kanunu m.3'te tanımlanan mevduat bankalarının faaliyetleri ve bu bankaların verileri dikkate alınmıştır.

KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL KAVRAMLAR VE BANKACILIK SEKTÖRÜNDE KİŞİSEL VERİ

Gerçek kişiye ait her türlü veri, ilgili kişinin belirlenebilir kılınmasına imkân verdiği ölçüde kişisel veri olarak nitelendirilmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu mevzuatımızda kişisel veri kavramını tanımlayan ve tüm kişisel veri işleme süreçlerine uygulanabilme kabiliyeti olan ilk çerçeve metindir. Kişinin adı, soyadı, fotoğrafı gibi bilgileri yanında; kişiyi belirlenebilir kılan bilgileri yani kişinin adresi, araç plakası, telefon numarası gibi bilgileri de kişisel veri olarak değerlendirilir. Kanun kapsamında kişisel veriler sadece gerçek kişiye ilişkin olduğu ölçüde koruma altındadır. Kanun sadece gerçek kişilere ilişkin verileri kişisel veri olarak değerlendirdiğinden, tüzel kişilerin verileri Kanun kapsamında kişisel veri olarak değerlendirilmez.

Kişisel verilere ilişkin temel yaklaşım; bir kısım daha "hassas" nitelikli yani daha fazla koruma gerektiren verinin özel nitelikli kişisel veri olarak nitelendirilmesi (Aksoy, 2010; Dülger, 2020; Küzeci, 2021; Yürük, 2023) ve bu nitelikteki verilerin – çalışma kapsamında – genel nitelikli olarak ifade edebileceğimiz kişisel veriler değerlendirildiğinde daha farklı bir hukuki rejime tabi kılınmasıdır. Kanun koyucu, özel nitelikli kişisel veriler açısından sınırlı sayım yöntemini benimsemiştir (Kanun m.6/1). Bu sebeple özel nitelikli kişisel veriler, Kanun'da belirtilenler ile sınırlıdır. Burada şunu da belirtmek gerekir ki, bazı durumlarda bir verinin özel nitelikli veri olarak değerlendirilip değerlendirilemeyeceğine

ilişkin tereddüt oluşabilmektedir (Küzeci, 2021). Örnek vermek gerekirse; kişinin fotoğrafında gözlük takması durumunda, kişinin gözü ile ilgili bir sağlık problemi olduğu varsayılabilir ve bu durumun kişinin sağlık durumuna ilişkin bir bilgi (*sağlık ile ilgili veriler özel nitelikli veridir*) olduğu kabul edilebilecektir. Burada dikkat edilmesi gereken husus ise verinin toplanma amacının da dikkate alınmasıdır (Küzeci, 2021). Yani; kişinin fotoğrafının çekilmesinin sebebi sağlık durumuna ilişkin bir değerlendirme yapılması olarak nitelendirilmediğinden, özel nitelikli kişisel veri olarak değerlendirilmez.

Temel Aktörler

İlgili kişi, veri sorumlusu ve veri işleyen, kişisel veri işleme süreçlerinde temel aktörlerdir. İlgili kişi, kişisel verisi işlenen gerçek kişi olduğundan; ticaret şirketleri gibi tüzel kişiler, Kanun kapsamında ilgili kişi olarak değerlendirilmez. Bu kişilerin verileri; ticari sır, müşteri sırrı, banka sırrı, hassas veri dahil; diğer mevzuat hükümlerinin uygulanabildiği ölçüde bu hükümlerin sağladığı hukuki korumadan yararlanacaktır.

Ancak, tüzel kişilerin ünvanında gerçek kişilere ilişkin ad ve soyadı yer alıyorsa bu durumda ihlalin yönelik olduğu hak ve menfaatler incelenerek ayrıca bir değerlendirme yapılmalıdır. Bazı ticaret şirketlerinin ünvanında, belirli ünvanlara sahip olan gerçek kişi ortakların ad-soyadlarının yer alması zorunluyken; diğer şirket türlerinde bu kişilerin ad-soyadlarına ticaret ünvanında yer verilmesi belirli şartların yerine getirilmesi ile mümkündür. Örneğin; 6102 sayılı Türk Ticaret Kanunu ("**TTK**") m.42 uyarınca kollektif şirketlerde ortakların tamamının tam ad-soyadlarının veya ortaklardan en az birinin tam ad-soyadının ve şirketin türü ticaret ünvanında yer almalıyken; Komandit şirketlerde adi veya sermayesi paylara bölünmüş olup olmadığına bakılmaksızın şirketin komandite ortaklarından en az birinin tam ad-soyadı, şirket ve türü ünvanda yer almalıdır. Anonim, limited ve kooperatif şirketlerin ticaret ünvanı ise, TTK m.43 uyarınca gerçek kişinin adı veya soyadına yer veriyorsa; şirket türünü ifade eden "Anonim Şirket", "Limited Şirket" veya "Kooperatif" kelimeleri kısaltma yapılmadan kullanılmalıdır. Kurul'un 2022/103 sayılı ve 10/02/2022 tarihli Kararı kapsamında yapılan inceleme sonucu, somut olayda karara konu sosyal medya paylaşımlarının ticaret ünvanında adı geçen gerçek kişi yerine tüzel kişiye yönelik yapılması sebebiyle gerçek kişinin hak ve menfaatlerine yönelik bir ihlal söz konusu olmadığından ve kullanılan bilgiler de tüzel kişiye ilişkin olduğundan; incelemeye konu olay kapsamında gerçek kişiye ait ad ve soyadın tüzel kişiye ait veri olduğu ve Kanun kapsamında değerlendirilmemesine karar verilmiştir.

Kişisel veri işleme süreçlerinde veri işleme faaliyetini gerçekleştiren ve Kanun kapsamında "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*" veri sorumlusudur. Burada en önemli hususlardan biri, ilgili kişi kanunen sadece gerçek kişi olabilecekken; veri sorumlusu gerçek kişi veya tüzel kişi olabilir. Ayrıca kamu ya da özel sektör tüzel kişisi olması da veri sorumlusu sıfatının izafe edilmesinde herhangi bir fark yaratmaz. Veri sorumlusunun yanında; "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*" şeklinde tanımlanan veri işleyen de kişisel veri işleme süreçlerinden sorumludur. Ancak veri işleyenin bu sıfatı; veri sorumlusundan aldığı talimat ve yetki ile sınırlıdır. Şöyle ki, veri işleyen talimatları uygulamaz veya yetkisini aşarsa yani veri sorumlusu tarafından belirlenen tanımın dışına çıkarsa bu durumda veri işleyen, yetkisini aştığı veri işleme süreçleri ve faaliyetleri açısından veri sorumlusu olarak değerlendirilebilir.

Kişisel verilerin korunması hukuku kapsamında bir diğer sorumluluk türü; ortak veri sorumluluğudur. Bu sorumluluk, 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün ("**GVKT**") 26. Maddesinde düzenlenmiştir. GVKT, hem Avrupa Birliği'ne üye olan ülkelerin tamamı tarafından ek bir prosedüre gerek duyulmaksızın uygulanabilirliğe sahip olan hem de kişisel verilerin korunması hukukunu düzenleyen ilk kapsamlı hukuki dokümandır. GVKT öncesi AB nezdinde yürürlükte olan 24/10/1995

tarihli 95/46/EC sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi ("**95/46/EC sayılı Direktif**") ortak veri sorumluluğuna yer vermemiştir. Bu sebeple Avrupa Birliği Adalet Divanı ("**ABAD**"), tarafına yapılan başvurulara istinaden içtihat yoluyla bu sorumluluk kabul edilmiştir. Kanun'un mehaz düzenlemesi 95/46/EC sayılı Direktiftir, bu sebeple Kanun'da ortak veri sorumluluğuna ilişkin herhangi bir madde yoktur. Kişisel Verileri Koruma Kurumu ("**Kurum**"), çağın ve günün ihtiyaçlarına uygun çözümler üretmek amacıyla yaptığı incelemeler sonucu bu sorumluluk biçimini 2021/1304 sayılı ve 23/12/2021 tarihli İlke Kararı ile mevzuatımıza kazandırmıştır. Ortak veri sorumluluğu söz konusuysa, birden fazla veri sorumlusunun ortak bir amacı olmalı ve kişisel verilerin işlenmesi süreçlerindeki temel araçlar veri sorumluları tarafından birlikte belirlenmelidir. Ortak veri sorumlularının yükümlülüklerinin nasıl belirleneceği, kusurlarının ne şekilde hesaplanacağı ve sorumluğun ne şekilde paylaştırılacağı ise somut olay bazında değerlendirilecektir.

Kişisel Veri İşleme Süreçlerine Genel Bir Bakış

Kanun'da, kişisel verilerin işlenmesine ilişkin veri işlenme şartları belirlenmiştir. Kanun'un 5. Maddesi genel nitelikli kişisel verilerin, 6. Maddesi ise özel nitelikli kişisel verilerin işlenmesine ilişkin veri işleme şartlarını açıklamaktadır. Genel nitelikli kişisel veriler, ilgili kişinin açık rızası alınmaksızın işlenemeyecektir. Açık rıza "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı*" ifade eder (Kanun m.3/1(a)). Bu açıdan daha kesin ve belirli bir irade açıklaması gerekmekte ve zımnen yapılan bir irade açıklaması açık rıza kavramını karşılamamaktadır (Akkurt, 2023). Yine bu sebeple banka tarafından gerçekleştirilen tüm bankacılık faaliyetlerini kapsayan, genel bir rıza verilmesi battaniye rıza olarak değerlendirileceği için açık rızanın belirli olma şartını sağlamaz. Kanun madde 5/2'de ise; ilgili kişinin açık rızasının alınmadığı durumlarda veri sorumlusu tarafından kişisel veri işleme süreçlerinin hukuki sebebi olarak kullanılabilecek veri işleme şartları sayılmaktadır. Bu noktada, açık rıza (Kanun m.5/1) ve diğer veri işleme şartları (Kanun m.5/2) arasında hiyerarşi olmadığını ifade etmek gerekir (Karamustafaoğlu & Ünsal Özden & Uz, 2021).

Bankaların faaliyetleri değerlendirildiğinde; bankalar tarafından Kanun'daki veri işleme şartlarından birine başvurulabileceği gibi, gerekmesi durumunda bu şartlardan birkaçına da başvurulması mümkündür. Bankacılık Kanunu uyarınca bankalar verdikleri kredilerden kaynaklanan risklerini ölçmek için gerekli bilgi ve belgeleri temin etmelidir, kredi müşterileri ise bu amaçla talep edilen bilgileri Banka'ya sunmakla yükümlüdür. Bu durumda müşteriden talep edilen belgelerdeki verilerin, kredi riski hesaplanması amacıyla kullanılması kanunda açıkça öngörülmüş olma şartını sağladığından; ilgili kişinin açık rızasının alınması gerekmez (Kanun m.5/2(a); Bankacılık Kanunu, m.52/1). Aynı şekilde Mevduat ve Katılım Fonunun Kabulüne, Çekilmesine ve Zamanaşımına Uğrayan Mevduat, Katılım Fonu, Emanet ve Alacaklara İlişkin Usul ve Esaslar Hakkında Yönetmelik ("**Mevduat Kabulüne ilişkin Yönetmelik**")'te, bankaların müşterilerden mevduat kabulü yapılabilmesi için müşterilerini tanımak amacıyla bankalara "*müşterilerin kimliklerini, T.C. kimlik ve vergi numaralarını belgeleme*" yükümlülüğü getirilmiştir. Bu yükümlülüğün yerine getirilmesinde de ilgili kişinin bu bilgileri içeren belgelerinin/verilerinin toplanması gerekir (Mevduat Kabulüne ilişkin Yönetmelik, m.4/2). Ayrıca hesap açılış işlemleri ve müşteri ile imzalanacak olan Kredi Sözleşmesi, Mevduat Sözleşmesi, Yatırım Sözleşmesi, Banka Kartı ve Kredi Kartı Sözleşmeleri, bireysel kredi başvuruları gibi, banka ile müşteri arasında imzalanacak sözleşmelerde yer alan ve Kanun 5/2(c) kapsamında bir sözleşmenin ifası veya kurulması ile doğrudan ilgili olması şartıyla, veri işleme faaliyeti için gerekli olan, taraflara ait kişisel veriler açık rıza alınmadan işlenmektedir (Yurtoğlu, 2020). İlgili kişinin açık rızası alınmaksızın kişisel verilerin işlenmesi için belirlenen veri işleme şartları, kanun koyucu tarafından sınırlı sayıda düzenlenmiştir (Demirtaş, 2024). Bu sebeple kişisel veri işleme şartlarının genişletilmesi mümkün değildir (Bankacılık Sektörü İyi Uygulama Rehberi, 2022).

Kişisel verilerin korunmasının temel amaçlarından biri, ilgili kişiye kendisine ait kişisel verilerin akıbetini öğrenme ve tayin etme imkânı verilmesidir. Kanun, ilgili kişinin; kişisel verilerini işleyen veri

sorumlusu (ve/veya temsilcisi), kişisel verilerinin işlenme amaçları, kişisel verilerinin işlenmesi durumunda kimlere ve hangi amaçlarla bu verilerin aktarılabileceği, kişisel verilerinin toplanma yöntemleri ve bu veri toplama faaliyetinin hukuki nedenleri ile Kanun kapsamında belirtilen hakları konusunda bilgilendirilmesi yükümlülüğünü veri sorumlusuna yüklemiştir. Aydınlatma yükümlülüğü olarak ifade edebileceğimiz bu yükümlülüğü, veri sorumlusu veya veri sorumlusu tarafından yetkilendirilen kişi yerine getirmelidir (Kanun, m.10; Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019). Ancak bu yükümlülüğünün ne şekilde yerine getirilmesi gerektiği Kanun'da yer almamaktadır. Bu yükümlülük yazılı veya sözlü olarak yerine getirilebileceği gibi; katmanlı aydınlatma yapılması da mümkündür (Özcan, 2020). Bankalar internet bankacılığı, mobil bankacılık ve dijital şube gibi kanallardan hizmet vermekte ve çağrı merkezi gibi kanallardan da verilen hizmeti takip etmektedirler. İlgili kişinin metnin tamamını dinlemesinin uygun bir aydınlatma yöntemi olmayacağı durumlarda, ön bilgilendirme ile katmanlı aydınlatma yönteminin kullanılması; internet sitesi üzerinden yapılacak işlemlerde ise ilgili kişinin aydınlatma metnine yönlendirildiği bir bağlantı ile aydınlatılması uygun olacaktır (Özcan, 2020). Öğretide bir görüş (Özcan, 2020) yazılı olarak aydınlatma yapılacaksa, 6502 sayılı Tüketicinin Korunması Hakkında Kanun ("**TKHK**") uyarınca, ilgili kişinin belirli özelliklere sahip bir yazı ile aydınlatılması gerektiğini ifade etmektedir. Buna göre, ilgili kişinin bilgilendirildiği yazının (i) puntosu en az on iki olmalı, (ii) anlaşılabilir bir dili olmalı, (iii) yazı okunabilir, sade ve açık şekilde düzenlenmelidir.

Bankalar Tarafından İşlenen Kişisel Veriler ve Bankacılık Sektöründeki Diğer Veri Kategorileri

Bankacılık faaliyetlerinin gerçekleştirilmesi amacıyla bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı olarak kabul edilmektedir (Bankacılık Kanunu m.73/3). Bu sebeple ilgili kişilerden toplanan ve bu faaliyetlerin gerçekleştirilmesi sırasında işlenen kişisel veriler müşteri sırrı haline gelir. Ancak; bu verilerin müşteri sırrı olarak değerlendirilmesi, verilerin kişisel veri olma niteliğini değiştirmez (Karamustafaoğlu & Ünsal Özden & Uz, 2021). Ayrıca bankalardaki iş/işlemlerin gerektirmesi durumunda velayet altındaki çocuklar için velilerin, vesayet altındaki gerçek kişiler için vasilerin, eşlerin, kefalet verilmesi gereken işlemler için kefillerin, tüzel kişiliği haiz kurumlarda bu kurumların yöneticilerinin (ve/veya temsilcilerinin) ve iletişim için gerekmesi durumu da dahil diğer birçok işlem için müşteriler haricindeki gerçek kişilerin kişisel verileri işlenmektedir (Yurtoğlu, 2020). Bu kapsamda; vatandaşlık bilgisi, medeni durumu, eğitim bilgileri, vekaletname/nüfus cüzdanı/pasaport fotokopileri, iletişim adresi bilgileri, telefon numaraları, yetki belgeleri, imza sirkülerleri, araç bilgileri, tapu kayıtları, faaliyet belgesi, ödeme bilgisi, para transferleri ve diğer işlemler kapsamında toplanan verileri dahil ilgili kişiye ait birçok kişisel veri, veri işleme süreçlerine konu olmaktadır (Yurtoğlu, 2020). Her ne kadar gerçek kişilerin verileri müşteri sırrı olarak korunmalarının yanında, kişisel verilerin korunması mevzuatı kapsamında da korunmakta olsa da tüzel kişilerin verileri, kişisel veri tanımına uymadığından Kanun kapsamında değildir. Tüzel kişilere ait veriler banka sırrı, ticari sır, müşteri sırrı gibi diğer veri kategorileri uyarınca sır saklama yükümlülüğü ve/veya gizlilik anlaşmaları çerçevesinde korunmaktadır.

Bankacılık mevzuatı incelendiğinde müşteri sırrına ek olarak banka sırrı ve hassas veri kavramlarını da açıklamak gerekir. Öncelikle banka sırrı, Bankacılık Kanunu veya buna istinaden çıkarılan ikincil düzenlemelerde tanımlanmamıştır. 2011 yılında "Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı" Meclis'e sunulmuştur. Bu düzenlemede banka sırrı "*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 hizmet ve faaliyetleri, risk pozisyonlarına ilişkin her türlü bilgi ve belge*" şeklinde tanımlanmıştır. Ancak bu, kanunlaşan bir tasarı olmadığından banka sırrının kapsamını belirleyen bir düzenlemenin halihazırda mevcut olmadığını söyleyebiliriz. Ayrıca, banka çalışanlarının verileri banka sırrı niteliğinde bir bilgi ya da veri ile işlenmemişse; bu durumda çalışanların kişisel verileri, genel ilkeler kapsamında işlenir (BDDK 2022/1 sayılı Genelge, 2022). Bankalar açısından bir

diğer veri kategorisi ise hassas verilerdir. Bilgi Sistemleri Hakkında Yönetmelik m.3/o'da tanımlanan hassas veriler; öncelikle kimlik doğrulama süreçlerinde kullanılan veriler olmak üzere, müşterilere ait olan ve bankalarca muhafaza edilen verilerden; üçüncü kişilerin eline geçmesi durumunda banka tarafından müşterilerin tanımlanması süreçlerindeki ayırt etme mekanizmalarında sorunlar yaratabilecek ve dolandırıcılık ya da sahte işlem yapılmasına sebebiyet verebilecek nitelikteki verilerdir. Belirtmek gerekir ki Bilgi Sitemleri Hakkında Yönetmeliğin taslak versiyonunda "sır niteliğindeki veriler" de hassas veri tanımında yer alırken; metnin yürürlükteki versiyonunda bu ibareye tanımda yer vermemiştir. Zira hassas verilerden kasıt; işlem güvenliğinin sağlanması için kimlik doğrulamada kullanılacak olan verilerdir (Candemir, 2020). Verilere ilişkin bu sınıflandırma ilerde açıklanacak olan veri envanteri açısından önem taşımaktadır.

BANKACILIK SEKTÖRÜNDE KİŞİSEL VERİ GÜVENLİĞİ

Bilgi güvenliğinin amaçları; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini (*kullanılabilirliğini*) sağlamaktır (Gazdağı & Çetinyokuş, 2020). Bankalar, Bankacılık Kanunu m.7/1-a uyarınca anonim şirket olarak kurulmak zorundadır ve ticaret şirketi olmaları sebebiyle tacir olan bankalar, her türlü ticari faaliyetlerinde basiretli tacir olarak hareket etmelidir. Bankalar, özel yasa ile kurulmaları ve kendilerine birtakım imtiyazlar tanınması sebebiyle; müşterileri ile kurdukları ilişkileri bakımından, bu ilişkinin güven tesis edecek tarafı olmaları dolayısıyla, hukukumuzda güven kuruluşu olarak nitelendirilmektedirler (Yargıtay H.G.K., Esas No. 2020/108, Karar No. 2022/1450, Tarih: 08.11.2022; Yargıtay 11. H.D., Esas No. 2020/5738, Karar No. 2020/4350, Tarih: 22.10.2020; İstanbul Anadolu 1. Tüketici Mahkemesi, Esas No. 2021/999, Karar No. 2024/653, Tarih: 07.06.2024). Güven kuruluşu olma niteliği bankalara, ağırlaştırılmış özen yükümlülüğü getirmekte ve herhangi bir tacirin basiretli davranma yükümlülüğüne kıyasla daha ağır sorumlulukları olmasına neden olmaktadır. Bu sebeple bankaların bünyesindeki bilgi kayıpları, güvenlik ihlalleri durumları ve bunlar sonucu ortaya çıkan maddi kayıplar ile bu maddi kayıplar sonucunda uygulanacak yaptırımlar; bilgi güvenliğinin sağlanması açısından önem arz etmektedir (Gazdağı & Çetinyokuş, 2020).

Veri güvenliği; kişiler, prosedürler ve ürünler aracılığıyla veriyi depolayan, işleyen ve/veya ileten cihazlarda bu verilerin bütünlüğünün, gizliliğinin ve erişilebilirliğinin korunmasıdır (Civan Kemiksiz, 2022; Yürük, 2023). Veri güvenliğinin sağlanması anlık bir korumadan ziyade bir süreci ifade etmektedir. Bu sebeple veri ile ilk temas edilen andan itibaren; verinin yok edildiği, ortadan kaldırıldığı, silindiği veya benzeri bir işlem ile kullanımına son verildiği her aşamada idari ve teknik tedbirleri sağlama yükümlülüğü veri sorumlusundadır (Ayözger Öngün, 2019; Dülger, 2020; Zor, 2020; Yürük, 2023). Veri güvenliğinin sağlanması, bilgi güvenliğinin sağlanmasında bir araçtır. Bilgi güvenliğinin sağlanmasındaki amaç, sistemdeki verilerin ve bilgilerin yetkisiz ve/veya izinsiz erişimlere karşı korunması ve meydana gelebilecek ihlallerin önlenmesidir. Kişisel veri güvenliğinde veri değil, ilgili kişinin korunması amaçlanmakta ve bunun için veri güvenliği de araç olarak kullanılmaktadır (Başar, 2020). Bu sebeple veri güvenliği ile kişisel veri güvenliği birbirinden farklıdır (Çekin, 2019; Küzeci, 2019; Gündüz, 2022; Yürük, 2023).

Kişisel veri güvenliği, Kanun'un 12. maddesinde düzenlenmektedir. Kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemeye ve ayrıca kişisel verilerin muhafazasını sağlamaya yönelik uygun güvenlik düzeyini temin etmek için gerekli her türlü teknik ve idari tedbir, veri sorumlusu banka tarafından alınmalıdır. Kanun m.12/2 uyarınca kişisel veriler veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenirse, bu durumda bu tedbirlerin alınması noktasında veri sorumlusu bu kişilerle birlikte müştereken sorumludur. Burada belirtmekte yarar olacak ki, veri işleyen veri sorumlusunun verdiği yetkiye dayanarak veri işlemektedir. Bu sebeple veri güvenliğinin sağlanması açısından, veri işleyen ve veri sorumlusu müştereken sorumlu kabul edilir. Burada müşterek sorumluluktan anlaşılması gereken; ortaya çıkan zarardan sorumluluklarının, veri işleyen ve veri sorumlusunun kusurları nispetinde belirlenmesidir (Börekçi, 2020). Kanuni olmayan

yollar, hukuka uygun olmayan tüm durumlar olduğundan, yürürlükteki tüm düzenlemelere aykırı davranışlar bu sonuca sebebiyet verebilir (Dülger, 2019; Sevindi & Ordu, 2023). Veri güvenliğinin ihlal edilmesi sonucunda ilgili kişilerin kişisel verilerinin kanuni olmayan yollarla başkalarının eline geçmesi durumunda ilgili kişiye ve Kurul'a en kısa sürede ihlalin bildirilmesi gerekir. GVKT veri ihlali riski bulunmayan ihlaller hariç olmak üzere; yetkili otorite tarafından veri ihlalinin fark edilmesi akabinde en geç 72 saat içinde bildirimde bulunulması gerektiğini düzenlemektedir. Kurul'da buna uygun olarak tarafına yapılacak veri ihlal bildiriminin ihlalin öğrenilmesini müteakip en geç 72 saat içinde yapılması gerektiğini belirtmiştir (Kurul'un 2019/10 sayılı ve 24.01.2019 tarihli Kararı; Sevindi & Ordu, 2023).

Kanun'da veri sorumlusu tarafından alınması gereken teknik ve idari tedbirlere yer verilmemiştir. Ancak Kurum, veri güvenliğine ilişkin örnek niteliğinde idari ve teknik tedbirlere yer verdiği bir "Kişisel Veri Güvenliği Rehberi" yayınlamıştır. Bu tedbirler Avrupa Birliği nezdinde yürürlükte olan GVKT m.32'de veri güvenliğine yönelik örnekleyici şekilde sayılan teknik ve idari tedbirler ile benzer niteliktedir (Yürük, 2023). Kişisel verilerin korunması bir süreç olduğundan, bu sürecin ayrıca yönetilmesi gerekmektedir. Bu sebeple kişisel verilerin işlenmesine ilişkin süreçlerin her kademesinde yer alan gerçek/tüzel kişi veri sorumlusu ve/veya veri işleyenler tarafından bu korumanın tesisi elzemdir. Sistemsel koruma sağlayan teknik tedbirlerin alınmasının yanında; idari tedbir olarak süreçte yer alan aktörler ve bilgi güvenliği tesisinden sorumlu yöneticiler bilgilendirilmeli, mevzuatın gerektirdiği politika ve prosedürler hazırlanmalı ve sunulması zorunlu raporlar ilgili mercilere sunulmalıdır. Bu tedbirlerin yanı sıra kişisel verilerin bankacılık sektöründe işlenmesine ilişkin sektörel olarak kişisel veri işleme süreçlerinin de yer aldığı "Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi" ("**İyi Uygulama Rehberi**") yayınlamıştır. İnternet sitelerindeki verilerin bilgisayar korsanlığı ile ele geçirilmesi, deneme yanılma yöntemleri veya istihbarat çalışmaları sonucunda gerçekleşen kimlik hırsızlığı akabinde bankaların alternatif dağıtım kanalları kullanılarak müşteriler dolandırılabilmektedir (Yurtoğlu, 2020). Bazı durumlarda ise bankanın da sorumluluğuna neden olabilecek oltalama, kartların kopyalanması, sistem ve/veya yazılım açıklarının kullanılması, sosyal mühendislik, kötü niyetli/casus yazılımların kullanıldığı yöntemler de kişisel verilerin güvenliğine risk teşkil etmektedir (Yurtoğlu, 2020). Veri ihlal durumunda ihlale konu olabilecek verilerin niteliği de göz önüne alındığında; bankalar, uygun güvenlik düzeyini teminen gerekli tedbirleri almalıdır.

Bankalarda Kişisel Veri Güvenliğinin Tesisine Yönelik İdari ve Teknik Tedbirler

Bilgi sistemlerinin kullanımındaki artış, bilgi güvenliğinin sağlanması için birtakım asgari güvencelerin tesisini zorunlu kılmıştır. Bankalar, güven kuruluşu olarak nitelendirilmeleri sebebiyle kendilerine izafe edilen ağırlaştırılmış özen yükümlülüklerinin gereklerini gerçekleştirdikleri bankacılık faaliyetleri açısından ve bu faaliyetleri gerçekleştirdikleri tüm süreç boyunca yerine getirmelidirler.

Kişisel veri güvenliğinin sağlanmasına ilişkin yöntemleri belirleyen düzenlemelerin tüm teknolojik gelişmelere uygulanabilme kabiliyetini haiz olması mümkün olmamakla birlikte; bunlara ilişkin belirli bazı kriterlerin olduğu söylenebilir, bu kriterlere aşağıda yer verilmiştir (Develioğlu, 2017; Zor, 2020; Dülger, 2020; Korucu, 2021; Gündüz, 2022; Yürük, 2023).

- Verinin yetkisiz kişiler ile kötü niyetli kişilerin eline geçmesini engellemelidir. (Veri Gizliliği)
- Verinin bozulması, silinmesi veya değiştirilmesi engellenmeli ve verinin doğruluğunu sağlamalıdır. (Veri Bütünlüğü)
- Bilgiye kesintisiz, tam ve eksiksiz olarak ulaşılabilmeli ve bilgi kullanılabilir olmalıdır. (Erişilebilirlik)
- İlgili kişi ile verileri kayıt altına alan mekanizmaları kullanmaya yetkili kişilerin kimliğinin doğruluğu kontrol edilebilmelidir. (Kimlik Doğrulama)

- Verilerin işlenmesine ilişkin tüm süreçlerde; kullanılan sistemler, eksiksiz ve tutarlı olacak şekilde çalışmalıdır. (Güvenilirlik)

Bilgi güvenliği esas olarak; bilginin tespiti, bu bilgiler sebebiyle oluşabilecek zafiyetlerin belirlenmesi ve gerekli güvenlik kontrollerinin yapılması sonucu önlem alınmasını gerektirir (Vural & Sağıroğlu, 2008). Burada amaç bilginin kullanıcıdan alınması itibarıyla; bozulmadan, değişmeden, 3. tarafların yetkisiz/izinsiz erişimlerine maruz kalmadan asıl alıcısına iletilmesinin ve bu alıcı tarafından da aynı şartlarda depolanmasının (*ve gerekiyorsa tekrar iletilmesinin*) sağlanmasıdır (Vural & Sağıroğlu, 2008). Bankalar sadece faaliyetleri gereği sahip oldukları kişisel verilerin işlenme süreçlerinde değil, finansal ve ticari veriler ile müşteri sırrı niteliğinde veriler ile bankanın kendisine ait banka sırrı niteliğindeki verilerinin de güvenliğini tesis etmekle yükümlüdür. Bilgi Sistemleri Hakkında Yönetmelik'te; bilgi güvenliği süreç dokümanları, bilgi güvenliği politikası ve prosedürleri ile bilgi güvenliği yönetim sisteminin ne şekilde oluşturulması gerektiği düzenlenmiştir. Bilgi güvenliği politikası, tüm bilgi güvenliği faaliyetlerini içeren ve bu faaliyetlere ilişkin talimatlara yer veren; bilgi kaynaklarına erişim sağlayabilecek herkesin uymakla yükümlü olduğu kuralları içermektedir (Vural & Sağıroğlu, 2008). Bilginin yetkili kişilerce yetkileri dahilinde erişilebilir olması, bilgi gizliliğinin sağlanması amacıyla sadece yetkili/izin verilen kişilerin bilgiyi kullanabilir olması ve bilginin, ilk elde edildiği andaki şekliyle herhangi bir değişikliğe uğramadan, doğru, güncel, geçerli ve tam olması gerekmektedir (Çetin, 2014).

Kurum tarafından hazırlanan İyi Uygulama Rehberi, alternatif dağıtım kanallarına yer vermekte ve bu süreçlerde dikkat edilmesi gereken kişisel veri işleme faaliyetlerini açıklamaktadır. İyi Uygulama Rehberi'nde, sistemlerde işlenen bilgilerin güvenliği sağlanamadığında ülkemizde büyük ekonomik zarar ve ulusal güvenlik açıklarına, kamu düzeninde bozulmaya sebebiyet veriliyorsa, bu durumda bu sistemler kritik altyapı olarak nitelendirilmektedir. Ülkemizdeki yatırımların devamlılığını sağlayacak fon aktarımlarının bankalar aracılığı ile gerçekleştiği nazara alınınca (Aydın, 2018); bu altyapılardan biri olarak değerlendirilen bankacılık sektörünün, sektörün bu gereklerine göre düzenlenmiş birtakım düzenlemeleri takip etmesi gerektiği aşikardır (İyi Uygulama Rehberi, 2022).

Teknik tedbirler, sistemsel açıdan meydana gelebilecek risklerin belirlenmesini ve olası senaryolar ile bu risklerin elenmesini ve/veya risklerin gerçekleşmesi sonucu oluşabilecek zararların en aza indirilmesini amaçlar. Bankalarda siber güvenliğin sağlanması için katmanlı güvenlik mimarisinin esas alınması, bankanın iç ve dış ağındaki trafiğin kontrolünün sağlanması, iç ağ ve dış ağdan gelebilecek tehditlerin niteliğine göre iç ağ bölümlerinin oluşturulması gerekir (Bilgi Sistemleri Hakkında Yönetmelik, m.14). Hassas veriler ile sır kapsamındaki veriler ise özel iç ağda yer almalı ve bu özel iç ağda proxy (vekil) uygulamalar veya güvenlik duvarı cihazları aracılığıyla iletişim kurulmalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.14). Bu noktada banka iç ağından dışarıya aktarılan trafiğin içeriğinin kontrolü de ayrıca önem arz eder. Zira Bankacılık Kanunu m.73/3 uyarınca -istisnalar hariç olmak üzere- müşterilerin açık rızası alınmış olsa dahi, herhangi bir yazılı talimat veya talep olmadıkça yurtiçinde veya yurtdışındaki 3. kişilere müşteri sırrı niteliğindeki bilgiler aktarılamayacaktır. Buradaki açık rıza Kanun'daki açık rızadır ve hem tüzel kişi hem de gerçek kişi müşteriler için açık rızanın alınması gerekir. Ayrıca müşteriden alınan yazılı talimat yerine kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte bir talep veya talimat alınması da aynı işlevi görecektir (Bilgi Sistemleri Hakkında Yönetmelik, m.10; Kalıcı Veri Saklayıcısı tanımı için bkz. Banka Kartları ve Kredi Kartları Hakkında Yönetmelik m.4/l). Bankacılık faaliyetlerinin ifası sırasında ve dışarıdan temin edilen tüm hizmetlerde (dış hizmet alımı için bkz. Bilgi Sistemleri Hakkında Yönetmelik m.3/k) bilgi sistemlerinin kullanılması yoluyla edinilen, saklanan ve işlenen müşteri sırrı niteliğindeki bilgilerin aktarımı için de aynı şartlar geçerlidir (Bilgi Sistemleri Hakkında Yönetmelik, m.10). Bankalar verilerin taşındığı, işlendiği, saklandıkları ve yedeklendikleri ortamların gizliliğini sağlamakla ve cihazların ortadan kaldırılacağı durumlarda, verinin içerdiği gizlilik derecesine uygun bir imha yöntemi ile cihazları imha etmekle yükümlüdür (Bilgi Sistemleri Hakkında Yönetmelik, m.9). Ayrıca hassas veri söz konusuysa

bu durumda, farklı güvenlik seviyelerine sahip ortamların iletişiminin güvenliği için uçtan uca şifreleme tekniklerinin kullanılması ve hassas verilerin şifrelenmiş ortamlarda saklanması, banka personelinin de hassas veri veya sır niteliğindeki verileri içeren cihazlarının içeriğinin şifrelenmesi gerekmektedir (Bilgi Sistemleri Hakkında Yönetmelik, m.9). Belirtmek gerekir ki; şifrelenen içerik kadar, bu verilere erişim yetkilerinin belirlenmesi, buna yönelik yetki matrisleri hazırlanması ve kullanıcı hesapları yönetiminin sağlanması da gerekir (Kişisel Veri Güvenliği Rehberi, 2018). Bankalar, kullanıcının yetkileri ve görevlerinin kapsamına uygun olacak erişim kontrollerini tesis etmekle ve bunu sağlarken görevler ayrılığı prensibini benimseyip uygulamakla yükümlüdür. Bilgi güvenliğinin sürekliliğinin gerektirdiği üzere, kullanıcıların sisteme dahil olduğu andan sistemden çıktıkları ana kadar geçen süre için ve bu sürenin tamamı boyunca kullanıcıların doğrulanması sağlanmalı ve bu doğrulamayı garanti edecek bir yapı kurulmalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.11). Görevler ayrılığı prensibinden kasıt, kritik bir işleme ilişkin süreçlerin başlama, onaylanma ve tamamlanma aşamalarının tek bir kişi tarafından gerçekleştirilmeyeceği şekilde kurulması ve bu aşamaların yetkilerine ait talep, yetkilendirme ve yönetim süreçlerinin de birbirinden ayrı olmasıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.11).

Teknik tedbirlere ek olarak, alınması gereken idari tedbirler de mevcuttur. İdari tedbirler yapıları gereği operasyonel süreçlerde meydana gelmesi muhtemel riskleri ve bu süreçlerin yönetimini kapsamaktadır. Bu sebeple öncelikle bir veri envanteri oluşturulmalı ve bu veri envanteri kapsamında, işlenen kişisel verilerin ve hassas verilerin ayrı veri kategorileri olarak belirlenmesi gerekmektedir (Bilgi Sistemleri Hakkında Yönetmelik, m.20, Kişisel Veri Güvenliği Rehberi, 2018). Bankalar kurumsal yapıları gereği birçok farklı birim aracılığıyla veri toplamaktadır. Her birim kendi görev alanına giren konularda kişisel verileri işlemektedir. Örneğin; operasyon birimleri kimlik ve iletişim bilgilerini, hazine birimleri yatırım hesabı bakiyelerini, pazarlama birimleri harcama alışkanlıklarını incelemektedir (Yurtoğlu, 2020). Veri envanteri kapsamında veri kategorilerine ilişkin belirlemenin yapılması için; varlığın tanımı, banka içindeki değeri, varlığın sahibi, güvenlik sınıfı ve gizlilik, bütünlük ve erişilebilirlik gibi değerlerine yer verilmektedir (Bilgi Sistemleri Hakkında Yönetmelik, m.6). Veri envanteri hazırlanması; veri sızıntısı olması durumunda Banka nezdinde alınması gereken önlemlerin alınması, hangi veri gruplarının tehlikede olduğunun tespitinin yapılması ve sızıntının tespitinden bu sızıntının Kurul'a bildirimine kadar geçen sürecin mümkün olan en kısa sürede değerlendirilmesi için elzemdir. Bilgi sistemlerindeki muhtemel risklerin belirlenmesi, azaltılması, takibi ve raporlaması için bir yönetim süreci belirlenir (Bilgi Sistemleri Hakkında Yönetmelik, m.7). Bu yönetim süreci belirlenirken, risk seviyesini aşağı çekmek amacıyla en az yetki prensibi ile birimlerin yetkilendirilmesi gerekir (Yurtoğlu, 2020). Bu envanterde riskin tespiti, riske maruziyet oranları, etki değerlerinin tespiti ve buna istinaden risk derecelendirmeleri yapılmakta, hazırlanan raporlar ise üst yönetime sunulmaktadır (Bilgi Sistemleri Hakkında Yönetmelik, m.7). Bu raporun her bir riski ayrıca tanımlayan güncel risk aksiyon planı ile birleştirilmesi sonucu Bankanın Bilgi Sistemleri Risk Envanteri oluşturulur, ayrıca bu envanter sistematik olarak güncellenir ve iç kontrol ve iç denetim faaliyetlerine tabidir (Bilgi Sistemleri Hakkında Yönetmelik, m.7). Operasyonel olarak önem arz eden hususlardan bir diğeri ise; banka çalışanlarının bankadaki kişisel veri işleme süreçlerini, kişisel verilerin korunmasına ilişkin mevzuatı ve kişisel veri güvenliğine ilişkin alınması gereken teknik ve idari tedbirleri içeren bir bilgi güvenliği eğitimi almalarıdır. Bankalar, bilgi güvenliği seviyesini arttırmak için çalışanlarına ve dış hizmet sağlayıcılara Bilgi Güvenliği Komitesi tarafından onaylanan kapsamlı bir bilgi güvenliği farkındalık programı hazırlamalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.19/2). Bu komite, bir yönetim kurulu üyesi veya genel müdürün başkanlığında; ilgili birimlerin üst düzey yönetici ve temsilcilerinin katılımı ile yılda en az iki defa toplanan ve en az bir kez yönetim kuruluna rapor sunan bir komitedir (Bilgi Sistemleri Hakkında Yönetmelik, m.8). Eğitim programına ek olarak, kurum içi bültenler hazırlanmalı ve bu bültenlerde banka içi bilgi güvenliğine ilişkin bir bölüme yer verilmelidir (Bilgi Sistemleri Hakkında Yönetmelik, m.7; İyi Uygulama Rehberi, 2022). Kanun m.4 uyarınca kişisel verilerin işlenmesine ilişkin temel ilkelerden biri, kişisel veriler hangi amaçla işleniyorsa, bu amaçla bağlantılı, sınırlı ve ölçülü olacak kadar verinin işlenmesidir. Bu kapsamda öğretide "veri minimizasyonu" şeklinde de anılan ilke sebebiyle ve veri işleme sürecinin bir bütün olması da dikkate alındığında, kişisel veri işleme amacının gerektirdiği kadar kişisel veri toplanmalıdır (Biega & Finck, 2021; İyi Uygulama

Rehberi, 2022; Demirtaş, 2024). Ayrıca, kişisel verilere erişimi olan personel ile gizlilik anlaşmaları imzalanmalı, disiplin yönetmeliklerinde yaptırımlar düzenlenmeli ve kişisel verilerin korunmasına yönelik bilgi güvenliği, imha, saklama ve erişim politikaları oluşturulmalıdır (Kişisel Veri Güvenliği Rehberi, 2018).

Bilgi Sistemleri Hakkında Yönetmelik bilgi güvenliğine ilişkin nihai sorumluluğun bankanın Yönetim Kurulu'nda olduğunu düzenlemektedir (Bilgi Sistemleri Hakkında Yönetmelik, m.8). Bilgi güvenliğinin tesisi için risklerin belirlenmesi, sınıflandırılması, risk bazında senaryoların oluşturulması ve bu senaryoların gerçekleşmesinin önlenmesi, önlenemediği durumda ise bilgi güvenliği ihlalinden kaynaklanan zararların en aza indirilmesi gerekmektedir. Bilgi Sistemleri Hakkında Yönetmelik, risklerin yönetiminin sağlanması için Yönetim Kurulu tarafından bilgi sistemleri strateji planı oluşturulması ve Bilgi Sistemleri Strateji Komitesi ("**Strateji Komitesi**") ile Bilgi Sistemleri Yönlendirme Komitesi ("**Yönlendirme Komitesi**") kurulması gerektiğini düzenlemektedir. Strateji Komitesi strateji planının doğru uygulanmasından sorumludur ve yılda en az bir kez Yönetim Kurulu'na rapor sunmaktadır; Banka Yönlendirme Komitesi ise, esas olarak Strateji Komitesi'ne ve üst düzey yönetime yardımcı olması amacıyla; bilgi sistemlerine ilişkin projeleri takip etmek, çözmek ve mevzuata uyumluluğunu sağlamak başta olmak üzere Bilgi Sistemleri Yönetmeliği m.4/4'te sayılan diğer işlemleri yapmakla yükümlüdür ve Strateji Komitesi'ne yılda en az bir kere rapor sunmaktadır (Bilgi Sistemleri Hakkında Yönetmelik, m.4). Yönetim Kurulu oluşturulan bilgi sistemleri stratejisini onaylamalı, bilgi sistemleri politika ve prosedürlerini belirleyecek komitelerin kurulmasını sağlamalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.5). Burada temel amaç bilgi sistemlerine ilişkin risklerin yönetilmesidir. Risklerin yönetilmesini sağlayan ve bilgi varlıklarının korunmasını amaçlayan kontrolleri açıklayan bilgi sistemlerine ilişkin prosedür, süreç ve politikalar banka tarafından oluşturulmalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.5). Bu dokümanlar yılda en az bir defa gözden geçirilmeli, belgelenmeli ve gerektiğinde de güncellenmelidir (Yurtoğlu, 2020). Burada ayrıca yapılan değişikliklerin takibini sağlamak için önceki versiyon ve revizyon tarihi, düzenlemeyi onaylayan kişi ve gözden geçirme tarihine ilişkin bilgiler mutlaka kayıt altına alınmalıdır (Bilgi Sistemleri Hakkında Yönetmelik, m.5). Önemli olan, iyi bir güvenlik politikasının banka bünyesinde uygulanıyor olmasıdır (Aydın, 2018). Belirtmek gerekir ki; Bilgi Sistemleri Yönetmeliği'nde belirtilenler, bu kayıtlar hazırlanırken asgari olarak eklenmesi gereken bilgilerdir. Bankalar bunlara ek başka bilgileri de takibin sağlanması adına talep edebileceklerdir. Dikkat çeken bir husus, bilgi sistemleri politikasını doğrudan Yönetim Kurulu'nun onaylaması gerekirken; bilgi sistemleri prosedür ve stratejilerini Yönetim Kurulu veya Yönetim Kurulu'nun bu yönde yetkisini devrettiği yöneticiler onaylayabilir. TTK m.370/2 uyarınca Yönetim kurulu, temsil yetkisini şirket bünyesindeki müdürlere (*üçüncü kişiler*) devredebilir. Bu noktada, bankalar için "yönetici" olarak ifade edilen kişilerin Bankacılık Kanunu m.3 kapsamında bankanın genel müdürü, genel müdür yardımcıları, yönetim Kurulu, Denetim ve Kredi Komitesi üyeleri ile imza yetkisini haiz bölge, şube ve genel müdürlük teşkilatındaki bölüm, kısım veya grup gibi ve buna eşdeğer birim yöneticilerinin olduğunu belirtmek gerekir.

Kişisel Verilerin Korunması Kurulunun Bankacılık Faaliyetlerine İlişkin Kararlarının Bankalarda Kişisel Veri Güvenliği Açısından İncelenmesi

İlgili kişinin Kanun'un uygulanmasına ilişkin herhangi bir talebi varsa bu durumda; Kanun m.13 uyarınca veri sorumlusuna başvurmalıdır. İlgili kişinin bu talebi, veri sorumlusu tarafından en kısa sürede ve en geç otuz gün içinde sonuçlandırılır. İlgili kişinin veri sorumlusuna usulüne uygun olarak başvurması ancak veri sorumlusu tarafından bu talebinin reddedilmesi, verilen cevabın ilgili kişi tarafından yetersiz bulunması veya veri sorumlusunun süresinde başvuruya cevap vermemesi durumunda Kanun m.14 uyarınca; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz gün ve her durumda başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyette bulunabileceği gibi; ihlal iddiasını öğrenmesi durumunda veya şikâyet üzerine Kanun m.15 uyarınca Kurul da re'sen gerekli incelemeyi yapmaya yetkilidir. Kişisel veri güvenliğinin sağlanmasına ilişkin veri güvenliği

yükümlülüklerinin yerine getirilmemesi durumunda Kurul, bu yükümlülükleri yerine getirmeyen veri sorumlularına idari para cezası uygulamaktadır. Kurul idari para cezalarını uygularken gerekçeli olarak ihlalin kapsamını, bu ihlal kapsamında uygulanacak cezanın yasal temelini, Kanun'da kişisel veri işleme süreçlerini ve kişisel verilerin korunması hukukuna ilişkin düzenlemeleri somut olaylara uygulanan diğer mevzuat hükümlerini de inceleyerek karar vermektedir. Ayrıca kişisel verilerin ihlaline ilişkin yaygın bir uygulama söz konusu ise bu durumda Kurul İlke Kararları almaktadır (Kanun, m.15). Örneğin, sağlık ve bankacılık gibi sektörlerde kamu kuruluşları ve özel kurumlar tarafından verilen hizmetlerde hizmet alan kişilerin, banko veya gişe gibi hizmet yerlerinde birbirini duymamasını temin edecek önlemlerin alınması ve yetkisi olmayan kişilerin bu bölümlerde yer almamasının temin edilmesi gerektiği, Kurul'un 2017/62 sayılı ve 21/12/2017 tarihli İlke Kararı'nda belirtilmiştir. Çalışmanın bu bölümünde bankaların faaliyetlerini gerçekleştirirken, veri güvenliğinin sağlanması açısından gerekli tedbirlerin alınıp alınmadığına ilişkin Kurul kararları incelenecektir.

Bankalar, müşteri ile ilişkilerinin kurulduğu ilk andan itibaren ilgili kişilerin kimlik ve iletişim bilgilerini işlemektedirler. Banka müşterilerinin iletişim bilgileri, ilgili kişinin iletişim tercihlerine göre, reklamcılık ve/veya ürün teklifleri için kullanılabileceği gibi bankanın müşteri ile arasındaki ilişkinin kurulması, sözleşmelerin ifası gibi banka tarafından yapılan işlemlerin takibinin gerektirmesi sebebiyle kullanılmaktadır. Kurul'un 2019/277 sayılı ve 18/09/2019 tarihli Karar Özeti'nde, ilgili kişinin kendisine ait iş ve işlemler için irtibata geçilmesi için bankaya verdiği telefon numarasının; eşinin müdürü olduğu şirkete ilişkin olarak ve ilgili kişinin eşiyle irtibata geçilmesini amaçlayarak kullanılması, hukuka aykırı bir kişisel veri işleme faaliyeti şeklinde değerlendirildiğinden, veri sorumlusu bankaya idari para cezası uygulanmıştır. Ayrıca, ilgili kişinin iletişim bilgilerini kapsayan kişisel verilerinin üçüncü kişilere aktarılması ve üçüncü kişiler ile paylaşılması da her olay bazında değerlendirilmeli ve somut olaya göre ilgili kişinin makul olarak paylaşılmasını bekleyeceğinden daha fazla kişisel verisi paylaşılmamalıdır. 2022/224 sayılı ve 10/03/2022 tarihli Kurul Karar Özeti'nde; ilgili kişi, veri sorumlusu bankanın müşterisine ait bir kartı bulmuş ve kartın sahibine teslimi için bankanın çağrı merkezi ile iletişime geçmiştir. Yapılan görüşmeye istinaden ilgili kişi, kişisel bilgilerinin paylaşılmasını istememesine rağmen; çağrı merkezi personeli tarafından "*(...)kartı sizin bulduğunuzu ileteceğim (...)*" ifadesine ilgili kişi tarafından tamam denilmesi sebebiyle ilgili kişinin telefon numarasının kart sahibi ile paylaşılması veri güvenliği ihlali olarak değerlendirilmiş ve veri sorumlusu bankaya idari para cezası uygulanmıştır. Zira, kartı kimin bulduğunun kart sahibine bildirilmesine olumsuz bakan ilgili kişinin yukarıdaki ifadeye tamam demesi sebebiyle, banka tarafından iletişim bilgilerinin paylaşılmasının beklenmesi uygun görülmemiştir.

Bankaların müşterileri ile iletişim sağladıkları kanalların güncel tutulması gerekir. Bankada kayıtlı e-posta adresinin, ilgili kişinin eski ortağı olduğu şirketin vekili olan üçüncü kişinin e-posta adresi olması sebebiyle, üçüncü kişilerin ilgili kişinin hesap bilgilerini öğrendiği; ancak kendisine sunulan evraklar imzalanırken ilgili kişinin bu e-mail adresinin bulunduğu forma onay verdiği ve sonradan talebi üzerine banka tarafından hemen e-mail adresinin düzeltildiği 2023/67 sayılı ve 12/01/2023 tarihli Kurul Karar Özeti'ne konu olayda ise; 2020/966 sayılı ve 22/12/2020 tarihli İlke Kararı'na atıfta bulunularak, banka işlemlerinde kullanılan ilgili kişilere ait iletişim bilgilerinin belirli aralıklarla doğrulanması ve bu bilgilerin güncelliğinin sağlanması gerektiği belirtilmiştir. İlgili kişinin hesap açtırma talebi ile bir banka şubesine gittiği ve daha önce hiç gitmediği bir şubede hesabının olduğunu öğrendiği 2020/103 sayılı ve 06/02/2020 tarihli Kurul Karar Özeti'nde ise veri sorumlusu banka, potansiyel müşteri edinimi için 3. bir taraftan ilgili kişiye ait bilgileri temin ettiğini ancak müşteri ile herhangi bir sözleşme imzalanmadığı için henüz müşteri numarasının etkinleştirilmediğini belirtmiştir. Kurul, her ne kadar ilk hesap açılışı Kanun'un yürürlük tarihinden önce olsa da Banka'nın ilgili kişinin talebi üzerine 2018 yılında verdiği cevapta ilgili kişinin verilerini hala bulundurması sebebiyle, bu faaliyetin herhangi bir veri işleme şartına dayanmadığını ve genel ilkelere aykırı olduğunu belirtmiş, bankaya idari para cezası uygulamıştır.

Bankaların temel faaliyetlerinden biri müşterilere kredi verme işlemleridir. Bankacılık Kanunu m.48 kredi olarak kabul edilen işlemleri belirtmiştir. Bu kapsamda; nakdî ve gayrinakdî krediler, verilen ödünçler, satın alınan tahvil ve benzeri sermaye piyasası araçları, varlıkların vadeli satışından doğan alacaklar, vadeli işlem ve opsiyon sözleşmeleri ile Kurul tarafından kredi olarak kabul edilen işlemler gibi banka tarafından verilen taahhütler ve üstlenilen risklerin bir kısmı kredi olarak değerlendirilmektedir. Kredilerin açılması öncelikle kredi talebinde bulunan tüzel veya gerçek kişinin risk grubunun ve buna istinaden kredi açılıp açılmayacağını ve açılacaksa açılacak kredinin limitinin belirlenmesini gerektirir. Bankaların Kredi İşlemlerine ilişkin Yönetmelik m.7 kredi verilmesi işlemleri sebebiyle bankanın maruz kalacağı risklerin ölçülmesi, kredi alan tarafın malî gücünün düzenli analizi ve takibi, gerekli bilgi ve belgelerin temini ve bunlara ilişkin esasların belirlenmesi yükümlülüğünü bankalara yüklemiştir. Kurul 2020/43 sayılı ve 16/01/2020 tarihli Karar Özeti'nde ilgili kişi ile aynı risk grubu içinde yer alan kişilerin kişisel verilerinin sadece kendi bünyesinde kullanılmak maksadıyla bankacılık faaliyetleri kapsamında işlenmesinin hukuki yükümlülüklerin yerine getirilmesi kapsamında olduğunu değerlendirmiş ancak; risk grubundaki bir kişinin borç bilgisinin paylaşılmasının bankacılık faaliyetleri dikkate alındığında müşterilere bildirimde bulunma yükümlülüğünün kapsamında olmayacağını ve veri güvenliğinin ihlal edildiğini ifade etmiştir. Bir başka olayda, Kurul tarafından risk merkezi üzerinden yapılan sorgulardan elde edilen kişisel verilerin finansal kuruluşlarca kullanımına ilişkin değerlendirmede bulunulmuştur. Bankacılık Kanunu Ek madde 1 uyarınca Kanunen risk merkezine üye olması öngörülen finansal kuruluşlar ve kredi kuruluşlarının, talep edilmesi durumunda, müşterilerin tüm bilgilerini Risk Merkezi'ne vermesi gerekmektedir. 2021/79 sayılı ve 03/02/2021 tarihli Karar Özeti'nde; banka müşterisi olan ilgili kişiye ulaşmak amacıyla risk merkezinden ilgili kişiye ilişkin bilgilerin sorgulanması akabinde bu kişinin ablası ve babasının arandığı olayda, bankanın kendisi ile müşterisi arasında olan ilişkiyi bu kişilerle paylaşmasının herhangi bir veri işleme şartına dayanmaması sebebiyle bankanın kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünün ihlal edildiği belirtilmiş ve bankaya idari para cezası uygulanmıştır. Bu noktada gerçekleştirilen banka içi denetim faaliyetlerinin de bankalarda bilgi güvenliğinin sağlanması noktasından önem arz ettiğini belirtmekte yarar vardır. Bu açıdan, 2020/344 sayılı ve 05/05/2020 tarihli Kurul Karar Özeti'ne konu olayda, banka iç kontrol süreçlerinde ortaya çıkan şüpheli Kredi Kayıt Bürosu (KKB) sorgulamalarına ilişkin Teftiş Kurulu tarafından gerçekleştirilen incelemeler sonucunda, KKB sorgusu yapma yetkisini haiz 3 banka personeli tarafından 3. kişilerden elde edilen kimlik numaralarına istinaden banka müşterisi olan ve olmayan kişilerin kredi bilgilerine erişildiği kaydedilmiştir. Kurul ihlallerin tespiti arasında geçen sürenin uzunluğu sebebiyle düzenli olarak erişim kontrollerinin gerçekleştirilmediğine, banka çalışanlarında yeterli düzeyde farkındalık yaratılmadığına ve ihlal sonrası tedbirlerde yapılan değişikliklerin aslında gerekli tedbirlerin ihlalin gerçekleştiği dönemde yeterince alınmadığına işaret ettiğini belirtmiş ve veri sorumlusu bankaya idari para cezası uygulamıştır.

Banka Kartları ve Kredi Kartları Hakkında Yönetmelik m.21/4 uyarınca, kart çıkaran kuruluş olmaları sebebiyle; bankalar kart basım aşaması dahil, kartın hamile teslimine kadar müşteriye ilişkin bilgilerin gizliliğini sağlamak adına uygun kontrol ortamını kurmalı ve muhtemel suiistimallere karşı gereken tedbirleri almalıdır. Kurul'un 2020/32 sayılı ve 16/01/2020 tarihli Karar Özeti'nde; ilgili kişinin beyan ettiği adrese kartın tesliminin sağlanamadığı ve bu sebeple kayıtlı ikinci adreste bir kişiye teslimin gerçekleştiği, buna ilişkin ilgili kişiye herhangi bir bildirim yapılmadığı ve kişinin ilk adresine teslim sağlanamamış olmasına karşın sistemde birinci adrese teslimatın sağlandığı belirtilmiştir. Karayolu Taşıma Yönetmeliği m.40/5 kapsamında taşıma yapan firma sunduğu hizmet açısından gönderici ve alıcıya ilişkin bilgileri tam ve doğru olarak kaydetmekle yükümlüdür. Bu açıdan taşımayı yapan şirket bu veriler için veri sorumlusu olarak nitelendirilmektedir. Karar kapsamında ilgili kişilerin bilgilerin güncelliğini temin etmeyen bankaya veri güvenliğinin ihlali sebebiyle idari para cezası uygulanmıştır.

Bankalar tarafından, yapılan harcamaların kart hamilince incelenmesi ve takibinin sağlanması amacıyla; hesap özeti bilgileri ilgili kişiye tebliğ edilmektedir. Hesap özeti, elektronik ortamda olabileceği gibi

basılı bir nüsha şeklinde de tanzim edilebilir. Kurul'un 2020/78 sayılı ve 30/01/2020 tarihli Karar Özeti'nde; ilgili kişinin şahsi banka hesabına ilişkin harcama hareketlerini içeren hesap özeti, sehven ilgili kişinin ticari hesaplarına ilişkin beyan edilen e-posta adresine iletilmiştir. Bankanın, ilgili kişinin hesap özetini e-ekstre ortağı olduğu firmanın kayıtlı e-posta adresine göndermesi Kanun'da yer alan veri işleme şartlarına aykırı olduğundan, yapılan aktarımın da hukuka aykırı olduğu belirtilmiş ve veri sorumlusu bankaya idari para cezası uygulanmıştır.

Bankalar, müşterilerine tanıtım ve reklam faaliyetleri kapsamında elektronik ticari ileti göndermektedir. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ("**Elektronik Ticaret Kanunu**") m.6/1 uyarınca ticari elektronik ileti gönderilebilmesi için, önceden alıcıların onayları alınmalıdır. Kurul'un 2021/361 sayılı ve 13/04/2021 tarihli Karar Özeti'nde; ilgili kişinin talebi veya izni olmaksızın, android işletim sistemine sahip cihazları olan müşterilerin bankanın uygulamasını yüklemesi durumunda elektronik ticari iletilerin otomatik olarak onaylı geldiği ve onay iptal edilmesi isteniyorsa, bunun müşteriler tarafından değiştirilmesi gerektiği belirtilmiştir. Kurul, bu şekilde bir veri işleme faaliyetinin yaygınlığı ve bu faaliyetin hukuka aykırılığı dikkate alındığında veri güvenliği riski oluştuğunu belirtmiş ve açık rıza alınmadan otomatik onaylı ticari elektronik izinlerin gönderilmesi sebebiyle uygun güvenlik düzeyini teminen alınması gereken tedbirleri almayan veri sorumlusu bankaya idari para cezası uygulamıştır. Ancak bankalar kanunen bazı bildirimleri yapmak zorundadırlar. Bu sebeple Kurul'un 2021/358 sayılı ve 13/04/2021 tarihli Karar Özeti'nde de belirtildiği üzere, yasal bilgilendirme içeren iletiler söz konusuysa, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik ("**Elektronik İletiler Hakkında Yönetmelik**") m.6/2 uyarınca hizmet sağlayıcının kanuni bilgi verme yükümlülüğü kapsamında ilgili kişinin gönderilen elektronik iletiye onayı aranmamaktadır, meğerki herhangi bir ürün ya da hizmetin tanıtım veya özendirilmesi de bu ileti ile sağlanıyor olmasın. Ancak bilgi verme yükümlülüğünün de sınırı ilgili kişinin kişisel verilerinin akıbetine ilişkin taleplerine göre değerlendirilmektedir. 2021/1104 sayılı ve 02/11/2021 tarihli Kurul Karar Özeti'nde veri sorumlusu Banka, covid-19 salgını döneminde banka nezdinde alınan önlemleri açıkladığı kısa mesajları bankadan hizmet almış olan tüm müşterilere iletmiştir. Ancak Kurul'a başvuruda bulunan ilgili kişi, Banka nezdindeki tüm hesaplarını pasife alması ve iletişim tercihlerini tüm elektronik iletilere kapalı hale getirmesi sebebiyle Kurul'a başvurmuş ve Kurul, ilgili kişinin kişisel verilerinin işlenmesi yoluyla kendisine kısa mesaj gönderilmesinin hukuki herhangi bir dayanağı olmadığına karar vermiş ve veri sorumlusu banka hakkında idari para cezası uygulamıştır.

Bankalar, mevduat kabulü veya her türlü kredi verme işlemleri hariç olmak üzere; faaliyetlerin kendi adına gerçekleştirilmesi için destek hizmeti kuruluşlarından faydalanabilir. Destek hizmeti kuruluşları banka sırrı veya müşteri sırrı niteliğindeki verilere erişim imkanına sahip olacaksa bu durumda destek hizmet kuruluşuna sağlanan veri işin gerektirdiği kadar veri ile sınırlı olmalıdır (Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik m.5/8). 2022/768 sayılı ve 03/08/2022 tarihli Kurul Karar Özeti'nde, ilgili kişi bir sigorta şirketi tarafından sürekli aranması sebebiyle ilgili sigorta şirketi ile yaptığı görüşmede, bir banka tarafından iletişim bilgilerinin taraflarına sağlandığı bilgisine ulaşmıştır. Kurul tarafından yapılan değerlendirmeler sonucunda, banka tarafından ilgili kişinin elektronik ticari izinlere onay verdiğini gösteren talimatta, verilerin aktarılacağına dair açık bir ibare yer almadığı ve bu sebeple açık rızanın "bilgilendirmeye dayalı olma" şartının yerine getirilmediği; sonraki tarihte banka tarafından kullanılacak kanalları ve tanıtılacak ürünleri de kapsayan rızanın "özgür iradeye dayanma" şartını sağlamayacağı, ayrıca onay verilen talimatın otomatik onaylı (opt-out) olmaması gerektiği belirtilmiştir. Bunun yanında her ne kadar, Elektronik İletiler Hakkında Yönetmelik, Elektronik Ticaret Kanunu'nun yürürlüğünden önce doğrudan hizmet teminine ilişkin kurulan ilişkilerden elde edilen veriler için ilgili kişiye ait iletişim bilgisini onaylı veri saysa da; bu maddenin banka tarafından sigorta şirketine yapılan aktarım için hukuki gerekçe olarak kabul edilemeyeceği sonucuna ulaşılmıştır. Son olarak; sigorta acenteleri, sigortacılık faaliyetinde bulunuyor olmaları sebebiyle finansal kuruluş olarak değerlendirilmektedir. Bankacılık Kanunu m.73/4 kapsamında finansal kuruluşlar ve bankalar arasında yapılan bilgi ve belge aktarımlarının (doğrudan aktarımlar) veya gerekli tedbirlerin alınması durumunda,

bankalar ve finansal kuruluşlar arasında hizmet alımları kapsamındaki işlemlerde kullanılan bilgi taleplerinin yerine getirilmesi; taraflar arasında bir gizlilik sözleşmesinin varlığı söz konusuysa ve belirtilen amaçlarla sınırlı bir aktarım varsa, bu aktarımlarda banka sırrı ya da müşteri sırrı niteliğindeki bilgilerin öğrenilmesi bankaların sır saklama yükümlülüğü dışında kabul edilmiş yani bu yükümlülükten istisna tutulmuştur (Ayrıca bkz. Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik m.5/2(a)). Ancak yapılan değerlendirmede bu nitelikte bir gizlilik sözleşmesinin de Kurul'a sunulmadığı değerlendirilmiş ve veri sorumlusu bankanın hiçbir kişisel veri işleme sebebine dayanmadan veri aktarımını gerçekleştirmesi sebebiyle; bu veri aktarımının kişisel verilerin hukuka aykırı olarak işlenmesine yol açtığı belirtilmiş ve Kurul, veri güvenliğinin ihlal edilmesi sebebiyle veri sorumlusu bankaya idari para cezası uygulamıştır.

Bankalar, bankacılık faaliyetlerinin niteliği gereği bulundurdukları verilerin saklandığı ortamlardaki güvenliğin sağlanmasına ek olarak; bu verilere kimler tarafından hangi amaçlarla erişilebileceğini de belirlemelidir. Zira yetkisiz ve amacına aykırı veri işleme faaliyetleri, Kanun m.4/2(a) ve 4/2(c)'de öngörülen kişisel verilerin işlenmesindeki genel ilkelere uygun olmayacaktır. Kurul, 2018/63 sayılı ve 31/05/2018 tarihli İlke Kararı kapsamında da görev veya pozisyonları sebebiyle kişisel verilere erişebilenlerin, yetkilerini aşması ve/veya kötüye kullanarak kişisel amaçlarla veya nedenlerle verilerin işlenme amacı dışında kişisel verileri işlemesini ve/veya verilerin üçüncü kişilerle paylaşılmasını veri güvenliğine aykırılık olarak kabul etmiş ve veri sorumlusu tarafından gerekli tedbirlerin alınması gerektiğini bildirmiştir. Bir banka görevlisi tarafından boşanma aşamasında olduğu eşine ait bilgilerin sorgulanması sonucu, elde edilen bilgilerin mahkemeye sunulduğu 2021/32 sayılı ve 12/01/2021 tarihli Kurul Karar Özeti'nde ise; ilgili kişi tarafından yapılan başvuruya istinaden Kurul, veri sorumlusunun bünyesindeki düzenlemelere ilişkin bir liste dışında kişisel verilerin işlenmesine ilişkin kurum içi düzenlemelerini ya da ilgili personelin eğitimine ilişkin bilgi sunmadığını, bu sebeple veri sorumlusunun gerekli idari ve teknik tedbiri almadığını belirtmiş ve veri sorumlusu bankaya idari para cezası uygulamıştır.

Bankaların müşterilerinden alacakları mevcuttur. Bu alacakların tahsil edilemediği noktada; icra takibi başlatılması ve/veya icra takiplerinin varlık yönetim şirketlerine devredilmesi gibi tahsilat yöntemleri ile bankalar alacaklarını tahsil etmekte ya da alacaklarını tahsil etmek amacıyla birtakım alacak haklarını varlık yönetim şirketlerine devredebilmektedir. Bu kapsamda yapılacak icra takipleri varlık yönetim şirketleri nezdinde gerçekleştirilmektedir. 2021/424 sayılı ve 27/04/2021 tarihli Kurul Karar Özeti'nde, ilgili kişinin T.C. Kimlik numarası sehven banka kayıtlarını alınmış ve bu sebeple banka tarafından temlik edilen alacaklar sebebiyle varlık yönetim şirketi, kredi borçlusu olarak kaydedilen ilgili kişi ile kendisine ait olmayan bir borcun ödenmesine ilişkin irtibata geçmiştir. Bankaya yapılan başvurular sonucunda T.C. kimlik numarası düzeltilmiş olmakla birlikte, varlık yönetim şirketi nezdinde gerekli düzeltmeler yapılmadığından ilgili kişi varlık yönetim şirketi tarafından aranmaya devam etmiştir. Kurul, ilgili kişi tarafından kişisel verilerini içeren belgelerin veri sorumlusuna iletilmesine rağmen düzeltmenin yapılmamasını hukuka aykırı veri işleme faaliyeti olarak değerlendirmiş ve gerekli tedbirleri almayan varlık yönetim şirketine idari para cezası uygulamıştır. Bankalar ayrıca haciz ihbarnamesi göndermek suretiyle de alacaklarını tahsil etme yoluna gidebilirler. Burada önem arz eden ve sıklıkla uyuşmazlık konusu olan husus, 2004 sayılı İcra ve İflas Kanunu'nun ("**İİK**") 89. maddesi uyarınca, borçlunun üçüncü bir şahıstaki alacak hakkı, talep hakkı veya taşınır bir malının haczi durumudur. Zira bu durumda, üçüncü kişilerin kişisel verileri; haciz ihbarnamesinin gönderilmesi ve borçlunun haciz ihbarnamesi gönderen kişiye olan borcunun, başkasının elinde bulundurduğu malı aracılığıyla tahsilini sağlamak amacıyla işlenmektedir. 2021/909 sayılı ve 09/09/2021 tarihli Kurul Karar Özeti'nde; ilgili kişinin kardeşine İİK m.89/1 uyarınca haciz ihbarnamesi gönderilerek kişisel verilerinin işlenmesi; avukat ile veri sorumlusu arasındaki vekalet ilişkisi kapsamında hukuka uygun bir veri işleme faaliyeti olarak değerlendirilmiştir. Ayrıca Kurul 2021/1069 sayılı ve 21/10/2021 tarihli Karar Özeti'nde; borçlunun üçüncü kişideki alacak hakkı, talep hakkı veya taşınır bir malının haczi için aynı haciz ihbarnamesinde tüm üçüncü kişilerin bilgilerinin yer almasını da yapılan işlemlerin doğası

gereği, ilgili kişilerin kimlik ve irtibat bilgilerinin avukat tarafından icra dairesi ile paylaşılması kapsamında hukuka uygun olarak değerlendirmiştir.

Kurul, özel nitelikli kişisel veriler işlendiğinde sağlıklı bir açık rızanın mevcut olduğu durumlarda; veri işleme faaliyeti kapsamında toplanan verilerin hukuka uygunluğunu, kişisel verilerin korunmasına ilişkin genel ilkeler kapsamında incelemektedir. Eğer toplanan özel nitelikli veri, verinin toplanma amacının gerektirdiğinden daha fazlaysa veya başka bir anlatımla, bu verinin toplanması yapılacak veri işleme faaliyeti kapsamında ölçülü değilse; bu durumda kişisel verinin işlenmesine ilişkin ilgili kişinin verdiği açık rıza hukuka uygun olsa da kişisel verinin işlenmesi veri koruma hukukunun genel ilkelerine aykırı olacağından, özel nitelikli kişisel verinin işlenmesi hukuka uygun kabul edilmeyecektir. Bu açıdan, spor salonu kararları öğretide önem arz etmektedir. Spor salonu üyeliği için üyelik talebinde bulunan müşterilere alternatif herhangi bir kanal sunulmadan, üyenin giriş çıkış kontrolünün ilgili kişinin el ve parmak izinin taranması sonucu biyometrik verilerinin işlenmesi suretiyle gerçekleştirildiği 2019/81 sayılı ve 25/03/2019 tarihli Kurul Karar Özeti ve 2019/165 sayılı ve 31/05/2019 tarihli Kurul Karar Özeti uyarınca, zorunlu olarak biyometrik verilerin işlenmesinin minimum düzeyde veri toplanması ilkesine uymayacağı belirtilmiş ve ilgili kişiler açık rıza vermiş olsa da özgür bir rıza verilebilmesi için açık rızanın hizmetin ön şartı olarak sunulmuyor olması gerektiği ifade edilmiştir. Giriş-çıkışların seçimlik haklarla doğrulanmasının imkân verilen bir olaya ilişkin 2020/167 sayılı ve 27/02/2020 tarihli Kurul Karar Özeti'nde ise; ilgili kişinin her ne kadar açık rızasında herhangi bir sakatlık olmasa da spor salonu giriş çıkışlarında biyometrik verilerin işleniyor olması minimum veri toplama ilkesine uygun bir veri işleme faaliyeti olmayacağından; ölçülülük ilkesine aykırı kabul edilmiştir. Ancak ilgili kişilerin finansal bilgilerini barındıran bankalar, yaptıkları doğrulama işlemlerinde; Bilgi Sistemleri Hakkında Yönetmelik m.34 uyarınca her türlü elektronik bankacılık hizmetinde müşterinin kimliğinin doğrulanması adına "müşteriye ait olan", "müşteri tarafından bilinen" veya "biyometrik bir karakteristiği olan" bilgilerden farklı ikisini içeren bilgileri kullanmalıdır. 2023/1310 sayılı ve 03/08/2023 tarihli Kurul Karar Özeti uyarınca ilgili kişi, banka tarafından mobil bankacılık kanalını kullanmak için dijital parola belirleme işlemlerinde bankanın kurumsal müşterilere, dijital parola belirleme yöntemlerinden sadece T.C. Kimlik Kartı ile dijital parola üretilmesine imkân verildiğini ve bu durumda ilgili kişinin yüz verisinin de işlenmesinin zorunlu olduğunu belirtmiştir. Banka, kurumsal müşterilere dijital kanallardan biyometrik verileri işlenmeksizin banka/kredi kartı kullanılarak parola belirleme imkanının sonraki bir tarihte tanındığını, bu imkân olmasa bile kurumsal müşterilerin şube aracılığıyla veya telefon bankacılığı ile parola belirleme imkânı olduğunu ifade etmiştir. Kurul yaptığı değerlendirmede, yüz tanıma yönteminde kullanılması amacıyla toplanan verilerin biyometrik veri olarak değerlendirilmiş ve banka tarafından açık bir yönlendirme içermese de dijital parola belirlemek için mobil bankacılık dışında alternatif kanalların da mevcut olduğu dikkate alındığında, ilgili kişilerin verdikleri açık rızanın geçerli olduğuna ve veri sorumlusu banka hakkında herhangi bir işlem yapılması gerekmediğine karar vermiştir.

Kişisel Veri Güvenliği İhlali Durumunda Kişisel Verilerin Korunması Kanunu Çerçevesinde Veri Sorumlularına İdari Para Cezası Uygulanması

Kanun m.18/1(b) uyarınca, kişisel verilerin güvenliğinin sağlanması için gerekli yükümlülüklerin yerine getirilmemesi durumunda bu yükümlülüğü yerine getirmeyenlere her sene yeniden değerleme oranında artış gösteren idari para cezası uygulanacaktır. Burada sorumluluk 5326 sayılı Kabahatler Kanunu ("**KK**") kapsamında incelenmektedir. Kanun m.18/2 uyarınca kişisel veri güvenliğini sağlama yükümlülüğünün ihlali durumunda idari para cezası "*(...) veri sorumlusu (...) gerçek kişi ile özel hukuk tüzel kişileri hakkında uygulanmaktadır.*" KK kapsamında fail yalnızca gerçek kişi olabilir (Kangal, 2019). Ancak KK m.8/1 uyarınca veri sorumlusunun özel hukuk tüzel kişisi olması durumda bu tüzel kişinin organ veya temsilcisi olan ya da tüzel kişi faaliyeti çerçevesinde görev üstlenen kişinin üstlendiği görev kapsamında işlediği kabahat sebebiyle tüzel kişi hakkında da idari para cezası uygulanmaktadır (Kangal, 2019). Burada tüzel kişi fail olarak nitelendirilmemekle birlikte idari para cezasının muhatabı

olabilecektir. Önemle belirtmek gerekir ki, tüzel kişinin yetkilendirdiği gerçek kişi fail olsa bile Kanun'un açık hükmü gereği sadece veri sorumlusu tüzel kişi hakkında idari para cezası uygulanacaktır (Kangal, 2019). Kamu hukuku tüzel kişileri ise Kanun m.18/2 kapsamında olmadığından, tüzel kişi tarafından yetkilendirilen gerçek kişinin fiilinden dolayı tüzel kişi veri sorumlusu hakkında idari para cezası uygulanmayacaktır (Kangal, 2019), bu kişiler için Kanun m.18/4'te ayrı bir prosedür öngörülmüştür.

SONUÇ VE DEĞERLENDİRME

Dijitalleşme, sistem ve cihazlara bağlılığı arttırmış ve bunun sonucunda birçok verinin ulaşılabilir olması ile teknolojik ortamlarda etkileşim oranının artması; kişisel verilerin güvenliğine ilişkin sorunlara zemin hazırlamıştır. Kişisel verilerin teknik anlamda ne şekilde işlendiğinin belirlenmesi, hangi hukuki gerekçeler ile veri işleme faaliyetlerinin sınırlanabileceği, veri işleme faaliyetlerinin hukuka aykırılığı durumunda uygulanması muhtemel yaptırımların veri sorumlusu ve veri işleyenlere ne oranda ve hangi sorumluluk kapsamında addedilebileceği mevzuat kapsamında düzenlenmiş ve Kurul aracılığıyla verilen kararlar ve Kurum tarafından yayınlanan Rehberler ile sektörel olarak değerlendirilmiştir.

Kişisel veri güvenliği; verilerin ilk toplandığı andan, kanuni yükümlülükler gereği verilerin saklanmasını gerektiren sebeplerin ortadan kalktığı ana kadar devam eden bir süreçtir. Her sürecin kendine özgü bir yönetim gerektirmesi sebebiyle kişisel veri güvenliğinin sağlanması da bir süreç yönetimi gerektirir. Veri ihlali riski teknolojik sistemlerde her zaman mevcuttur, önemli olan bu risklerin minimize edilmesini temin edecek sistemlerin kurulması, yöntemlerin belirlenmesi ve bu yöntemlerin uygulanmasıdır. Bankacılık sektörünün ana aktörü bankalar; faaliyetleri gereğince müşteri ilişkilerinin kurulması, yükümlülüklerin ifası ve bu ilişkilerin sonlandırılması süreçlerinde topladıkları verilerin güvenliğini sağlarken; mevzuatın ve yargı kararlarının kendilerine yüklediği güven kuruluşu olma niteliğini de göz önünde bulundurmalıdırlar.

Kurul, bankaların yükümlülüklerini de dikkate alarak; kişisel verilerin korunması hukuku ve ilkelerini somut olaya uygulamakta ve buna istinaden değerlendirmelerde bulunmaktadır. Operasyonel süreçlerdeki aksaklıklar birçok veri ihlaline sebebiyet vermektedir. Bankalar mevzuatta ve rehber niteliğindeki dokümanlarda yer verilen tedbirleri almalı ve operasyonel risklerin minimizasyonuna yönelik olarak banka içi eğitimleri ve bilinçlendirme faaliyetlerini etkili bir yöntemle ve eğitim içeriğinin güncelliğini sağlayarak gerçekleştirmelidir. Özellikle GVKT'de düzenlenen tasarımdan itibaren (*data protection by design)* ve varsayılan olarak *(data protection by default*) verilerin korunması ilkeleri uygulamada etkili şekilde kullanılmalı ve veri işleme süreçlerinin en başından itibaren banka müşterilerinin kişisel verilerini en az ihlal edecek nitelikte sistemlerin oluşturulmasına yönelik prensipler uygulanmalı ve kişisel veriler olabilecek en üst seviyede korumadan yararlanmalıdır.

KAYNAKLAR

Akkurt, S. S. (2023). "Açık Rıza", iç. Kişisel Verilerin Korunmasına Akademik Bakış - KVKK Akademi Derleme Çalışması (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik, 155-195.

Aksoy, H. C. (2010). Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması. Ankara: Çakmak Yayınevi.

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.

Aydın, S. (2018). Bankacılık Sektöründe Kişisel Verilerin Korunması ve İşlenmesinin Bireyler Üzerinde Algısı ve Etkileri. [Yayınlanmamış yüksek lisans tezi]. T.C. İstanbul Arel Üniversitesi.

Ayözger Öngün, A. Ç. (2019). Kişisel verilerin korunması hukuku: Elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil. İstanbul: Beta Basım Yayın.

Bankacılık Düzenleme ve Denetleme Kurumu. (2022). Sır Niteliğinde Bilgilerin Paylaşılması Hakkında Yönetmeliğin uygulamasına ilişkin 2022/1 sayılı Genelge. https://www.bddk.org.tr/Mevzuat/DokumanGetir/1135 (Erişim Tarihi: 24.10.2024).

Başar, C. (2020). Türk idare hukuku ve Avrupa Birliği hukuku ışığında kişisel verilerin korunması. İzmir: On İki Levha Yayıncılık.

Biega A. J. & Finck M. (2021). ''Reviving Purpose Limitation and Data Minimisation in Data Driven Systems'' Technology and Regulation.

Börekçi, E. B. (2020). Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu (TCK m. 136). On İki Levha Yayıncılık.

Candemir A. (2020). Bankacılık Sektöründe Kişisel Verilerin Korunması Alanında Yaşanan Gelişmeler. https://blog.lexpera.com.tr/bankacilik-sektorunde-kisisel-verilerin-korunmasi-alaninda-yasanan-gelismeler/ (Erişim Tarihi:11.09.2024)

Civan Kemiksiz, R. (2022). Büyük veri çağında kişisel veri güvenliği üzerine bir alan araştırması: Dijital yerliler ve dijital göçmenlerin güvenlik algıları. Maltepe Üniversitesi İletişim Fakültesi Dergisi, 9(1), 64-91.

Çekin, M. S. (2019). Avrupa birliği hukukuyla mukayeseli olarak 6698 sayılı kişisel verilerin korunması kanunu. İstanbul: On İki Levha Yayıncılık.

Çetin, H. (2014). Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. Akdeniz İİBF Dergisi, 14(29), 86-105.

Demirtaş, A. (2024). CHATGPT'nin Gölgesinde Kişisel Verilerin Korunması. Kişisel Verileri Koruma Dergisi, 6(1), 14-27.

Develioğlu, H. M. (2017). 6698 sayılı kişisel verilerin korunması kanunu ile karşılaştırmalı olarak avrupa birliği genel veri koruma tüzüğü uyarınca kişisel verilerin korunması hukuku. İstanbul: On İki Levha Yayıncılık.

Dülger, M. V. (2019). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi Yayıncılık.

Dülger, M. V. (2020). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi Yayıncılık.

European Commission. What does data protection 'by design' and 'by default' mean? https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (Erişim Tarihi: 12.09.2024).

Erdoğdu, A. (2019). Bankacılık Sektöründe Kişisel Verilerin Korunması ve Müşteri İlişkileri Yönetimi. Kişisel Verileri Koruma Dergisi, 1(2), 87-94.

Erturan, E. (2019). Prof. Dr. Sabih Arkan'a Armağan.Veri Sorumlusunun Siber Tehditleri ve İnternet Dolandırıcılığını Önlemek Amacıyla "Başkalarının" Kişisel Verilerini İşlemesinin "Meşru Menfaat" Kapsamında Değerlendirilmesi Meselesi, On İki Levha Yayıncılık, 421-436.

Gazdağı, O. & Çetinyokuş, T. (2020). Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme. Journal of Humanities and Tourism Research, 10(2), 475-491.

Gündüz, M. Ş. (2022). Uluslararası insan hakları açısından kişisel veri güvenliği. Ankara: Adalet Yayınevi.

Hafızoğlu, E. (2024). Banka hukukunda sır kavramı. [Yayınlanmamış yüksek lisans tezi]. Bahçeşehir Üniversitesi.

Henkoğlu, T. (2017). Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme. Arşiv Dünyası, (18-19), 36-47.

Kangal, Z.T. (2019). Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması. İstanbul: On İki Levha Yayıncılık.

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.

Kartal, M.T. (2018). Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme. Uluslararası Ekonomi ve Yenilik Dergisi, 4 (1), s.1-18.

Kaya, M. B. (2024). KVKK Reformu: 2024 Değişiklikleri (Dijital Baskı 1.0), https://mbkaya.com/hukuk/kvkk-reformu.pdf (Erişim Tarihi: 24.10.2024).

Khiar, Dr. I. L. & Trautwein K. & Huber A. & Stamm J. (2017). The EU General Data Protection Regulation (GDPR) in the Banking Industry. (https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf) (Erişim Tarihi: 24.10.2024).

Korucu, O. (2021). Veri güvenliğinin iyileştirilmesi sürecinde risk tabanlı küresel standart, çerçeve ve en iyi uygulama yaklaşımları. Ankara: Adalet Yayınevi.

Kişisel Verileri Koruma Kurumu. Araç Kiralama Sektöründeki Kara Liste Uygulamaları hakkında Kişisel Verileri Koruma Kurulu'nun 23/12/2021 Tarihli ve 2021/1304 Sayılı İlke Kararı. https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf (Erişim Tarihi: 26.10.2024).

Kişisel Verileri Koruma Kurumu. (2019). Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Erişim Tarihi: 12.09.2024).

Kişisel Verileri Koruma Kurumu. Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi hakkında Kişisel Verileri Koruma Kurulu'nun 03/08/2023 Tarihli ve 2023/1310 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7775/2023-1310 (Erişim Tarihi: 08.08.2024).

Kişisel Verileri Koruma Kurumu. Banka tarafından ilgili kişinin cep telefonu numarasına SMS gönderilmesi suretiyle kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 Tarihli ve 2021/1104 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7263/2021-1104 (Erişim Tarihi: 24.10.2024).

Kişisel Verileri Koruma Kurumu. Bankanın avukatı tarafından borçlu yakını olan ilgili kişiye haciz ihbarnamesi gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulu'nun 21/10/2021 Tarihli ve 2021/1069 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7262/2021-1069 (Erişim Tarihi: 05.08.2024).

Kişisel Verileri Koruma Kurumu. Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulu'nun 21/12/2017 Tarihli ve 2017/62 Sayılı İlke Kararı. https://www.kvkk.gov.tr/Icerik/4114/2017-62 (Erişim Tarihi: 25.07.2024).

Kişisel Verileri Koruma Kurumu. Bir banka tarafından ilgili kişinin para transferleri ile hesap bilgilerinin üçüncü kişiye ait e-postaya gönderilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 12/01/2023 Tarihli ve 2023/67 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7592/2023-67 (Erişim Tarihi: 11.09.2024).

Kişisel Verileri Koruma Kurumu. Bir bankanın çağrı merkezi tarafından ilgili kişinin telefon numarasının üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulu'nun 10/03/2022 Tarihli ve 2022/224 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7296/2022-224 (Erişim Tarihi: 06.08.2024).

Kişisel Verileri Koruma Kurumu. Bir bankanın mobil uygulamalar üzerinden ilgili kişiye rızası dışında tanıtım iletileri göndermesi Hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 Tarihli ve 2021/361 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7109/2021-361 (Erişim Tarihi: 26.07.2024).

Kişisel Verileri Koruma Kurumu. Bir Bankanın Potansiyel Müşteri Kazanımı Amacıyla İlgili Kişinin Kişisel Verilerini Hukuka Aykırı Şekilde İşleyerek Hesap Açmasına İlişkin Olarak Kurula Yapılan Başvuru Hakkında Kişisel Verileri Koruma Kurulu'nun 06/02/2020 Tarihli ve 2020/103 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/6733/2020-103 (Erişim Tarihi: 13.09.2024).

Kişisel Verileri Koruma Kurumu. Bir bankanın, varlık yönetim şirketinin ve üç farklı avukatın borçlu olmayan ilgili kişinin kişisel verisini işleyerek icra takibi başlatması hakkında Kişisel Verileri Koruma Kurulu'nun 27/04/2021 Tarihli ve 2021/424 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7114/2021-424 (Erişim Tarihi: 05.08.2024).

Kişisel Verileri Koruma Kurumu. Bir bankanın veri ihlali hakkında 05/05/2020 tarihli ve 2020/344 sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/6764/2020-344 (Erişim Tarihi: 13.09.2024).

Kişisel Verileri Koruma Kurumu. Bir banka tarafından ilgili kişinin kredi kartının rızası dışında üçüncü kişilere teslim edilmesine ilişkin Kişisel Verileri Koruma Kurulu'nun 16/01/2020 tarihli ve 2020/32 sayılı Kurul Karar Özeti. https://kvkk.gov.tr/Icerik/6700/2020-32 (Erişim Tarihi: 24.10.2024).

Kişisel Verileri Koruma Kurumu. (2018). Kişisel Veri Güvenliği Rehberi (teknik ve idari tedbirler). https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Erişim Tarihi: 12.09.2024).

Kişisel Verileri Koruma Kurumu. (2022). Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf (Erişim Tarihi: 12.09.2024).

Kişisel Verileri Koruma Kurumu. İlgili kişinin kardeşine ait borca dair yürütülen icra takibi kapsamında, veri sorumlusu avukat tarafından ilgili kişinin kişisel verilerinin İcra Müdürlüğüne iletilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 09/09/2021 Tarihli ve 2021/909 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7141/2021-909 (Erişim Tarihi: 05.08.2024)

Kişisel Verileri Koruma Kurumu. İlgili kişinin kişisel verilerinin bilgisi dışında veri sorumlusu banka nezdinde sorgulanması Hakkında Kişisel Verileri Koruma Kurulu'nun 12/01/2021 Tarihli ve 2021/32 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7107/2021-32 (Erişim Tarihi: 29.07.2024).

Kişisel Verileri Koruma Kurumu. İlgili kişinin, kişisel verisi olan cep telefonu numarasının bir banka tarafından veriliş amacı dışında kullanılması hakkında Kişisel Verileri Koruma Kurulu'nun 18/09/2019 Tarihli ve 2019/277 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/5545/2019-277 (Erişim Tarihi: 25.07.2024).

Kişisel Verileri Koruma Kurumu. İlgili kişiye ait verilerin bir banka tarafından rızası olmaksızın babası ile paylaşılması karşısında Bankadan tazminat talep etmesi hakkında Kişisel Verileri Koruma Kurulu'nun 16/01/2020 Tarihli ve 2020/43 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/6715/2020-43 (Erişim Tarihi: 25.07.2024).

Kişisel Verileri Koruma Kurumu. İlgili kişiye bir banka tarafından SMS gönderilmesi ve ilgili kişinin bu banka nezdindeki kişisel verilerinin imha edilmesi talebinin yerine getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 13/04/2021 Tarihli ve 2021/358 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7106/2021-358 (Erişim Tarihi: 29.07.2024).

Kişisel Verileri Koruma Kurumu. Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kurul'un 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Erişim Tarihi: 01.12.2023)

Kişisel Verileri Koruma Kurumu. Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması hakkında 25/03/2019 tarihli ve 2019/81 sayılı Kurul Kararı ve 31/05/2019

Tarihli ve 2019/165 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Erişim Tarihi: 09.09.2024)

Kişisel Verileri Koruma Kurumu. Spor salonu hizmeti sunan sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması hakkında Kişisel Verileri Koruma Kurulu'nun 27/02/2020 Tarihli ve 2020/167 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/6738/2020-167 (Erişim Tarihi: 09.09.2024)

Kişisel Verileri Koruma Kurumu. Unvanında ilgili kişinin adının geçtiği bir şirket hakkında başlatılan icra takibine ilişkin dosya içeriğinin sosyal medyada paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 10/02/2022 Tarihli ve 2022/103 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7293/2022-103 (Erişim Tarihi: 24.10.2024)

Kişisel Verileri Koruma Kurumu. Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulu'nun 22/12/2020 Tarihli ve 2020/966 Sayılı İlke Kararı. https://www.kvkk.gov.tr/Icerik/6858/2020-966 (Erişim Tarihi: 11.09.2024).

Kişisel Verileri Koruma Kurumu. Veri sorumlusu banka tarafından ilgili kişinin verilerinin yakınları ile paylaşılması Hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 Tarihli ve 2021/79 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7111/2021-79 (Erişim Tarihi: 26.07.2024).

Kişisel Verileri Koruma Kurumu. Veri sorumlusu banka tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın bir sigorta şirketine aktarılması hakkında Kişisel Verileri Koruma Kurulu'nun 03/08/2022 Tarihli ve 2022/768 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/7570/2022-768 (Erişim Tarihi: 12.09.2024).

Kişisel Verileri Koruma Kurumu. Veri sorumlusu bankanın ilgili kişiye ait kredi kartı ekstresinde yer alan kişisel verileri yanlış e-posta hesabına göndermesi Hakkında Kişisel Verileri Koruma Kurulu'nun 30/01/2020 Tarihli ve 2020/78 Sayılı Kurul Karar Özeti. https://www.kvkk.gov.tr/Icerik/6922/2020-78 (Erişim Tarihi: 26.07.2024).

Kişisel Verileri Koruma Kurumu. Veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu verileri işlemesi hususunun değerlendirilmesine ilişkin 31/05/2018 Tarih ve 2018/63 Sayılı İlke Kararı. https://www.kvkk.gov.tr/Icerik/5248/2018-63 (Erişim Tarihi: 29.07.2024).

Küzeci, E. (2019). Kişisel verilerin korunması, Ankara: Turhan Kitabevi.

Küzeci, E. (2021). Kişisel Verilerin Korunması, İstanbul: On İki Levha Yayıncılık.

Özcan G. (2020). Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık.

Sevindi N. S., & Ordu M. E. (2023). AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi. Kişisel Verileri Koruma Dergisi, C5(1), 12-22.

Türkiye Bankalar Birliği. (2024). Dijital, İnternet ve Mobil Bankacılık İstatistikleri (Aralık 2023). https://www.tbb.org.tr/Content/Upload/istatistikiraporlar/ekler/4312/Dijital-Internet-Mobil_Bankacilik_Istatistikleri-Aralik_2023.pdf (Erişim Tarihi: 12.09.2024).

Türkiye Bankalar Birliği. (2024). Dijital, İnternet ve Mobil Bankacılık İstatistikleri (Haziran 2024). https://www.tbb.org.tr/Content/Upload/istatistikiraporlar/ekler/4437/Dijital-Internet-Mobil_Bankacilik_Istatistikleri-Haziran_2024.pdf (Erişim Tarihi: 12.09.2024).

Vural, Y. & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Yurtoğlu, T. (2020). Türk Bankacılık Sektörü Açısından Kişisel Verilerin Korunması Kanunu'nun Değerlendirilmesi. [Yayınlanmamış yüksek lisans tezi]. Ankara Hacı Bayram Veli Üniversitesi.

Yürük, Z. (2023). Veri sorumlusunun veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 22(48), 899-920.

Zor, A. (2020). Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu. İstanbul: On İki Levha Yayıncılık.