

BANKACILIK SEKTÖRÜNDE KİŞİSEL VERİ GÜVENLİĞİ ÜZERİNE BİR İNCELEME*

Aylin ERDOĞDU**

Öz

Çalışmada; modern hukuk devleti olmanın mihenk taşlarından, bireylerin ayrılmaz parçası olan kişisel verilerin korunması, Türk hukuk sisteminde, Kişisel Verilerin Korunması Kanunu ve kanuna dair yapılan düzenlemelerin, bankacılık sektörüne yansımaları incelenmiştir.

Çalışma toplam beş bölümden oluşmaktadır:

Birinci bölümde, konuya ilişkin genel bilgiler aktarılmıştır.

Çalışmanın ikinci bölümünde, son 10 yılda konuya dair yapılan akademik çalışmalar hakkında kısaca bilgi verilmiştir.

Diğer bölümde, kişisel veri kavramından hareketle, kişisel verilerin korunması analiz edilmiştir.

Müteakip gelen bölümde ise, kişisel verilerin korunmasına ilişkin düzenlemelerin tarihsel gelişimi ele alınmıştır.

Çalışma, özellikle bilgi teknolojilerini de kullanan ilgili servislerdeki iş süreçlerini kapsayan görev dağılımlarının yanı sıra, uyum faaliyetlerinin de doğru, şeffaf ve zamanında olacak şekilde yerine getirilmesi bağlamında her türlü yasal denetime hazır olunması gerektiği sonucuna ulaşmıştır.

Anahtar Kelimeler: Kişisel Veri, Kişisel Bilgilerin Gizliliği, Kişisel Veri Güvenliği, Kişisel Verilerin Korunması, Kişisel Verilerin Korunması Kanunu.

* Bu makale, 04-05 Mayıs 2018 tarihlerinde Ankara'da gerçekleştirilen I. Uluslararası Bankacılık Kongresi'nde sunulan sözlü bildirinin geliştirilmesiyle hazırlanmıştır.

** Dr.Öğr.Üyesi, T.C. İstanbul Arel Üniversitesi, Bankacılık ve Finans Bölümü

A REVIEW ON PERSONAL DATA SECURITY IN BANKING SECTOR

Abstract

In this study, the protection of personal data, which is an inseparable part of individuals from the cornerstones of being a modern state of law, the regulations in the Turkish legal system, the Law on the Protection of Personal Data and the laws and regulations on the banking sector are analysed.

The study consists of five sections:

The first part lays out the general information about the topic.

Secondly, there is based on a literature review covering last 10 years.

The next section is related to the protection of personal data.

The subsequent part is based on the historical perspective of the regulations on the protection of personal data.

It concludes that the segregation of duties might be certain in order to be more precise in process operations, especially for information technology related services, as well as compliance activities in terms of ensuring accuracy, transparency and timely for all type of regulatory inspections.

Keywords: Personal Data, Security and Safety of Personal Data, Personal Data Security, Protection of Personal Data, Law on the Protection of Personal Data.

Giriş

Bilgi teknolojileri ve iletişim ağlarının her geçen gün baş döndürücü bir hız kazandığı 21.yüzyılda, kişilik haklarının risk altında olması doğaldır. Kaydedilen bu ilerlemeler kişiye teknik açıdan konfor alanını genişletmekte yardımcı olurken, transparan hale gelen hayatını korumak açısından ağır sorumlulukları beraberinde getirmiştir. Bireysel tutum ve davranışların ön planda olması, doğal olarak dikkatleri kişilik haklarındaki kayıp ve kazançların odağına çekmiştir. Kişilik hakları gerçekleşmiş ya da gerçekleşmesi olası tüm saldırılara karşı korunmak istenir. İnsanlık tarihinde, her hak bir mağduriyete dayanarak kendini hissettirmiştir. Doğal olarak, kişisel verilerin korunması hakkının da ihlal edildiği ve korunmaya değer bir hak olduğunun anlaşıldığı olaylar mikro ve makro seviyede yaşanmaktadır. Özellikle kişilik haklarının ayrılmaz bir parçası olan kişisel verilerin toplanması, elektronik ortamda işlenmesi ve bu bilgilerin paylaşımı konularında yeni çağda yaşanan gelişmeler, ulusal ve uluslararası alanlarda birçok hukuki düzenlemenin yapılmasına zemin hazırlamıştır. Bu sebeple, kanun koyucular, özel hukukun sunduğu olanakları, bilgi teknolojilerinin olası tehditleri karşısında, riskleri bertaraf edebilmek amacıyla kişiyi koruma altına almayı hedeflemektedirler. Ancak düzenlemelerin; sektör bazında değerlendirmeleri yapılırken, uygulamada yaşanan aksaklıklar gözönünde bulundurularak zaman için güncellenmelerin işleyişi kolaylaştıracağından bahsedilebilir. Toplumsal hayattaki gelişim ve değişimler, konunun önümüzdeki süreçte çok farklı mecralara taşınacağına göstergesidir. Teknolojinin getireceği yeni imkanlarla birlikte, yapılan her yasal düzenleme, bir yenisine zemin hazırlayacak sürdürülebilirlik arz etmekte ve tarihsel süreçte devinim devam edecektir.

1-Literatür Taraması

Özenç sözlü bildirisinde, kişisel ve kurumsal bilgi güvenliğinin sağlanması konusundaki çalışmasında, “Kişisel Verilerin Korunması Kanunu”nun yasallaşmasının ardından kurulacak olan “Kişisel Verileri Koruma Kurumu” ile telekomünikasyon alanında kişisel verilerin korunması hususunda ortak politikalar gerçekleştirilmesi gerekli olduğunu ve Türkiye’de bilgi-iletişim teknolojilerinde veri güvenliği olmak üzere, diğer teknolojik alanlarda da Devlet-Sanayi-Üniversite işbirliğinin geliştirilmesinin, ülke menfaatleri açısından doğru bir yaklaşım olacağını belirtmiştir (Özenç, 2007:49).

Yavanoğlu, Sağıroğlu ve Çolak ortak eserlerinde, sosyal paylaşım ağları; detaylı olarak incelenmiş, güvenlik ihlalleri araştırılmış, karşılaşılabilecek ihlallerinin daha iyi anlaşılabilmesi için örnekler verilmiş, bilgi güvenliği bakış açısıyla sosyal ağlar değerlendirilmiş, paylaşım sitelerinde karşılaşılabilecek tehditler sınıflandırılmış ve alınması gereken önlemler sıralanmıştır (Yavanoğlu, Sağıroğlu ve Çolak, 2012:15-27).

Önlem olarak, yanında beklenmeyen tehdit ve tehlikeleri de beraberinde getireceğinin farkındalığı için, gereğinden fazla bilginin sanal ortamlara aktarılmaması, paylaşılmaması, erişimin denetlenmesi ve korunması bilincinin, her kesiminden bireyler tarafından içselleştirilmesi gerektiği vurgulanmıştır. Bu tür hizmetleri veren kurumların kişisel verilerin mahremiyetinin sağlanması için kullanım politikalarını geliştirmeleri, tehdit ve tehlikeleri önleyici tedbirleri almaları, kullanıcıları bilgilendirici dokümanlara daha fazla yer vermeleri ve bu konuda daha hassas davranmaları gerektiği düşünülmektedir.

Oğuz, eserinde Kişisel Verilerin Korunması Kanununun, Avrupa Birliği uyum sürecinin tamamlanması amacıyla, çıkarılmaya çalışıldığını, bu amacın, kavramın soyut hale gelmesinde baş rolü üstlendiğini beyan etmiştir. Kanun Tasarısı’nın “Avrupa Birliği ile uyum” ana fikrine odaklanmaktan başka, Türkiye’de hukuksal uygulamalarda ortaya çıkan aksaklıklar ve hali hazırda mevcut olan eksikliklerin giderilmesine istinaden, çalışmalar yapılarak düzenlenmesi hedeflenmiştir. Konuya ilişkin hazırlanacak olan çerçeve kanunun, Alana dair yapılacak ikincil düzenlemelere temel teşkil etmesi esas alınmıştır.

Yukarıda belirtilen Anayasa, kanunlar ve yönetmeliklerde eksiklik hissedilirse, ilave maddelerle regüle edilmesi ve ya kuvvetli kılınması gerekli alanları maddelerin revize edilmesiyle birlikte, toplumdaki yansımalarının daha pozitif bir algı oluşturacağı ifade edilmiştir (Oğuz, 2013: 1-38).

Açıkgöz, makalesinde, kişisel verilerin hukuka aykırı şekilde elde edilmesi ve internet bankacılığında kullanılması sonucu malvarlığı zarara uğratılan bankaya karşı mevduat sahibinin hukuki sorumluluklarını incelemiştir. Mevduat sahibinin kusurunun her olayda banka tarafından ispat edilmesinin gerekli olduğunu ve bankanın, mevduat sahibinin internet bankacılık hizmet sözleşmesini ihlal ederek koruma yükümlülüğünü zedelediğini açıklamıştır. Oluşan zarar ile zedelenen yükümlülük arasında illiyet bağı bulunduğunun ispatının zorunlu olduğu sonucuna varmıştır (Açıkgöz, 2016:389-432).

3-Kavramsal Çerçeve

Bu bölümde, kişisel veri kavramından hareketle, kişisel verilerin korunması izah edilmeye çalışılmıştır. Böylece, çalışmanın tamamında, karşılaşılabilecek bu kavramlarla ilgili bir anlam birliğine varılması hedeflenmiştir. Kavramsal çerçevede, öncelikle kelimelerin sözlük anlamlarından yola çıkılmış, konuya dair ulusal ve uluslararası düzenlemelerden alıntılar yapılarak, bölüm detaylandırılmıştır

Kişisel verilerin korunmasının temelinde de bireyin hak ve özgürlüklerinin korunması düşüncesinin yatması (Şimşek, 2008:15), nedeniyle bugüne kadar yapılan çalışmalarda daha çok hukuki kavramlar üzerinden hareket edilmiş ve kavramsal çerçeve daha çok hukuk terminolojisi üzerine inşa edilmiştir.

Sözlük anlamı olarak kişisel veri; haklara ve borçlara sahip olan varlıklara ilişkin; bir araştırmanın, bir istişarenin, bir akıl yürütmenin temeli olan doneler, kısaca kişiye ait bütün bilgiler şeklinde tanımlanabilir.

İngilizce’de ise; kişisel veri, kelimesi “personal data” olarak kullanılmaktadır. Uluslararası düzenlemelerde kişisel veri tanımı; OECD’nin verilerin korunmasına ilişkin olarak 23 Eylül 1980 tarihli Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Kılavuz İlkeler Düzenlemesi’nde karşımıza çıkmaktadır. Adı geçen düzenlemenin “Birinci Bölüm, Genel Tanımlar” başlıklı 1.maddesinde kişisel veriler, “Belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm veriler” olarak tanımlanmıştır. (OECD Kılavuz İlkeler, Madde 1).

Ulusal düzenlemelerde ise; 12 Eylül 2010 tarihinde yapılan referandumla Türkiye Cumhuriyeti Anayasasının 20. maddesine kişisel verilerin korunmasına ilişkin:

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

“(Ek fıkra: 12/9/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükümleri yer almaktadır (T.C. Anayasası Madde 20:4).

Kişisel verilerin korunması ile ilgili olarak ilk düzenleme olan; Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin “Tanımlar ve Kısaltmalar” başlıklı 3. maddesinde kişisel veri şu şekilde tanımlanmıştır: “Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler” (Kişisel Veri Yönetmeliği Madde 3). Kişisel Verilerin Korunması Kanunu (KVKK) metninde de aynı tanım korunmuştur.

Ulusal ve uluslararası düzenlemelerde yer alan kişisel veri tanımlamalardan yola çıkılarak, ortak dört paydadandan bahsedilebilir

- 1- Kişinin belirli ya da belirlenebilir olması,
- 2- Gerçek kişi olması,
- 3- Kişiyile ilgili olması,
- 4- Her türlü veriyi içermesi.

Söz konusu bu dört payda, istisnası olmaksızın, gerçek kişiyle ilişkilendirilebilen verinin, belirli bir kişi hakkında değerlendirme yapılırken kullanılabilmesini kastetmektedir. Tüzel kişilerin bu konunun dışında tutulduğu aşikârdır.

Kişisel verilerin oluşturulması ve elde edildikten sonra üzerlerinde işlem yapılması ve herhangi bir şekilde transfer edilmeleri kişisel verilerin işlenmesi olarak ifade edilebilir. Kişisel verilen işlenmesi, KVKK’da Madde 5’te düzenlenmiştir; “(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

hükmü yer almaktadır.

4-Tarihsel Perspektif

Bu bölümde, öncelikle dünyadaki düzenlemelere değinilmiştir. Daha sonra Türkiye'deki durum ir- delenmiştir. 12 Eylül 2010 tarihli halk oylaması ile kabul edilen maddeler arasında yer alan ve Ana- yasasının 20. maddesine eklenen kişisel verilerin korunması hakkı incelenmiş, şu an yürürlükte olan yasa ve yönetmeliklerde kişisel verilerin doğrudan veya dolaylı olarak düzenlendiği maddelere de değinilerek Kişisel Verilerin Korunması Kanunu (KVKK) ele alınmıştır.

4.1-Uluslararası Alanda Yapılan Düzenlemeler:

Kişisel verilerin korunması hakkının ilk olarak, M.Ö. 5. yüzyılda Hipokrat Yemininde kendine yer bul- duğu ve günümüzde de geçerliliğini koruduğunu söyleyebiliriz. Şöyle ki; Yemin Hekime hastasını muayene sırasında bizzat hastadan veya tetkikler sonucu öğrendiği verileri hiçbir şekilde paylaşma- ma ve koruması yükümlülüğünü getirmekteydi (Höfelmann'dan akt. Şimşek, 2008:20).

Kişisel verilerin korunması kapsamında ilk çalışma yapan uluslararası kuruluş ise; Avrupa Konseyi olmuştur. Konsey 1973 ve 1974'te kabul ettiği iki kararda (73/22 ve 74/29 sayılı karar suretleri) kamu ve özel sektör tarafından işlenecek kişisel verilerle ilgili dikkat edilmesi gereken ilkeleri tespit etmiştir.

OECD tarafından da 1978 yılında kişisel verilerin ülkeler arasında paylaşılmasında dikkat edilmesi gereken unsurlara yönelik çalışmalar yapılmış. 23.09.1980 tarihinde milletlerarası birliği ve teknik gelişmeleri sağlamak amacıyla, OECD'ye üye ülkeler tarafından, "Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler" (Guidelines on The Protection of Privacy and Trans- border Flows of Personal Data) kabul edilmiştir. Rehber ilkeler, tavsiye niteliğinde kararlar içermesi ve ülkelerin iç mevzuatına doğrudan etki edememesi sebepleriyle uygulamada yaptırım gücü ol- mamasına rağmen, ilerleyen zamanda yapılan ulusal ve uluslararası birçok düzenlemede dikkate alınmış ve yol gösterici olmuştur (Özdemir, 2009:50).

OECD ilkelerinin bağlayıcı olamaması, uluslararası anlaşma niteliğine sahip, hükümlerinin bağlayıcı olduğu bir metin ihtiyacını gündeme getirmiştir. AK'nin 28 Ocak 1981 tarih ve 108 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleş- me" (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)'si bu ihtiyaca cevap vermiş ve kişisel verilerin korunması alanında uluslararası alanda bağla- yıcılığı olan ilk sözleşme olarak tarihe geçmiştir. Sözleşme 1 Ekim 1985 yılında yürürlüğe girmiştir. 108 Sayılı Sözleşme Avrupa başta olmak üzere diğer tüm kişisel veri korunmasına önem atfeden ülkeler için referans bir düzenleme olmuş ve yapılan ulusal düzenlemelerde dikkate alınmıştır (Er- soy, 2009:70).

Avrupa Birliği Veri Koruma Yönergesi (EU General Data Protection Regulation – GDPR), 1995 yılın- da yürürlüğe soktuğu direktifin genişletilerek, regülasyon haline getirilmiş halidir. Üye ülkeler için çerçeve bir yasa oluşturan ilgili direktif yerine, tüm ülkelerin harfiyen uymak zorunda olduğu daha sıkı ve ağır tedbirler içeren regülasyon (GDPR) Mayıs 2016'da yayınlandı ve akabinde Avrupa Birliği (AB) uyum için, 2 yıl süre tanıdı. Bu süre ise 2018 Mayıs ayında sona erecek.

4.2. Ulusal Alanda Yapılan Düzenlemeler:

AB Konseyi'nin 2000 Yılı Türkiye İlerleme Raporu başta olmak üzere, tüm İlerleme Raporlarında, Türkiye'de kişisel veri korunmasına dair bir yasanın ve bağımsız denetleyici bir otoritenin olmadığı eleştirilmiştir (Avrupa Birliği Bakanlığı, 2013). Buna rağmen, Kişisel verilerin korunmasına, 12 Eylül 2010 tarihinde yapılan referandumla kadar anayasamızda yer verilmemiştir. Bu tarihe kadar; Anayasa'nın 17. maddesinde, "kişinin maddî ve manevî varlığını koruma ve geliştirme" hakkına ve insan onuruna, 20. maddesinde, özel hayatın gizliliğinin korunması hakkına ve 22. maddesinde haberleşme özgürlüğüne yer verilerek bir nevi kişisel verilerin korunmasına temel teşkil eden anayasal ilkelerden bahsedilmekteydi. Bu haklar, kişisel verilerin korunmasına belli başlı anayasal garantiler getirmekteydi (Özdemir, 2009:58).

Ulusal düzenlemelerde kişisel verilerin nasıl tanımlandığına bakacak olduğumuzda karşımıza çok sınırlı sayıda düzenleme çıkmaktadır. 12 Eylül 2010 tarihinde yapılan referandumla Türkiye Cumhuriyeti Anayasası'nın 20. maddesine kişisel verilerin korunmasına ilişkin:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır (T.C. Anayasası Madde 20)

Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu internet kullanımının yaygınlaşması; kişisel verilerin know-how olarak kabul edilmesi sonucunda 07 Nisan 2016'da yürürlüğe girdi. Kanunda, şirketlere yeni sürece uyum sağlayabilmeleri amacıyla, yürürlük tarihinden önce alınmış, işlenmiş, saklanmış kişisel verilerin düzenlenebilmesi adına, 07 Nisan 2016 tarihinden başlamak üzere ile 2 yıllık uyum süresi tanıdı. Buna göre; herhangi bir uzatma öngörülmemesi halinde, Türkiye için uyum süresi Nisan 2018'de sona erdi. Akabinde KVKK bir açıklama yayınladı:

Kanuna Uyum Süreci (Geçici 1.madde) İle İlgili Duyuru

"Son günlerde medyada yer alan bazı haberler ile Kurumumuza şifahi olarak iletilen sorular neticesinde, 6698 sayılı Kişisel Verilerin Korunması Kanununun Geçici 1 inci maddesinin uygulanmasıyla ilgili tereddütler yaşandığı görülmüştür. Söz konusu tereddütlerin önüne geçilmesi ve kamuoyunun doğru bilgilendirilmesini teminen konuya ilişkin açıklama yapılması gereği doğmuştur.

Bilindiği üzere, Kanunun Geçici 1 inci maddesinin üçüncü fıkrasında; Kanunun yayımı tarihinden önce işlenmiş olan kişisel verilerin, yayımı tarihinden itibaren iki yıl içinde (7 Nisan 2018) Kanun hükümlerine uygun hale getirileceği, Kanun hükümlerine aykırı olduğu tespit edilen kişisel verilerin derhal silineceği, yok edileceği veya anonim hale getirileceği, ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızaların, bir yıl içinde (7 Nisan 2017) aksine bir irade beyanında bulunulmaması halinde, bu Kanuna uygun kabul edileceği hükme bağlanmıştır.

Bu itibarla, Kanunun yayımı tarihinden önce yürürlükte bulunan mevzuat çerçevesinde hukuka uygun olarak alınmış rızaların, ilgili kişilerce aksi belirtilmediği sürece, yukarıda yer verilen hüküm uyarınca Kanuna uygun olduğu kabul edildiğinden, veri sorumlularınca bu şartlar dâhilinde alınmış mevcut rızaların güncellenmesine veya yeniden ilgili kişilerden açık rıza alınmasına gerek bulunmamaktadır. Dolayısıyla, ilgili kişilerce Kanunun yayımı tarihinden itibaren bir yıl içerisinde aksine bir irade beyanında bulunulmamış ise, bu kişisel verilerin de silinmesi veya yok edilmesi gerekmemektedir.

Unutulmamalıdır ki kişisel verilerin işlenmesi için yegane şart açık rıza değildir. Kişisel veri işleme şartları, Kanunun 5 inci ve 6 ncı maddesinde açıklıkla belirtilmiştir. Bu bağlamda; Kanunun yayımından önce toplanmış kişisel veriler açık rıza dışındaki Kanunun 5 inci ve 6 ncı maddesindeki şartlar dairesinde işleniyorsa, bu işleme faaliyetleri için de açık rıza alınmasına ve bu faaliyetlerin de açık rızaya dayalı olarak yürütülmesine gerek yoktur.

Kamuoyuna saygıyla duyurulur.”

Kanunda çıkarılacağı belirtilen ikincil düzenlemelerde gecikmeler yaşanması, doğal olarak sektörel bazdaki düzenlemelerin de ertelenmesine yol açmıştır. Kanun yayınlanması itibari ile 1 yıl içerisinde çıkarılması beklenen yönetmeliklerden biri olan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik 28 Ekim 2017’de Resmi Gazete’de yayımlanmış ve 1 Ocak 2018’de yürürlüğe girmiştir.

Veri sorumluları siciline ilişkin taslak yönetmelik ise henüz nihai haline ulaşmamıştır.

Kişisel verilerin korunmasının yasalaşmasının, kişileri tam anlamıyla garantiye alındığını söylemek mümkün olmadığı gibi, girişte bahsedildiği üzere; ilerleyen süreçte, sürekli gelişen teknolojiyle birlikte, bazı hükümlerin koyuluş amacına hizmet edemeyebileceği de göz ardı edilmemelidir.

5-Sonuç

Bankacılık sektörü ele alındığında;

5411 sayılı Bankacılık Kanununun “Sırların Saklanması” başlıklı 73. Maddesine göre, “Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar.” Bu maddede bankacılık sektöründeki çalışanların, müşterilere ait kişisel verilerin de içinde olduğu sır niteliğindeki verileri kanununda yetkili kılınan merciler dışında hiçbir kişi veya kuruluşla paylaşamayacağını belirtilmektedir. Bu madde ile yapılan düzenleme, kişisel verilerin üçüncü kişilere transferinde izlenecek yol haritası niteliğindedir.

Yine bankalar 5411 sayılı Kanun’da belirtildiği üzere; bankacılık faaliyetinin yanı sıra acente sıfatı ile sigortacılık da yapabilirler. Bankalar özellikle bu iki faaliyet alanında yoğun olarak, özel nitelikli kişisel verileri işlemektedirler. BDDK tarafından regüle edilen bankacılık sektöründe; KVKK Kanunda öngörülen yükümlülüklerin yerine getirilmesi ve kanunun ilkelerine uyum sağlayabilmek amacıyla yürütülen uyum projeleri neticesinde, tespit edilen hususlar:

- Kimliği belirli veya belirlenebilir gerçek kişilere ait her türlü bilgi, kanun uyarınca kişisel veri niteliğine haizdir. Bu bakış açısıyla, bir veya birden fazla niteliksiz veri, gerçek bir kişiye ulaşılması halinde ne yazık ki kişisel veri olarak kabul edilmektedir. Ayrıca kanun, kişiler nezdinde din, mezhep, ırk, etnik köken, siyasal fikirleri, felsefe inanışları ya da öteki inanç prensipleri, giyim tarzları, dernekler, vakıflar vey a sendika üyelikleri, cinselliğe bakış açıları, sağlık durumları, ceza-i mahkûmiyet alıp almadıkları ve güvenlik önlemlerine ilişkin verileri ile biyometrik ve genetik bilgilerini özel nitelikli kişisel veri olarak tanımlıyor ve bu bağlamdaki verileri daha özellikli bir korumaya tabi tutuyor. AB’deki yeni düzenleme olan GDPR’ye ise yalnızca bu kategorideki (sensitive data) veriler için açıkça rıza alınma şartını öngörmüştür.

- Sigorta faaliyetleri için, acente sıfatı ile hareket eden bankalar, kişisel verileri yoğun olarak bünyesinde barındırıyor sigortacılık iş süreçlerinde de özel nitelikli kişisel veriye sürekli olarak dokunuyor.
 - Hali hazırda banka ile ilişkisi bulunmayan müşteri olabilme olasılığı bulunan bireylerin kısacası potansiyel müşterilerin ve ya dolaylı yoldan örneğin kefil sıfatıyla banka ile yolları kesişen kişilerin sınıflandırılması ve ilgili müşteri sınıfına dair verilerin işlenmesi. Sektör işleyişi gereğince potansiyel müşteri verisi sıklıkla işleniyor ve kullanılıyor. Bu husus özelinde kanun değerlendirildiğinde, riski minimize etmek adına, açık rıza alarak ilerlemek gerekiyor.
 - Bankacılık sektörü risk analizleri ve öngörülerle çalıştığı için, düzenli ve periyodik raporlamaların yapılması ihtiyacı doğal olarak ortaya çıkıyor. BDDK'ya bağlı olarak çalışmanın gereği olarak mevzuata dayalı ve faaliyetlerini sürdürebilme kapsamında iştirakler, partnerler ve yerli veya yabancı hissedarlar ile iç raporlamalar 2006 yılından beri periyodik olarak hazırlanmaktadır. Mevzuat dayanağı olmayan ancak içeriğinde kişisel veri barındıran raporlar, kanun nezdinde değerlendirildiğinde yüksek risk faktörü içerdiği görülmektedir. Kanun kapsamında öngörülen riskleri bertaraf edebilmek için, ardıl düzenlemeler ve sektörel bazda bilgi paylaşımı yapıncaya kadar, raporlamalarda kullanılan kişisel verilerin minimum seviyeye indirilerek, sayısal olarak en asgari düzeyde tutulması ve zorunlu olmayan kişisel verilerin işlenmesinden kesinlikle kaçınılmasının an itibari ile en sağlıklı çözüm önerisi olduğu ifade edilebilir.
 - İlave olarak, en büyük risk unsurunu CRM olarak bilinen müşteri ilişkileri yönetimi faaliyetlerinin taşıdığı söylenebilir. Zira bankacılık sektörü için mihenk taşı olan CRM raporlamaları ve pazarlama faaliyetleri, Bankacılık Kanunu'na bakıldığında bankaların gerçekleştirebileceği faaliyet listesinde yer almıyor. BDDK ve Türkiye Bankalar Birliği toplantıları ve kanuna dair yapılan ikincil düzenlemelerin de uygulamada yer alması ile durumun bir netlik kazanması bekleniyor.
- Sonuç olarak, uyum sürecinin tamamlanması için öngörülen Nisan 2018 tarihi dolmuş olmasına rağmen kanunda öngörülen veri sorumlularının sicile kayıt ve işleyişlerini düzenleyecek olan yönetmelik henüz yayınlanmadı, mevcut olanın düzenlenmesine gidildi. Bu sebeple hali hazırda mevzuata dair birtakım soruların olması da göz önünde bulundurularak, ilk etapta kolaylıkla alınabilecek en risksiz aksiyonun; kişisel veriye dokunan iş süreçlerinde mümkün oldukça asgari düzeyde verilerin işlenmesi GDPR'da yer alan şekli ile verilerin minimize edilmesi, saklanması ve aktarılması olacağı gözüküyor.

KAYNAKÇA

Açıköz, Osman (2016) Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratan Bankaya Karşı Mevduat Sahibinin Hukuki Sorumluluğu, Marmara Üniversitesi Hukuk Fakültesi, Hukuk Araştırmaları Dergisi, İstanbul, Cilt:22, Sayı:1,s.389-432. Aksoy, Hüseyin Can, (2008), Kişisel Verilerin Korunması, Yayınlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Atak, Songül, (2010), Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, Türkiye Barolar Birliği Dergisi, 22(87), s.90-120.

Bankacılık Kanunu, https://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanunu/15405411_sayili_bankacilik_kanunu.pdf, (E.T. 15 Aralık 2017)

Başalp, Nilgün, (2004), Kişisel Verilerin Korunması ve Saklanması. Ankara: Yetkin Yayınları.

Başalp, Nilgün, (2013), Bağımsız Veri Koruması Kurumlarının Yapısı, Erzincan Üniversitesi, http://www.erkincan.edu.tr/userfiles/file/haber_gundem/bilisim_hukuku/veri_korumasi_sunum.ppt, (E.T. 25 Aralık 2017).

Civelek, Dilek Yüksel, (2011), Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Yayınlanmamış Uzmanlık Tezi, Ankara: Devlet Planlama Teşkilatı.

Dağ, Güray, (2011), Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Yayınlanmamış Doktora Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Ersoy, Uğur, (2009), Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması", Yayınlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Kişisel Verilerin Korunması Kanunu, <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>, (E.T.11 Aralık 2017).

Küzeci, Elif, (2010), Kişisel Verilerin Korunması, Ankara: Turhan Kitabevi Yayınları.

OECD, (1980), Klavuz İlkeler, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>, (E.T. 20 Aralık 2017).

Oğuz, Habip (2013), Elektronik Ortamda Kişisel Verilerin Korunması Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, Uyuşmazlık Mahkemesi Dergisi, Sayı:3, s.1-38.

Özdemir, Hayrunnisa, (2009), Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, 1. Baskı, Ankara: Seçkin Yayıncılık.

Özenç, Köksal (2007), Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması,Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 48-62.

Şimşek, Oğuz, (2008), Anayasa Hukukunda Kişisel Verilerin Korunması, 1. Baskı, İstanbul: Beta Basım.

T.C. Anayasası, https://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf, (E.T.11 Aralık 2017).

T.C. Avrupa Birliği Bakanlığı, (2013), TR-AB ilişkileri, <http://www.abgs.gov.tr/index.php?p=113&l=1>, (E.T. 12 Aralık 2017).

Avrupa Konseyi, (1981), Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme, http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm, (E.T. 9 Aralık 2017).

Yavanoğlu, Uraz, Sağıroğlu Ş ve Çolak İ. (2012), Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler, Politeknik Dergisi, Cilt:15, Sayı:1, s.15-27.