MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN İŞLENMESİ VE YASAL OLARAK DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Yasin AYDOĞDU[*]

ÖZ

Teknolojik gelişmeler sonucu tablet, telefon, saat gibi insanların rahatlıkla yanında bulundurabileceği mobil cihazlar işlemci hızı ve kapasite bakımından masaüstü bilgisayarlara oldukça yaklaşmışlardır. Mobil cihazların kullanım kolaylığının yanı sıra internete erişimin yaygınlaşması sonucu bu alana ilgi artmış ve bunun sonucunda bu cihazlar için özel olarak tasarlanmış ve kodlanmış yazılımlar oluşturulmuştur. 'Mobil uygulama' olarak adlandırılan bu yazılımlar kullanıcıların hayatını kolaylaştırmak için yapılan banka işlemlerinden haberlere, müzik, oyun ve tasarım gibi hayatın birçok alanına yönelik ürün ve hizmetler sunmaktadır. Taşıma ve erişme kolaylığının yanı sıra mobil uygulamalar bilgisayar ve internet sitelerinden alınan hizmeti daha az veri kullanarak sunabilmektedir. Bu bakımdan günümüz insanları için lüksten ziyade ihtiyaç konumuna gelmiştir.

Mobil uygulamaların büyük çoğunluğu kullanıcılarının verileri üzerinde tasarrufta bulunmaktadır. Kullanıcıları belirli yahut belirlenebilir kılan bu veriler esasında kişisel verilerdir. Kişisel verilerin korunması, özel hayatın gizliliği hakkı kapsamında anayasalar ve uluslararası sözleşmelerle güvence altına alınmış temel bir insan hakkıdır. Çalışmada öncelikle mobil uygulamaların çalışma mantığı ve veriler üzerindeki tasarruf durumları ele alınacak; ardından insanlar için artık vazgeçilmez bir konumda olan mobil uygulamalar ve bu uygulamaları işleten kişilere karşı kişisel verilerin korunması hususu ele alınacaktır.

Anahtar Kelimeler: *Kişisel Veri, Mobil Uygulama, Akıllı Cihaz, Veri İşleme, Veri Madenciliği*

---

[*] **Dr. Öğretim Üyesi**, Kırıkkale Üniversitesi Hukuk Fakültesi Anayasa Hukuku Anabilim Dalı, Yahşihan/KIRIKKALE, **e-posta:** aydoğdu@kku.edu.tr

ORCID: 0000-0003-3248-5199

DOI : 10.34246/ahbvuhfd.1065420

Yayın Kuruluna Ulaştığı Tarih : 08/07/2021

Yayınlanmasının Uygun Görüldüğü Tarih: 06/01/2022

PROCESSING PERSONAL DATA IN MOBILE APPLICATIONS AND LEGALLY MATTERS TO BE CONSIDERED

ABSTRACT

As a result of technological developments, mobile devices such as tablets, phones and watches that people can easily carry with them have come close to desktop computers in terms of processor speed and capacity. In addition to the ease of use of mobile devices, the interest in this field has increased as a result of the widespread use of internet access, and as a result, specially designed and coded software has been created for these devices. These software, called 'mobile applications', offer products and services for many areas of life such as banking transactions, news, music, games and design to make the life of users easier. In addition to the ease of transportation and access, mobile applications can offer the service received from computers and websites using less data.In this respect, it has become a necessity rather than luxury for today's people.

The vast majority of mobile applications disposition on the data of their users. These data that make users identified or identifiable are essentially personal data. Protection of personal data is a fundamental human right guaranteed by constitutions and international conventions within the scope of the right to privacy. In the study, firstly, the operating logic of mobile applications and dispositioningon data will be discussed; then, the issue of protecting personal data against mobile applications and their operator, which are now indispensable for humans, will be discussed.

Key Words: *Personal Data, Mobile Application, Smart Device, Data Processing, Data Mining*

Giriş

Teknolojik gelişmeler birçok işlemin elektronik olarak kayıt altına alınmasını ve bunlara istenildiğinde ulaşılabilmesini kolaylaştırmakla beraber, bu işlemlerin çok daha ucuza mal edilmesini sağlar duruma gelmiştir. Bu süreçte geleneksel bilgisayar uygulamaları yerini önce web uygulamalarına ardından mobil uygulamalara bırakmıştır. Nitekim web uygulamaları ve mobil uygulamaların bilgisayar uygulamalarına nazaran en önemli

avantajı taşınabilir yani her an her yerde kullanıcının yanında ve erişilebilir olmasıdır. Bu uygulamaların bilgisayar, cep telefonu, tablet ve saat gibi akıllı (*smart*) cihazlar üzerinden çalışabiliyor olması onlar için "mobil"[1] sıfatının getirilmesine sebep olmuştur.

Taşınma kolaylığı ile beraber teknolojik gelişmeler bağlamında, mobil cihazlar işlemci hızı ve kapasite bakımından masaüstü bilgisayarlara oldukça yaklaşmışlardır. Kullanım kolaylığı bulunan bu cihazlara sahip kullanıcı sayısı her geçen gün artmakta ve bunun sonucunda mobil cihazlar için geliştirilen uygulamalar bir o kadar önem kazanmaktadır.

Mobil cihazların kazandığı değer ve önemin farkında olan ticari işletmeler insan hayatının her alanına bu uygulamaları sokmuştur. Nitekim internetin yaygın olarak kullanımının hız kazandığı 21. yüzyılda bilgiye hızlı erişim başta olmak üzere çevrim içi işlemler yapma ve daha birçok kolaylık sağlayan mobil uygulamalar akıllı cihazlarla beraber gündelik hayatımızın vazgeçilmez birer parçası haline gelmiştir. Akıllı cihazların diğer mobil teknolojilere göre daha cazip olmasını sağlayan en temel özellik bu cihazlar için geliştirilen kişilere özel mobil uygulamalardır. Başta bilgisayar, tablet ve akıllı telefonlar olmak üzere tüm akıllı cihazlara, elektronik (web) mağazalar aracılığıyla birçok mobil uygulama indirilebilmektedir. Mobil uygulama mağazaları dışında mail, bulut, CD/DVD yahut harici disk üzerinden yükleme gibi farklı kurulum yöntemleriyle de bu uygulamalara erişilebilmektedir.

İnternete erişimin giderek daha kolay bir hâl aldığı günümüzde mobil uygulamalara talep artmakta, bununla paralel bir şekilde mobil uygulama üretimi de hız kazanmaktadır[2]. 2021 yılı başlarında yapılan bir araştırmaya göre[3] Dünya genelinde 3.2 milyar insan akıllı telefon, 1.14 milyar insan tablet kullanmaktadır. Yine aynı araştırmada bu cihazları kullananların, kullanım sürelerinin %88'ini uygulamalarda geçirdiği tespit edilmiştir. Araştırmanın yapıldığı tarih itibariyle mobil uygulama marketlerinden en büyüğü olan

[1] Fransızca "*mobile*" kelimesinden Türkçeye "mobil" kullanımıyla geçen bu kelime sözlükte "hareketli, taşınabilir" olarak açıklanmaktadır. TDK Güncel Türkçe Sözlük, <https://sozluk.gov.tr> Erişim Tarihi 25 Nisan 2021.

[2] Dijital teknolojilerin gelişmesi ile ortaya çıkan elektronik mağazalar, çağımız dijital dünyasında ticaretin temel öznesi olan müşterilerine güncel ürünleri pazarlama eylemini üstlenmektedir. Noam Tractinsky ve Oded Lowengart, "Web-Store Aesthetics in E- Retailing: A Conceptual Framework and Some Theoretical Implications", 2007, 1(1), Academy of Marketing Science Review, s. 1-18.

[3] Buildfire, Mobile App Download and Usage Statistics (2021), Şubat 2021, <https://buildfire.com/app-statistics/#> Erişim Tarihi 20 Nisan 2021.

Google Play Market'te 2.87 milyon uygulama, Apple Store'da ise 1.96 milyon uygulama bulunmaktadır. Bu iki uygulama marketi dışında daha yakın bir geçmişte kurulan Huawei Uygulama Mağazası'nda yer alan uygulama sayısı da her geçen gün artmaktadır.

Bu uygulama marketlerinin ortaya çıkışları 2000'li yıllara dayanmaktadır. Aradan geçen kısa bir zaman dilimi içerisinde eriştikleri seviye göz önünde bulundurulduğunda yakın gelecekte ulaşacakları sayı ve kapsayacakları alan insanoğlunun hayal gücü sınırlarını zorlayacak düzeydedir.

Çalışmada mobil uygulamalar üzerinden elde edilen kişisel verilerin hukuka uygun bir şekilde işlenmesi için dikkat edilmesi gereken hususlar ele alınacaktır. Zira günümüzde başta teknoloji şirketleri olmak üzere birçok firmanın veri elde etme yarışı hız kazanarak veriye olan talep artmıştır.

Aslında çok uluslu teknoloji şirketleri ve bazı devletlerin veri elde etme yarışı çok daha önce başlamıştı. 2012 yılında düzenlenen Davos Dünya Ekonomik Forumu'nda "veri"nin de döviz yahut emtia gibi yeni bir ödeme aracı yani ekonomik varlık olduğu deklare edilmişti[4]. O günden bu yana yaşanan teknolojik alandaki hızlı gelişmeler ticari faaliyetlerde verinin değerini çok daha fazla artırmıştır.

Yeni ekonomik düzen içerisinde verinin değeri ve bu alana artan ilgi karşısında belirli temel hak ve özgürlükler daha fazla risk altına girmiştir. Bu bakımdan dijitalleşmeyle beraber temel bir insan hakkı olarak özel hayatın gizliliği bağlamında kişisel verilerin korunmasına gösterilen özen de artmalıdır. Çünkü, teknolojik alanda yaşanan gelişmeler kişisel veriye ulaşmayı yani kişilerin özel hayatlarına müdahale etmeyi kolaylaştırmaktadır. Kişisel veriye en kolay yoldan ulaşım araçlarından biri de mobil uygulamalardır.

Açıklama ve tartışma yöntemlerinin kullanılacağı bu çalışmada öncelikle mobil uygulama kavramı üzerinde durulacaktır. Bu kısımda "mobil uygulama nedir?", "mobil uygulamalar nasıl edinilir?" ve "mobil uygulamalar verileri nasıl kullanır?" sorularına cevap vereceğiz. Ardından mobil uygulamaların enerji kaynağı olarak veri (*data*) konusu bağlamında büyük veri (*big data*) ve veri madenciliği *(data mining*) konuları üzerinde duracağız. Her iki konu da başlı başına kapsamlı çalışma konuları olmakla beraber; biz bu konuları genel hatlarıyla açıklayacağız. Çalışmamızın esas konusu ise mobil uygulamalarda

[4] Remzi Altunışık, "Büyük Veri: Fırsatlar Kaynağı mı Yoksa Yeni Sorunlar Yumağı mı?", 2015, 1(1), Yıldız Social Science Review, s. 47.

işlenen kişisel veriler ve bu veri işleme faaliyetleri esnasında yasal olarak dikkat edilmesi gereken hususlardır.

Mobil uygulama geliştirici ve işleticilerin dikkat etmesi gereken hususlar ile yasal yükümlülükleri çalışmanın son bölümünde ele alınacaktır. Bu bölümde dikkat edilmesi gereken hususlar sadece Türk Hukuk mevzuatındaki düzenlemeler bakımından değil; alana dair uluslararası düzenlemeleri de kapsayacak şekilde aktarılacaktır. Bu konudaki açıklamalarımızın kullanıcılar için farkındalık oluşturacağı gibi mobil uygulama üreticileri için de bir rehber oluşturacağı kanaatindeyiz.

I. MOBİL UYGULAMA

A. Genel Olarak Mobil Uygulama

Günümüzde neredeyse herkesin yanından ayırmadığı telefon, tablet, saat gibi akıllı cihazlarda kullanılmak için özel olarak kodlanmış ve tasarlanmış olan belirli yazılımlara mobil uygulama denir.

Mobil uygulamalar gündelik hayatımızı kolaylaştırdığı gibi birçok insanın eğlenceli vakit geçirdiği platformlar olarak da gözlemlenmektedir. Bu bakımdan haber uygulamalarından yemek tariflerine, finans işlemlerinden elektronik ticarete, sosyal medya ve anlık sohbet platformlarından çevrim içi oyunlara kadar çok geniş bir mecraya mobil uygulamalar üzerinden ulaşılabilmektedir. Akıllı cihazlar, mobil uygulamalar üzerinden internet sitelerini, sosyal medya uygulamalarını, kamerayı, uydu bağlantısını, haritayı ve daha birçok özelliği minimal dizaynlarında bir araya getirmekte ve kullanımı yaygınlaştıkça sosyal ve kültürel bir fenomen haline gelmektedir[5].

Mobil uygulamalar esasında internet sitelerinden alınan hizmeti daha pratik bir şekilde sunmaktadır. Hatta günümüzde internet sitelerinin de mobil versiyonları veya mobil uygulamaları vardır[6]. Zira mobil uygulamalar normal web sitelerinden daha az veri kullanarak aynı hizmete yahut bilgiye ulaşılabilmesini sağlamaktadır. Kısaca mobil uygulamalar sayesinde insan

[5] Naciye Guliz Uğur ve Aykut Hamit Turan, "Üniversite Öğrencilerinin Mobil Uygulamaları Kabulü ve Kullanımı: Sakarya Üniversitesi Örneği", 2015, 6(2), İnternet Uygulamaları ve Yönetimi Dergisi, s. 74.

[6] Yapılan araştırmalara göre, mobil cihaz kullanıcılarının uygulamalarda geçirdikleri süre, mobil sitede geçirdikleri sürenin katbekat üstündedir. Sun Han Rebekah Wong, "Which platform do our users prefer: Website or mobile app?", 2012, 40(1), Reference Services Review, s. 103-115.

hayatı ciddi anlamda kolaylaşmaktadır. Örneğin kişinin bulunduğu konum tek bir işlemle başkalarıyla paylaşabilmektedir. Hatta kişi hareket halinde olması durumunda dahi anlık konum verileri istediği kişilere aktarılabilmektedir. Yine istenirse mobil cihazın donanımında başka bir amaç için tasarlanmış bir özelliğin (örneğin ses açma-kısma tuşu) farklı başka bir amaç için (örneğin fotoğraf çekimi) kullanılması mümkün olabilmektedir.

Ezcümle, taşıma ve kullanım kolaylıklarıyla beraber mobil cihazları cazip kılan ve bu cihazlara ilgiyi artıran en önemli etken, cihazlara uyumlu mobil uygulamaların çeşitliliği, sayısı ve bunun sonucunda bilgisayarda çalışan ve kullanıcının hoşuna giden uygulamanın, mobil uygulamasının da olmasıyla kullanıcının her daim yanında olması ve hayatını daha fazla kolaylaştırabilmesidir[7].

B. Mobil Uygulama Edinme Yolları

Mobil uygulamalar genellikle akıllı cihazların mobil işletim sistemleri üzerinden kurulan platformlardan edinilebilmektedir. Örneğin Apple markasının iOS işletim sistemi ile çalışan akıllı cihazları Apple App Store isimli platform üzerinden mobil uygulamaları edinebilmektedir. Yine Google Android işletim sistemi ile çalışan cihazlara[8] Google Play Store isimli platform üzerinden ulaşılabilmektedir. Huawei isimli teknoloji şirketi ise yakın zamana kadar Google yazılımlarını kullanmakta iken; kısa süre önce kendi yazılım sistemini geliştirerek akıllı cihazlarına mobil uygulamaların kendi platformu olan Huawei App Gallery üzerinden indirilmesini sağlamıştır. Yine bu üç örnek dışında Windows, Blackberry vb. teknoloji şirketlerinin kendi mobil uygulama mağazaları bulunmaktadır[9].

Uygulama mağazalarından erişilen mobil uygulamalar, üretici ve işleticilerinin isteğine ve sağladıkları hizmetin kalitesine göre, bir ücret mukabilinde yahut ücretsiz şekilde akıllı cihazlara yüklenebilmektedir. Ücretsiz mobil uygulamalar, ilgili mağazalardan indirilebilir ve sınırsız bir şekilde kullanılabilir. Bazı mobil uygulamaları ücret ödemeksizin indirdikten sonra tüm imkanlarından faydalanabilmek için ücret ödemek gerekebilmektedir.

---

[7] Muhammed İkbal Bilgili, "Adaptif Bağlam Bilinçli Mobil Uygulama Geliştirme", Gazi Üniversitesi Bilişim Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, 2014, s. 10.

[8] Google Android yazılımını en yaygın kullanan markalardan biri Güney Koreli teknoloji şirketi Samsung'tur. Samsung, tüm akıllı cihazlarında bu yazılımı kullanmaktadır.

[9] Bunlar dışında birçok uygulama mağazası daha bulunmaktadır. Örneğin: Amazon App Store, ApkMirror, Getjar, AppBrain, Aptide, Opera Mobile, SlideMe bunlardan bazılarıdır.

Ücretli mobil uygulamaları kullanabilmek için ise uygulamayı sanal mağazadan kredi kartı yahut başka bir ödeme yöntemi kullanarak satın almak gerekmektedir.

Mobil uygulamalar mağazalar dışında haricen cihazlara yüklenme (kurulum) şeklinde de edinilebilir. CD, flash disk (USB bellek) yahut farklı bir veri taşıma cihazı vasıtasıyla akıllı cihazlara kurulumun yanı sıra internet üzerinde kurulum programının indirilmesi ve ardından uygulamanın cihaza kurulumunun sağlanması da diğer yöntemler olarak ifade edilebilir.

C. Mobil Uygulamaların Enerji Kaynağı: Veri (*Data*)

Mobil uygulamalar kısaca, bilişim sistemleri üzerinden kodlanmış ve özel olarak tasarlanmış yazılımlardır. Kodlama, mobil uygulama yazılımı ve geliştirme konuları işin mühendislik kısmını oluşturup özel uzmanlık bilgisi gerektiren ayrı bir çalışmayı gerektirmektedir. Biz ise çalışmanın bu kısmında mobil uygulamaların nasıl çalıştığından ziyade kullanımları esnasında veriye neden ihtiyaç duydukları sorusuna cevap vermeye çalışacağız. Nitekim hangi yöntemle edinilirse edinilsin mobil uygulamaların büyük çoğunluğu kişisel verileri işlemektedir[10].

Mobil uygulamalar faaliyet alanlarına ve kuruldukları akıllı cihazın türüne göre farklılık arz etmekle beraber genel olarak şu verileri işlemektedir: Cihaz bilgileri[11], cihazın bağlı olduğu internet bilgileri[12], üyelerin kimlik bilgileri, telefon numarası, elektronik posta, konum bilgileri, görsel ve işitsel dokümanlar, kayıtlı numaralar, arama kayıtları, internet kullanım istatistikleri...

[10] Bir uygulama çalışmak için herhangi bir kişisel veriye ihtiyaç duymasa dahi, yüklendiği cihaz üzerinden gerçek bir kişiye ulaşma ihtimali oldukça yüksektir. Çünkü bu uygulamaların önemli bir kısmına kişilerin üye olduktan sonra kullanabildiği mobil uygulama mağazalarından erişilebilmektedir. Ancak diğer kurulum yöntemleriyle yahut farklı kimlik verileriyle açılacak hesaplar üzerinden yapılan indirme işlemlerinde uygulama üzerinden kullanıcının kişisel verilerine ulaşım engellenebilir.

[11] Örneğin "*International Mobile Equipment Identity* (IMEI)" yani "Uluslararası Mobil Cihaz Kodu" şeklinde tercüme edilen cihazın uluslararası kimlik bilgisi bunlardan biridir. Telefon olarak üretilen her bir cihaza üretim aşamasında bir IMEI numarası verilmektedir. 15 haneden oluşan bu numara ilgili cihazın kimlik numarası olup o cihazı belirli kılmaktadır. Ancak günümüzde IMEI numaralarının çalınarak farklı bir telefona kopyalanması sık rastlanılan bir durumdur. Böyle bir durum yaşanmadığı sürece cihazın üretim kuruluşu tarafından verilen IMEI numarası her zaman için o cihazı belirlenebilir kılmaktadır.

[12] Örneğin "*Internet Protocol Adress*" yani IP adresi; internet ağına bağlı tüm cihazlara veri alışverişi için tanımlanan belirli bir adrestir. Bu internet adresi özgün numaralardan oluşur ve bilgisayar kodlama sistemine göre belirlenir. Dijital dünyada internete bağlı her cihazın IP adresi vardır.

Mobil uygulamalar verilerin bir kısmına uygulama cihaza yüklendiği an, bir kısmına ise uygulamanın kullanımı esnasında erişebilmektedir. Erişim yöntemleri ise kodlama ve yazılım şekline göre farklılık arz edebilmektedir. Mobil uygulamalar üzerinden veri elde etme yöntemleri oldukça fazla olmakla beraber çalışmada biz en yaygın kullanılan yöntemlerden büyük veri ve veri madenciliği yöntemleri üzerinde duracağız.

1. Büyük Veri (*Big Data*)

Yapılan araştırmalarda dünya genelinde fiziki ve dijital ortamda kaydedilen toplam verilerin 2025 yılına kadar 175 zettabayta[13] ulaşması beklenmektedir[14]. Yine aynı araştırmada günümüzde kaydedilen toplam verilerin tamamına yakınının son birkaç yılda elde edildiği ifade edilmektedir. Bu istatistikler bizi büyük veri (*big data*) kavramına götürmektedir.

Büyük veri, geleneksel[15] veri tabanı tekniklerinin kullanılmasıyla işlenmesi mümkün olmayan, farklı hacimlerdeki heterojen veriyi tanımlayan yeni bir kavramdır ve çeşitli dijital içeriklerden meydana gelmektedir[16].

Büyük veri ile tek başına değersiz, etkisiz ve hükümsüz görünen veriler farklı algoritmalar ve teknik yöntemlerle birleştirilip sentezlenerek kullanılmakta ve satılmaktadır[17].

Büyük veriyi tanımlamak için 4V kuralı kullanılmaktadır[18]. Bunlar:

---

[13] 1 zettabayt: 1024 eksabayt, 1048576 petabayt, 1073741824 terabayt, 1099511627776 gigabayt, 1125899906842620 megabayt, 1152921504606850000 kilobayt, 1180591620717410000000 bayt ve 1208925819614630000000000 bit'e eşittir.

[14] Aparavi, Big Data Growth Statistics to Blow Your Mind (or, What is a Yottabyte Anyway?), Nisan 2017, <https://www.aparavi.com/data-growth-statistics-blow-your-mind/> Erişim Tarihi 22 Nisan 2021.

[15] Geleneksel kayıt yöntemlerinden ziyade makine öğrenmesi (*machine* learning) ve derin öğrenme (*deep learning*) yöntemleriyle büyük veri elde edilmektedir. Çok sayıda verinin birden çok katmandan oluşan hiyerarşik devinimlerle anlamlandırıldığı bir metot olarak derin öğrenme, devasa büyüklük ve genişlikte veri setlerini ezberleyerek büyük veriyi oluşturmaktadır. Seda Kara Kılıçarslan, "Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", 2019, 4(2), Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi Dergisi, s. 368.

[16] Youssef Gahi, Mouhcine Guennoun ve Hussein T. Mouftah, "Big Data Analytics: Security and privacy challenges", IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 2016, s. 953.

[17] Muammer Ketizmen ve Aslıhan Kart, "Kişisel Veri ve Rekabet Hukuku Kapsamında -Big Data-", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 66.

[18] Bu dört kavrama ilaveten "*value*" yani "değer" kavramını dahil ederek 5V kuralı olarak açıklayanlar da vardır. Muhammet Atalay ve Enes Çelik, "Büyük Veri Uygulamasında Ya-

Veri hacmi (*volume*), veri hızı (*velocity*), veri çeşitliliği (*variety*) ve veri doğrulama (*veracity*) şeklinde sıralanmaktadır[19]. Bu dört bileşen göz önünde bulundurulduğunda karşımıza günümüz dijital dünyasının üzerinde farklı çalışmalar yaptığı büyük veri (*big data*) kavramı çıkar. Ancak uygulamada ve bilimsel çalışmalarda üzerinde uzlaşılmış net bir büyük veri tanımı bulunmamaktadır. Article 29 Working Party tarafından hazırlanan bildiri[20] uyarınca büyük veri; bazıları iyi tanımlanmış bazıları ise hala belirsiz ve yakın gelecekte geliştirilmesi beklenen çok sayıda veri işleme faaliyetini kapsayan geniş bir terimdir.

Büyük veri kavramı, genel olarak bilgi, teknoloji, yöntem ve etki kavramları ile ilişkilendirilmektedir. Bununla beraber bu kavramı tanımlayabilmek için kullanılan hız, verinin gerçek zamanlı olması; çeşitlilik, verinin çeşitli kaynaklardan elde edilebilir olması; hacim, verinin büyük veri kümelerinden oluşması ve değer ise kullanımının bir fayda yaratması şeklinde açıklanmaktadır[21].

Büyük veri birçok kaynaktan beslenmekle beraber[22], temel olarak şu üç kaynaktan veri elde ettiği ifade edilmektedir[23]:

- Dolaşan veriler,
- Sosyal medya uygulamaları üzerinden toplanan veriler,
- Kamuya açık veri tabanlarında bulunan veriler.

Farklı kaynaklardan beslenen büyük veri teknolojileri reklam, pazarlama,

---

pay Zekâ ve Makine Öğrenmesi Uygulamaları", 2017, 9(22), Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, s. 156.

[19] Daniar Supriyadi, "Personal and Non-Personal Data in the Context of Big Data", Tilburg Institute for Law, Technology and Society, 2017, s. 12-13, <http://arno.uvt.nl/show.cgi?fid=142300> Erişim Tarihi 13 Nisan 2021.

[20] Article 29 Working Party, "Statement on Statement of the WP 29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU", WP 221, Bildiri, 16 Eylül 2014, s. 3. Bildiriye ulaşmak için bkz. <https://www.pdpjournals.com/docs/88352.pdf> Erişim Tarihi 23 Nisan 2021.

[21] Şehriban İpek Aşıkoğlu, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Oniki Levha Yayınları, 2018, s. 21.

[22] Ertuğrul Aktan, "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu", 2018, 1(1), Bilgi Yönetimi Dergisi, s. 6.

[23] Aşıkoğlu, 2018, s. 22.

istihbarat, suç ile mücadele, sağlık[24], ulaşım, akademik çalışmalar, sosyal bilimler gibi birçok alanda kullanılmaktadır. Örneğin belirli bir toplumun tüketim alışkanlarını yahut hobilerini tespit edebilmek için birey bazlı anket yapmak yerine günümüzde büyük veri uygulamaları tercih edilmektedir[25]. Temelde büyük veri uygulamaları ile amaçlanan, yığın halinde ve anlamsız olarak bulunan yüksek hacimli veriden anlamlı sonuçlar çıkarmaktır[26]. Bunun için kullanılan yöntemlerden bir diğeri veri madenciliğidir.

2. Veri Madenciliği (*Data Mining*)

Teknolojik gelişmelerin geldiği konum itibariyle veri kaydı yapılan alanların sayısı artmış ve bu alanlarda saklanan veri miktarı insan aklının sınırlarını zorlayacak düzeye erişmiştir. Erişilen veri miktarı bakımından büyük veri kavramı hakkında yukarıda açıklamalarda bulunduk. Büyük verinin içindeki verilerden yola çıkarak bir sonuca ulaşma yöntemlerinden biri de veri madenciliğidir.

Veri madenciliği; büyük miktardaki verileri işleyerek, bu verilerin içinden bağlantılı olabilecek olanları bulmaya yardımcı olan ve veri tabanı sistemleri içerisinde gizli kalmış bilgilerin bulunarak çekilmesini sağlayan veri analiz tekniği olarak açıklanmaktadır[27]. Daha kısa anlatımla, çok büyük miktardaki veriden istenilen desenlerin ya da bilginin çıkarılması sürecidir[28]. Bu bakımdan, veri madenciliği yerine; veri tabanlarından bilgi keşfi, bilgi çıkarma, veri analizi, veri arkeolojisi, veri tarama, iş zekâsı gibi alternatif

---

[24] Özellikle Covid19 küresel salgını sonrası yapılan aşı çalışmalarında sağlık verileri ve genetik verilerin ne kadar önemli olduğu bir kez daha anlaşılmıştır. Sağlık alanında büyük veri işleme faaliyetleri hakkında bkz. Wullianallur Raghupathi ve Viju Raghupathi, "Big data analytics in healthcare: promise and potential", 2014, 2(3), Health Information Science and Systems, s. 1-10.

[25] Başka bir örnek olarak GSM operatörlerinin edindiği mobilite verilerinin navigasyon ve trafik yoğunluğunun gösterilmesi hizmetlerinde de kullanılması gösterilmektedir. Ketizmen ve Kart, s. 67.

[26] Aşıkoğlu, 2018, s. 22.

[27] Bir başka çalışmada; büyük veri yığınları içerisinden gelecek hakkında tahminde bulunabilmeyi sağlayabilecek bağıntıların bilişim teknolojilerinin sağladığı imkânları kullanarak, matematik, istatistik, mantık gibi bilim dallarının katkısı ile bulunması süreci olarak açıklanmaktadır. Canan Özcan, "Veri Madenciliğinin Güvenlik Uygulama Alanları ve Veri Madenciliği ile Sahtekârlık Analizi", İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı Yayımlanmamış Yüksek Lisans Tezi, 2014, s. 1.

[28] Talha Murathan ve Sebahattin Devecioğlu, "Veri Madenciliği ve Spor Alanındaki Uygulamaları", 2018, 29(3), Hacettepe Journal of Sport Sciences, s. 147.

adlandırmalar da kullanılmaktadır[29]. Özellikle otomatik karar mekanizmaları tarafından veri madenciliğinden yararlanılmaktadır[30].

Veri madenciliği yeni ve disiplinler arası bir alana sahip olarak farklı disiplinlerde aktif olarak kullanılmaktadır. Özellikle veri tabanı sistemleri, veri görselliği, matematiksel modelleme, istatistik, yapay zekâ, spor, pazarlama, finans, tıp, mühendislik, sigortacılık, borsa, perakendecilik, telekomünikasyon, sağlık, biyoloji, genetik, hukuk, endüstri, güvenlik, istihbarat, optimizasyon vb. alanlarda kullanılabilmektedir[31].

İnsan yaşamını ilgilendiren hemen her alanda kullanılan veri madenciliği özellikle mobil uygulamalar üzerinden faaliyette bulunan firmalar için çok önemlidir. Bu firmalar ellerinde bulunan veriler üzerinden çıkardıkları analiz sonucunda daha anlamlı ve işlevsel bilgiler elde etmekte ve elde edilen bu bilgileri reklam, pazarlama, satış stratejisi yahut başka amaçlarla kullanabilmektedir.

Mobil uygulamalar üzerinden elde edilen veriler üzerinde yapılan tasarruflar veri işleme faaliyeti olarak adlandırılmaktadır. Bu faaliyetler hakkında ayrı bir başlık altında bilgi vermekte fayda mülahaza etmekteyiz.

II. Mobil Uygulamalar Üzerinden Veri İşleme Faaliyetleri ve Kişisel Veriler

A. Veri İşleme Faaliyetleri

Gündelik hayatta her gün kullandığımız bilgisayar, cep telefonu, tablet, televizyon, akıllı saat, oyun konsolu ve diğer birçok elektronik cihaz internet yahut kendilerini birbirlerine bağlayan başka sistemler[32] üzerinden elde ettikleri verileri işlemektedir.

---

[29] Tuncay Özcan, Veri Madenciliği, İstanbul Üniversitesi Yayınları, 2015, s. 7. Çalışmaya şu adresten ulaşılabilir:
<http://auzefkitap.istanbul.edu.tr/kitap/endustrimuhlt_ue/verimadenciligi.pdf> Erişim Tarihi 25 Nisan 2021.

[30] Liane Colonna, "Mo' Data, Mo' Problems? Personal Data Mining and the Challenge to the Data Minimization Principle", 2013, 18, Big Data And Privacy Making Ends Meet, Standford Law School, The Center for Internet And Society, s. 20, <https://fpf.org/wp-content/uploads/2021/05/Big-Data-and-Privacy-Paper-Collection.pdf> Erişim Tarihi 18 Nisan 2021.

[31] Murathan ve Devecioğlu, s. 150.

[32] Günümüzde internet dışında örneğin radyo frekansı ile tanımlama (RFID) ve sensör teknolojilerinin gelişmesi, kullanımın artması ile birlikte gündelik hayatın her alanında çeşitli kaynaklardan verilerin toplanması olanaklı hale gelmiştir. Aşıkoğlu, 2018, s. 21.

Veri işleme faaliyeti ile anlatılmak istenen; verilerin tamamen veya kısmen otomatik olan yahut herhangi bir veri kayıt sisteminin parçası olmak şartıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, değiştirilmesi, depolanması, korunması, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü tasarruftur[33]. Örneğin, verilerin belirli bir yerde (bulut sistemleri, hard-disk, CD, USB bellek vs.) tutularak depolanması, başka hiçbir işlem yapılmasa dahi, bir veri işleme faaliyeti olarak kabul edilir. Bu bakımdan verilerin elde edilmesi ve kaydedilmesinden başlayarak veriler üzerinde yapılan tüm işlemler veri işleme faaliyeti olarak kabul edilir.

Günümüzde internet siteleri, bilgisayar programları ve mobil uygulamalar başta olmak üzere elektronik cihazlar üzerinden toplam işlenen veri sayısı tahmin edilemez boyutlara ulaşabilmektedir. İşlenen verilerden bir kısmı hukuk sistemleri için ayrıca koruma mekanizması gerektiren bir alandır. Kişisel veriler ve dahi bu grup içerisinde yer alan bir grup hassas veri, özel hayatın gizliliği hakkı kapsamında hukuk normlarınca korunmakta ve güvence altına alınmaktadır.

B. Veri-Kişisel Veri Ayırımı

"Veri" kavramı, bilişim literatüründe "*olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli şekilde gösterimi*"[34], "*bir çözüme ulaşmak için işlenebilir duruma getirilmiş gözlemler, ölçümler*"[35], "*bilgisayar için işlenebilir duruma getirilmiş sayısal ya da sayısal olmayan nicelikler*"[36] olarak farklı şekillerde ifade edilebilir. Ancak bu kavram günümüzde daha çok "bilgi" kavramını açıklamakta kullanılmaktadır. Bu bakımdan veri, kelimeler ve sayılar gibi kayıt altına alınmış ancak biçimlendirilmemiş bilgi olarak da ifade edilebilir.

Veri kavramı kendi başına değersizdir. Başka bir ifade ile tek başına bir anlamı yoktur. Veriyi anlamlı kılan faaliyetlerden birisi olarak veri

---

[33] Konuyla ilgili daha ayrıntılı bilgi için ayrıca bkz. Aşıkoğlu, s. 70; Elif Küzeci, Kişisel Verilerin Korunması, 4. Baskı, Oniki Levha Yayınları, 2020, s. 16; Gamze Turan Başara, "Kişisel Veri İşleme Sözleşmesi", 2020, 8(16), Uyuşmazlık Mahkemesi Dergisi, s. 59-64; Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2. Baskı, Oniki Levha Yayınları, 2019, s. 46.

[34] TDK Güncel Türkçe Sözlük, <https://sozluk.gov.tr> Erişim Tarihi 19 Kasım 2021.

[35] TDK Güncel Türkçe Sözlük, <https://sozluk.gov.tr> Erişim Tarihi 19 Kasım 2021.

[36] Bilişim Sözlüğü, <http://www.bilisimsozlugu.net/data> Erişim Tarihi 19 Kasım 2021.

madenciliğine yukarıda değindik. Ancak çalışma planımız esas olarak veri madenciliği değil, kişiyi belirli ya da belirlenebilir kılan veri olarak kişisel veri kavramı üzerine kuruludur. Bu bakımdan kişisel veri kavramı ile anlatılmak istenin ne olduğunu kısaca açıklamakta fayda görmekteyiz.

Kişisel veri kavramı bu alana dair ulusal ve uluslararası düzenlemelerde "kimliği belirli yahut belirlenebilir gerçek kişiye yani insanlara ait tüm bilgileri" ifade eder şekilde kullanılmaktadır. Gerçek kişilerle ilişkilendirilemeyen veriler ise anonim veri olarak nitelendirilmekte ve bu tür verilere kişisel verilerin korunması mevzuatında koruma sağlanmamaktadır[37].

Kişisel verilerin içinde bazı veriler yapıları gereği daha büyük önem arz etmektedir. Özel nitelikli kişisel veriler (*special categories of personal data*) ya da hassas veri (*sensitive data*) olarak adlandırılan bu gruptaki veriler, başkalarınca öğrenildiği takdirde ilgili kişinin daha fazla zarara uğramasına yahut ayrımcılığa maruz kalabilmesine sebep olabilecek nitelikteki verilerdir. Bu tür verilerin işlenmesi genel olarak kişisel verilerin işlenmesi şartlarından daha özel şartlara tabi tutulmuştur. Başka bir anlatımla, bu tür veriler ayrımcılık gibi sorunlara sebebiyet verme ihtimalinin yüksekliğinden dolayı diğer kişisel verilere göre daha fazla koruma uygulanan küçük bir grup veri olarak değerlendirilebilir[38]. Nitekim Türk Hukukunda 6698 sayılı Kişisel Verilerin Korunması Kanununda hangi kişisel verilerin özel nitelikli olduğu tahdidi olarak belirtilmiş olup[39], bu sayılanlar dışındaki veriler özel nitelikli olarak kabul edilmemektedir. Bu bakımdan, özel nitelikli kişisel verilerin belirlenmesi hususunda sınırlı sayı (*numerus clausus*) ilkesinin benimsendiğini söyleyebiliriz.

Özel nitelikli kişisel veriler ayrıca belirtilmekte ve diğer kişisel verilere karşı daha sıkı tedbirlerle korunmakta ise de kanaatimizce kişisel veriler arasındaki bu ayırım sadece belirli grup (özel nitelikli) kişisel verilerin kişiler için daha büyük zararlar ortaya çıkarma ihtimalinin yüksekliğindendir.

---

[37] Aşıkoğlu, 2018, s. 11. Gerçek kişiyle ilgilendirilmeyen büyük veriler hukukun farklı alanlarına (Telif Hukuku, Sözleşme Hukuku, Sorumluluk Hukuku) ait düzenlemelerde koruma mekanizmalarından faydalanabilir. Ancak Kişisel Verilerin Korunması Hukuku bakımından korunan özne muhakkak gerçek kişiler olmalıdır.

[38] Küzeci, 2020, s. 281.

[39] "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir*" (m. 6/1).

Kişisel veriler günümüz demokratik hukuk sistemlerinde anayasal düzeyde koruma altına alınmaktadır. Zira içinde bulunduğumuz dijital çağda kişilere ait veriler ekonomik, sosyal, siyasi ve daha birçok alanda hazine niteliğindedir. Bu hazineye ulaşma yollarından biri de mobil uygulamalardır. Özellikle ücretsiz indirilen ve kullanılabilen mobil uygulamalara karşı daha temkinli olmakta fayda vardır. Nitekim son yıllarda özellikle ücretsiz hizmet sunan platformlara karşı şu argüman dile getirilmektedir: "Parasını ödemiyorsan ürün sensin!"[40]. Bu ifadenin doğruluk payı olmakla beraber; ücretsiz tüm ürün ve hizmetlerin kullanıcı ve müşterilerinin kişisel verilerini işlediğini söylemek kanaatimizce doğru değildir. Zira günümüzde şirketler müşterilerine verdiği güven ve yaygın kullanım gibi etmenlerle piyasa değerlerini yükselterek daha fazla kâr elde edebilmektedir. Bu bakımdan belirli zamanlarda ürünleri ve/veya hizmetlerini ücretsiz şekilde kullanıma sunarak hacmini genişleterek şirketin değerini arttırmaktadır. Ancak biz yine de ücret mukabilinde yahut ücretsiz şekilde kullanılan mobil uygulamalar için kişisel verilerin korunması mevzuatı ile getirilen asgari yükümlülüklerin yerine getirilmesi ve uygulama kullanıcılarının kullanım esnasında bilinçli bir şekilde davranmaları gerektiği kanaatindeyiz.

III. Mobil Uygulamalarda Kişisel Veriler İşlenirken Yerine Getirilmesi Gereken Hususlar

Akıllı cihazlar, mobil uygulamalar sayesinde kişilerin ihtiyaçlarına uygun özelliklerle donanarak insanların sosyal hayatında çok önemli bir konuma gelmiştir. Bu uygulamalar, insanların haberleşme başta olmak üzere farklı sosyal gruplarla bağlantı kurmalarında ve gündelik hayatlarını düzenlemede fonksiyonel birer araç olarak değerlendirilmektedir. Başka bir ifade ile akıllı cihazları diğer mobil teknolojilere göre farklı kılan, daha fonksiyonel, kullanışlı ve kişiye özel olmasını sağlayan en önemli özellik bu cihazlar için geliştirilen mobil uygulamalardır[41].

Kişiye özel kullanıma müsait olan mobil uygulamaların elde ettiği verilerden yola çıkarak kullanıcıya ulaşmak ise günümüz teknolojisinin geldiği nokta bakımından çok daha kolaydır. Bu bakımdan mobil uygulamalar üzerinden elde edilen ve işlenen veriler bakımından kişisel verilerin korunması mevzuatı hükümleri dikkate alınmak zorundadır. Aksi halde mobil uygulama

[40] Margaret McGartney, "If you don't pay for it you are the product", 2018, 362, BMJ. <https://www.bmj.com/content/362/bmj.k3249> Erişim Tarihi 20 Kasım 2021.

[41] Uğur ve Turan, s. 74.

kullanıcılarının kişisel verileri başta olmak üzere özel hayatlarının gizliliği ihlal edilecektir. Temel hak ve özgürlüklerin güvence altına alındığı demokratik hukuk sistemlerinde böyle bir ihlal durumunda mobil uygulama üretici ve işleticilerinin hukuki, cezai ve idari sorumlulukları gündeme gelecektir.

Mobil uygulama işleticilerinin kişisel verilerin korunması alanındaki hak ve yükümlülüklerini ele almadan evvel Veri Koruma Hukukunda riayet edilmesi gereken temel ilkeleri kısaca açıklamakta fayda görmekteyiz. Kişisel veri işlenmesine ilişkin kurallar, izinler ve yasaklardan oluşan şu sekiz ilke faaliyetlerini hukuka uygun bir şekilde icra etmek isteyen herkes için uygulanacak tüm düzenlemelerin esasını oluşturmaktadır. Bu ilkeleri genel olarak[42];

1. Kişisel verileri hukuka ve dürüstlük kurallarına uygun bir şekilde toplama ve işleme,

2. Kişisel verilerin işlendikleri amaçla sınırlı ve ölçülü olması (veri minimizasyonu ilkesi),

3. Kişisel verilerin hukuka uygun bir şekilde önceden belirlenmiş olan amaçlar dahilinde işlenmesi (amaca bağlılık ilkesi),

4. Belirlenen amaçlar dışında başka bir amaç için kişisel verilerin kullanımının, ancak veri sahibinin rızası veya kanunlarda izin verilmesi hallerinde mümkün olması (açık rıza-kanunilik)

5. Kişisel verilerin doğru, tam ve işlenme amaçları ile ilgili olması (güncellik ilkesi),

6. Kişisel verilerin ifşa, değiştirilme yahut yok edilme gibi hukuka aykırı işlemlerden korumak için gerekli güvenlik önlemleri alınması (verilerin korunması ilkesi),

7. İlgili kişilerin, işlenen verileri hakkında bilgilendirilmesi, bunlara erişimlerinin temini ve düzeltme hakkına sahip olması (bireysel katılım ilkesi),

8. Veri sorumlularının hukuki, cezai ve idari sorumluluklarının işletilmesi,

---

[42] Lee A. Bygrave, "Data Protection Pursuant to Right to Privacy in Human Rights Treaties", 1998, 6(3), International Journal of Law and Information Technology, s. 250. Makaleye ayrıca şu adresten de ulaşılabilir:
<https://academic.oup.com/ijlit/article/6/3/247/655366> Erişim Tarihi 26 Nisan 2021.

şeklinde sekiz başlık altında toplamak mümkündür[43]. Bu ilkeler üzerine doktrinde halihazırda fazlasıyla çalışma bulunmaktadır[44]. Biz bu başlık altında çalışma konumuzu ilgilendiren ve uygulamaya yönelik şu üç husus üzerinde duracağız.

A. Aydınlatma Yükümlülüğü

Hukuka uygunluğun denetiminde aydınlatma metinleri temel hak ve özgürlüklerin merkezini oluşturmaktadır. Bu bakımdan aydınlatma yükümlülüğü veri işleme faaliyetinin hukuka uygunluğunun denetlenmesinde ve ilgili kişilerin verileri üzerinde hakimiyetlerini korumalarında bel kemiği vazifesi görmektedir[45].

Aydınlatma yükümlülüğü esasında şeffaflık ve hesap verilebilirlik ilkelerinin gerekliliğidir. Bu ilkeler kamu idareleri ve şirketler için olduğu kadar kişisel veri işleyen herkes için bağlayıcıdır[46].

Mobil uygulamalarda işlenen kişisel verilerin düzeyine ilişkin yukarıda yaptığımız açıklamalar doğrultusunda, mobil uygulama kullanıcılarının kişisel verilerinin korunması hakkının uygulaması bakımından aydınlatma metinleri olmazsa olmaz bir unsurdur[47].

Mobil uygulama aydınlatma metinlerinin şeffaflık ilkesi uyarınca ilgili kişiyle ya da kamuyla paylaşılacak olan bilginin sade, şeffaf, anlaşılır, kolayca ulaşılabilir ve basit bir dille hazırlanmış olması gerekmektedir. Açık

---

43 Bu ilkeler, kişisel verilerin korunmasına dair uluslararası düzenlemeler (GDPR m. 5, 108+ sayılı Konvansiyon m. 5) ve Türk Hukuk mevzuatında bu alandaki özel düzenleme olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda da (m. 4) yer almaktadır.

44 Aşıkoğlu, 2018, s. 79-89, 115-136; Çekin, s. 61-72; Küzeci, 2020, s. 227-277; Salih Polater, "Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 1-20.

45 Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda", 2019, 1(2), Kişisel Verileri Koruma Dergisi, s. 41.

46 Bu yükümlülüğün yerine getirilmesi bakımından muaf tutulan kişiler mevzuatta açıkça düzenlenmelidir. Nitekim hem Avrupa Veri Koruma Tüzüğü (GDPR) hem de 6698 sayılı Kişisel Verilerin Korunması Kanununda aydınlatma yükümlülüğünden muaf olanlar özel olarak sayılmaktadır (m. 28).

47 Mobil uygulamalar ve bu uygulamaların yer aldığı akıllı cihazların otomatik veri işleme faaliyetleri karşısında ilgili kişilerin haklarının korunabilmesi için şeffaflık ilkesinin uygulama işleticileri tarafından her aşamada benimsenmesi gerekmektedir. Mireille Hildebrandt, "The Dawn of a Critical Transparency Right for the Profiling Era", Digital Enlightenment Yearbook, IOS Press, 2012, s. 45. Makaleye şu adresten ulaşılabilir: <https://core.ac.uk/reader/16178580> Erişim Tarihi 8 Mayıs 2021.

ve anlaşılır bir dille kaleme alınmayan bir aydınlatma metni açık rızanın doğru bilgilendirmeye dayalı olma unsurunu sağlamayacağından veri işleme faaliyetini hukuka aykırı hâle getirecektir[48]. Yine aydınlatma metninde veri işleme şartlarının ilgili kişiye kasten yahut ihmal suretiyle yanlış, hatalı ya da eksik olarak bildirilmesi ilgili kişinin yanılmasına yol açıyorsa dürüstlük kuralı da ihlal edilmiş olacak ve veri işleme faaliyeti hukuka aykırı hale gelecektir[49].

Mobil uygulama işleticilerinin dikkat etmesi gereken bir başka husus ise uygulamalarda yapılacak değişiklikler ve güncellemeler sonrası veri işleme faaliyetinde de bir değişiklik söz konusu olmaktaysa bu durumun kamuoyuna ve kullanıcılara bildirilmesi ve aydınlatma metninin revize edilmesi gerekliliğidir.

Mobil uygulamalar için aydınlatma yükümlülüğünün yerine getirilme şekli bakımından farklı yöntemler tercih edilebilir. Mobil uygulamanın yüklü olduğu akıllı cihazın türüne göre yazılı metin[50] halinde olabileceği gibi, görsel şema, video, infografik yahut sesli mesaj yolları ile bu yükümlülük yerine getirilebilir.

Fransız Veri Koruma Kurumu (CNIL), şeffaflık ilkesine riayet etmediği ve aydınlatma metninin kolay ulaşılabilir olmadığı gerekçesiyle Google hakkında 50.000.000 EURO idari para cezası vermiştir[51]. Türkiye Cumhuriyeti Kişisel Verileri Koruma Kurumu da ulaşım hizmeti sunan bir mobil uygulamanın aydınlatma metninde yer almayan bir faaliyet üzerinden kullanıcılarının kişisel verisini işlediği gerekçesiyle uygulamayı işleten firmaya idari para

48 Aşıkoğlu, 2019, s. 44.

49 Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 48-49.

50 İnternet ortamında yazılı metinlerin kullanıcılara sunulması için '*click-wrap* (tıklama yoluyla kabul)', '*browse-wrap* (kabul edilecek metne göz gezdirme/göz atma)' ve '*sign-in-wrap contact* (oturum açma işlemi)' olarak adlandırılan farklı yöntemler kullanılmaktadır. Bir bağlantıya tıklayarak metnin açılması veya metnin bir kutucuğun içinde (HTML dilinde *textarea* veya *iframe* gibi) sunulması gibi farklı yöntemler hakkında daha fazla bilgi için bkz. Uri Benoliel and Shumel I. Becher, "The Duty to Read the Unreadable", 2019, (60), Boston College Law Review, s. 2255-2296.

51 The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority), Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.

<https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> Erişim Tarihi 1 Mayıs 2021.

cezası vermiştir[52]. Yine Kurul'un farklı bir kararında çevrim içi platformlarda aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiğine hükmedilmiştir[53].

Türkiye Cumhuriyeti Kişisel Verileri Koruma Kurumu'nun verdiği isabetli karardan da görüleceği üzere mobil uygulamalarda aydınlatma metni üzerinden kullanıcıların açık rızasının alınması hukuka aykırı olup; açık rıza beyanının ayrı bir işlemle alınması gerekmektedir.

B. Açık Rıza Beyanı

Sözlükte[54] "razı olma, isteme, istek" olarak açıklanan "rıza (*consent*)" kavramı hukukun çeşitli alanlarında hukuka uygunluk sebebi olarak kabul edilmektedir[55]. Veri Koruma Hukukunda ise kişilik haklarının önemine binaen salt rıza kavramı ile yetinilmeyerek "açık rıza (*explicit consent*)" kavramının kullanımı tercih edilmektedir. Bu bakımdan kişisel verilerin işlenmesinde hukuka uygunluk halleri müstesna olmak üzere kişisel verilerin işlenebilmesi ve aktarılabilmesi için veri sahibi ilgili kişinin açık rızası aranmaktadır[56].

95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunmasına İlişkin Avrupa Konseyi Direktifine göre açık rıza; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde mahal vermeyecek şekilde ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır. 6698 sayılı Kanundaki tanımıyla açık rıza "*Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı*" ifade etmektedir (m. 3/1-a). Bu ifade doğrultusunda rıza, ilgili kişinin sahip olduğu verinin işlenmesine, kendi isteği ile veya veri sorumlusu tarafından gelen istek üzerine, onay vermesi anlamını taşımaktadır.

---

52 Karar No: 2020/65, Karar Tarihi: 27.01.2020. Karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/6717/2020-65> Erişim Tarihi 27 Nisan 2021.

53 Karar No: 2018/90, Karar Tarihi: 26.07.2018. Karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5420/2018-90> Erişim Tarihi 27 Nisan 2021.

54 TDK Güncel Türkçe Sözlük, <https://sozluk.gov.tr> Erişim Tarihi 10 Mayıs 2021.

55 Roma Hukukunda, "*volenti non fit iniuria*" (rızanın olduğu yerde hukuka aykırılık olmaz), "*nulla iniuria est, quae in volentem fiat*" (rızayla gerçekleştirilen fiil haksızlık oluşturmaz) ilkeleri benimsenmektedir. Alperen Polat, Sorumluluk Hukukunda Rıza, On İki Levha Yayınları, 2019, s. 39.

56 Uluslararası hukuki düzenlemeler ve karşılaştırmalı hukukta aranan bu şart 6698 sayılı KVK Kanununda da yer almaktadır (m. 5-6, 8-9).

Veri işleme faaliyetini hukuka uygun hale getirecek açık rızanın belirli unsurları bulunmaktadır. Bunlar[57]:

- Belirli bir konuya ilişkin olma,
- Rızanın bilgilendirmeye dayanması,
- Rızanın özgür iradeyle açıklanması.

Mobil uygulama kullanıcılarının kişisel verilerinin işlenebilmesi ve aktarılabilmesi için, hukuka uygunluk sebebi bulunan haller hariç olmak üzere, kullanıcıların açık rızasını almak gereklidir. Rızanın alınması herhangi bir şekil şartına bağlanmamıştır ancak rızanın varlığını ispat yükü veri sorumlusu olarak mobil uygulama işleticisindedir.

Rıza beyanı yazılı olarak alınabileceği gibi, elektronik ortamda yahut çağrı merkezi üzerinden farklı yollarla da alınabilir. T.C. Kişisel Verileri Koruma Kurumu rızada şekil şartı aramamakla beraber rızada kişinin "olumlu irade beyanı"nın açıkça anlaşılması gerektiğini ifade etmektedir[58].

Mobil uygulama kullanıcıları yeterli düzeyde aydınlatıldıktan sonra ayrı bir işlem ile bu kullanıcıların açık rızalarına başvurulmalıdır. Veri işleme faaliyetine başlamadan evvel açık rıza alınması gerekmektedir. Kullanıcının tepki göstermeksizin uygulamayı kullanmaya devam etmesi açık rıza gösterdiği anlamına gelmez ve veri işleme faaliyetini hukuka aykırı hale getirir[59].

---

[57] Kişisel Verileri Koruma Kurumu, Açık Rıza, KVKK Yayını, 2018a, s. 5, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf> Erişim Tarihi 13 Nisan 2021.

[58] Kişisel Verileri Koruma Kurumu, 2018a, s. 3. AB Veri Koruma Tüzüğü'nde de rızanın geçerli olabilmesi için belirli şartlar aranmaktadır. Tüzükteki ilgili düzenleme şöyledir: "*Veri sahibinin rızasının diğer hususlarla da ilgili olan yazılı bir beyan bağlamında verilmesi durumunda, rıza talebi diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulur. Söz konusu beyanın bu Tüzük açısından ihlal teşkil eden hiçbir kısmı bağlayıcı değildir*." (m. 7/2).

[59] Christopher Kuner, European Data Protection Law, Corporate Compliance and Regulation, 2. Edition, Oxford University Press, 2007, s. 69. Mobil uygulama kullanıcılarına "kişisel verilerinizin işlenmesine onay vermiyorsanız işaretleyin" gibi opt-out yöntemi açık rıza olarak kabul edilmemektedir. Türkiye'de de 2018/90 sayı ve 26.07.2018 tarihli Kişisel Verileri Koruma Kurulu kararında aynı ilke benimsenmiştir. Karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5420/2018-90> Erişim Tarihi 27 Nisan 2021. Hollanda Veri Koruma Kurulu da internet siteleri ve mobil uygulamalardaki çerez (*cookies*) kullanımına müsaade etmeyen kullanıcıların buralardan faydalanamamasını hukuka aykırı bulmuştur.

<https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies> Erişim Tarihi 10 Mayıs 2021.

Mobil uygulama işleticileri tarafından hukuka uygun bir şekilde rıza alındıktan sonra veri işleme faaliyetlerinde meydana gelen değişiklikler yahut hiçbir değişiklik olmasa dahi aradan uzun bir zaman geçmişse yeniden açık rıza alınması gerekmektedir[60].

İlgili kişiler[61] rıza beyanlarını diledikleri zaman geri alabilecekleri[62] gibi, rızalarının bulunduğu zaman içerisinde mobil uygulama üzerinden işlenen kişisel verileri hakkında bilgi alma hakkına da sahiptirler.

C. Veri Sorumlusuna Başvuru İmkânı (Bireysel Katılım)

Özel hayatın gizliliği kapsamında kişisel verisi işlenen gerçek kişiye yaratılan koruma alanı içerisinde verilerinin ilgili kişi tarafından kontrolünün sağlanması, kişinin özgür iradesiyle hareket etmesi ve bu irade doğrultusunda kişiliğini geliştirmesi ve geleceğini belirlemesi kişilik hakkı kapsamında temel haklar arasında yer almaktadır[63]. Nitekim uluslararası düzenlemeler ve ulusal mevzuatta[64] ilgili kişilerin kişisel verilerinin korunmasını talep etme hakkı kadar; işlenen verileri hakkında bilgi talep etme ve tasarrufta bulunma hakkı da tanınmaktadır.

Mobil uygulama işleticileri, uygulama üzerinden yahut otoritelerce belirlenen uygun yöntemler ile kullanıcılarının taleplerini almalı ve makul süre içerisinde[65] kullanıcılarını bilgilendirmelidirler. Buna göre kişisel

---

60 Kuner, s. 314.

61 Burada ayrıca değinmekte fayda gördüğümüz bir husus ise çocuklara yönelik geliştirilen mobil uygulamalardır. Türk Hukuku bakımından tam ehliyetli kategorisinde yer almayan bu kişiler için verdikleri açık rızanın hukuki geçerliliği bulunmamakla beraber; AB Veri Koruma Tüzüğü bu gruptaki çocuklar için 16 yaş sınırı getirmiştir. Tüzüğe göre: "... *doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması halinde, ilgili çocuğun kişisel verilerinin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur*. (2) *Üye devletler, 13 yaştan küçük olmamak kaydıyla, bu amaçlara yönelik olarak kanunla daha küçük bir yaş belirleyebilir*."

62 AB Veri Koruma Tüzüğü m. 7/3.

63 Elif Küzeci, "İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", 2014, 32, İnsan Hakları Yıllığı, s. 53-75.

64 Bu konudaki ulusal mevzuat: Başta Anayasa (m. 20/son) olmak üzere 6698 sayılı Kanun (m. 13) ve Kurum tarafından çıkarılan 10.3.2018 tarih ve 30356 sayılı Resmî Gazetede yayınlanarak yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'den oluşmaktadır.

65 Daha detaylı düzenlemeler 10.03.2018 tarihli Resmi Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de yer almaktadır.

verisi işlenen kişi veri sorumlusuna başvurarak işlenen verileri hakkında bilgi alabileceği gibi daha önce verdiği açık rızasını geri çekme, verilerin anonim hale getirilmesini, silinmesini yahut imha edilmesini talep etme gibi tasarruflarda bulunabilecektir. İlgili kişinin talepleri yerine getirilmezse kişi, Veri Koruma Kuruluna başvuracağı gibi; mahkemeler nezdinde dava yoluna da gidebilir.

Mobil uygulama kullanıcıları olarak gerçek kişiler tarafından veri sorumlusuna yapılacak başvurular bakımından belirli sıkıntılar yaşanmaktadır. Bu sıkıntıların başında ilgili kişilerin nereye, nasıl başvuru yapacağı yönünde yaşanan belirsizlik gelmektedir. Zira uygulama işleticilerinin büyük çoğunluğu yurt dışı yerleşik durumdadır. Bu durum başvuru sürecini büyük ölçüde zorlaştırmaktadır. Ülkeler bu hususta, özellikle sosyal medya uygulamalarını işleten şirketlere karşı, yeni kanuni düzenlemelerle veri sorumlularına yönelik temsilci atama gibi belirli yükümlülükler getirmektedir[66].

D. Teknik Tedbirler

Kişisel verilerin korunmasına dair uluslararası düzenlemelerde veri sorumlularının işlediği kişisel verilerin güvenliğini sağlamakla yükümlü olduğu ve bu kapsamda yeterli teknik önlemleri almak zorunda olduğu belirtilmektedir[67]. Ancak alınacak teknik tedbirlere ilişkin ayrı bir düzenleme yapılmamaktadır. Keza Türk Hukuk mevzuatı bakımından da kişisel verilerin korunmasına dair özel kanun olarak çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanununa göre Kişisel verilerin işlenmesi sürecinde veri sorumluları kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır (m. 12/1-c). Alınacak teknik tedbirlerin ne olacağı hususunda ise ne Kanunda ne de Kişisel Verileri Koruma Kurumu tarafından

[66] Türkiye'de 29.7.2020 tarihinde TBMM'de kabul edilen ve 31.07.2020 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe giren 7253 sayılı Kanunla, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda yapılan değişiklikler ile sosyal ağ sağlayıcı olarak adlandırılan, aynı zamanda mobil uygulama işleticisi olarak veri sorumlusu sıfatına haiz çok uluslu teknoloji şirketlerine temsilci atama yükümlülüğü getirilmiştir. Temsilci atama yükümlülüğünün yanı sıra belirli aralıklarla resmî kurumlara rapor sunma, Türkiye'deki kullanıcıların verilerini yurt dışına aktarmama gibi farklı yükümlülükler de getirilmiştir. Bu yükümlülüklere uyulmaması durumunda idari para cezası ve sonrasında giderek ağırlaşan yaptırımlar öngörülmüştür. Türkiye'deki bu son düzenlemeler Almanya ve Fransa'daki sosyal medya düzenlemelerine benzerlik göstermektedir.

[67] Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi m. 7; Avrupa Birliği Veri Koruma Tüzüğü m. 5/1-e,f.

çıkarılan diğer düzenleyici işlemlerde bir açıklama bulunmamaktadır. Ancak Kurum tarafından hazırlanan rehberlerde yer alan konulardan yola çıkarak ve uygulamadan edindiğimiz gözlemlere dayanarak teknik tedbirlerin bazılarını şöyle sıralayabiliriz[68]:

- Ağ güvenliği,
- Güvenlik duvarı,
- Saldırı tespit ve önleme sistemleri,
- Veri kaybı önleme yazılımları,
- Şifreleme,
- Erişim loğları,
- Yetki matrisi,
- Sızma testi…

Elbette bu tedbirler saydıklarımızdan çok daha fazladır. Veri sorumlularının bunların tamamını uygulamaları beklenemez. Ancak olası bir ihlal durumuna karşı yeterli önlemi alma yükümlülüğü veri sorumlusundadır. Nitekim günümüzde dijital ortamlara yönelik saldırılara sıklıkla rastlanmaktadır. Çok uluslu bir antivirüs şirketi, 2020 yılının 3. çeyreğinde kullanıcılarına karşı 16.440.264 virüs saldırısını önlediğini kamuoyu ile paylaşmıştır[69]. Bu tür saldırıların gün geçtikçe artacağı şüphesizdir[70]. Üreticilerin[71] bu durum karşısında güvenlik önlemlerini arttırması, kişisel verilerin korunması bakımından elzemdir. Aksi halde, yeterli teknik tedbir almayan veri sorumlularının hukuki ve cezai sorumlulukları gündeme gelecektir.

---

68 Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), KVKK Yayını, 2018b, s. 5,
<https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf> Erişim Tarihi 21 Kasım 2021.

69 <https://securelist.com/it-threat-evolution-q3-2020-mobile-statistics/99461/> Erişim Tarihi 26 Nisan 2021.

70 Kaspersky adlı bu şirket, bir önceki dipnottaki raporda bu rakamın 2020 yılının 2. çeyreğine göre 2.2 milyon artış gösterdiğini de bildirmektedir.

71 Mobil işletim sistemleri uygulama mağazalarına bir uygulamayı dahil ederken belirli güvenlik önlemleri almaktadır. Zira zararlı yazılımların cihaza en kolay bulaşma şekli uygulama içinde gömülü vaziyette gelmesidir. Selma Büyükgöze, "Mobil Uygulama Marketlerinin Güvenlik Modeli İncelemeleri", 2019, 12(1), Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, s. 12.

Sonuç (Değerlendirme)

Teknolojik gelişmelerin eriştiği konum itibariyle akıllı cihaz üretiminin yaygınlaşması ile insanların bu cihazlara erişimi de kolaylaşmıştır. Telefon, tablet, saat gibi akıllı cihaz kullanımının artış göstermesi bu cihazlar için özel olarak tasarlanmış yazılımlar olarak mobil uygulamalara da yansımıştır. 26 Ekim 2021 tarihinde yayımlanan bir rapora göre 2020 yılında dünya genelinde akıllı cihazlara indirilen mobil uygulama sayısı yaklaşık 218 milyar olmuştur[72].

İnsan hayatının merkezi konumuna gelen mobil uygulamalar için kişisel verilerin korunması mevzuatı bakımından uygulama üretici ve işleticileri olarak veri sorumlularının yerine getirmesi gereken hususlara çalışmada değindik. İdari yükümlülükler olarak aydınlatma yükümlülüğünün yerine getirilmesi, kullanıcıların açık rızalarının alınması, veri sorumlusuna başvuru imkanının sağlanması gibi hususlar yetkili otoriteler tarafından denetlenebilmektedir. Ancak idari yükümlülüklerinin yanı sıra mobil uygulama şirketleri kişisel verileri koruma bakımından teknik tedbirleri de almakla yükümlüdür. Ancak bu aşamada otoriteler için ciddi bir sorun karşılarına çıkmaktadır. Zira veri sorumluları idari yükümlülüklerini ne kadar yerine getirse de bilişim teknolojilerinin eriştiği konum itibariyle teknik tedbirlerin ne düzeyde alındığı tespit edilse dahi veri sorumlusu tarafından kişisel veriler üzerinde kötüye kullanım durumlarında tespit imkânı çok zordur. Çünkü veri sorumlusu sıfatıyla mobil uygulama işleticilerinin büyük çoğunluğu yurt dışı yerleşik olduğu için fiziki denetimi mümkün olamamaktadır. En çok kullanılan mobil uygulamaları işleten çok uluslu şirketlerin merkez yerleri ve bilgi depolama yerleri olarak kişisel verilerin korunması hakkına Avrupa Kıtası ülkeleri kadar özen göstermeyen ülkeleri tercih etmesi ise bu konuda zihinlerde şüpheli düşünceler uyandırmaktadır.

Tüm açıklamalarımıza ilaveten ayrıca vurgulamak istediğimiz son bir husus ise: Mobil uygulama işleticilerinin yükümlülüklerini yerine getirip getirmediğine bakmaksızın ilgili kişiler olarak kullanıcıların kendi tedbirlerini almaları gerekmektedir. Bunun için mobil uygulama kullanmaktan vazgeçmeksizin ve fakat özellikle başkaları tarafından ele geçirildiğinde ilgili kişi, çevresi ve kamu için sıkıntı doğurabilecek verilerin mobil uygulama ve dahi akıllı cihazlarda bulundurulmaması en güvenli önlem olacaktır. Örneğin,

[72] <https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/> Erişim Tarihi 21 Kasım 2021.

devlet sırrı niteliğinde bir video kaydının bir akıllı cihaz üzerinden anlık iletişim amaçlı bir mobil uygulama vasıtasıyla başka bir kaynağa gönderilme işlemi, mobil uygulama tüm yükümlülükleri yerine getirse ve teknik tedbirleri almış olsa dahi, başlı başlına risk taşımaktadır. Çünkü internet teknolojisinde bilinmeyen alan, bilinen kısmından çok daha büyüktür. Ve insanoğlu kestiremediği alanlarda her zaman temkinli olmalıdır.

KAYNAKÇA

Aktan E, "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu", 2018, 1(1), Bilgi Yönetimi Dergisi, s. 1-22.

Altunışık R, "Büyük Veri: Fırsatlar Kaynağı mı Yoksa Yeni Sorunlar Yumağı mı?", 2015, 1(1), Yıldız Social Science Review, s. 45-76.

Aparavi, Big Data Growth Statistics to Blow Your Mind (or, What is a Yottabyte Anyway?), Nisan 2017, <https://www.aparavi.com/data-growth-statistics-blow-your-mind/> Erişim Tarihi 22 Nisan 2021.

Article 29 Working Party, "Statement on Statement of the WP 29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU", WP 221, Bildiri, 16 Eylül 2014, <https://www.pdpjournals.com/docs/88352.pdf> Erişim Tarihi 23 Nisan 2021.

Aşıkoğlu Ş İ, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Oniki Levha Yayınları, 2018.

Aşıkoğlu Ş İ, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda", 2019, 1(2), Kişisel Verileri Koruma Dergisi, s. 41-65.

Atalay M ve Çelik E, "Büyük Veri Uygulamasında Yapay Zekâ ve Makine Öğrenmesi Uygulamaları", 2017, 9(22), Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, s. 155-172.

Benoliel U ve Becher S I, "The Duty to Read the Unreadable", 2019, (60), Boston College Law Review, s. 2255-2296.

Bilgili M İ, "Adaptif Bağlam Bilinçli Mobil Uygulama Geliştirme", Gazi

Üniversitesi Bilişim Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, 2014.

Buildfire, Mobile App Download and Usage Statistics (2021), Şubat 2012, <https://buildfire.com/app-statistics/#> Erişim Tarihi 20 Nisan 2021.

Büyükgöze S, "Mobil Uygulama Marketlerinin Güvenlik Modeli İncelemeleri", 2019, 12(1), Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, s. 9-18.

Bygrave L A, "Data Protection Pursuant to Right to Privacy in Human Rights Treaties", 1998, 6(3), International Journal of Law and Information Technology, s. 247-284, <https://academic.oup.com/ijlit/article/6/3/247/655366> Erişim Tarihi 26 Nisan 2021.

Colonna L, "Mo' Data, Mo' Problems? Personal Data Mining and the Challenge to the Data Minimization Principle", 2013, 18, Big Data And Privacy Making Ends Meet, Standford Law School, The Center for Internet And Society, <https://fpf.org/wp-content/uploads/2021/05/Big-Data-and-Privacy-Paper-Collection.pdf> Erişim Tarihi 18 Nisan 2021, s. 19-22.

Çekin M S, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2. Baskı, Oniki Levha Yayınları, 2019.

Gahi Y, Guennoun M ve Mouftah H T, "Big Data Analytics: Security and privacy challenges", IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 2016, s. 952-957.

Hildebrandt M, "The Dawn of a Critical Transparency Right for the Profiling Era", Digital Enlightenment Yearbook, IOS Press, 2012, <https://core.ac.uk/reader/16178580> Erişim Tarihi 8 Mayıs 2021, s. 41-56.

Kara Kılıçarslan S "Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", 2019, 4(2), Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi Dergisi, s. 363-389.

Ketizmen M ve Kart A, "Kişisel Veri ve Rekabet Hukuku Kapsamında -Big Data-", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 64-76.

Kişisel Verileri Koruma Kurumu: Açık Rıza, KVKK Yayını, 2018a, <https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf> Erişim Tarihi 13

Nisan 2021.

Kişisel Verileri Koruma Kurumu: Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), KVKK Yayını, 2018b, <https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf> Erişim Tarihi 21 Kasım 2021.

Kuner C, European Data Protection Law, Corporate Compliance and Regulation, 2. Edition, Oxford University Press, 2007.

Küzeci E, "İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", 2014, 32, İnsan Hakları Yıllığı, s. 53-75.

Küzeci E, Kişisel Verilerin Korunması, 4. Baskı, Oniki Levha Yayınları, 2020.

McGartney M, "If you don't pay for it you are the product", 2018, 362, BMJ, <https://www.bmj.com/content/362/bmj.k3249> Erişim Tarihi 20 Kasım 2021

Murathan T ve Devecioğlu S, "Veri Madenciliği ve Spor Alanındaki Uygulamaları", 2018, 29(3), Hacettepe Journal of Sport Sciences, s. 147-156.

Özcan C, "Veri Madenciliğinin Güvenlik Uygulama Alanları ve Veri Madenciliği ile Sahtekârlık Analizi", İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı Yayımlanmamış Yüksek Lisans Tezi, 2014.

Özcan T, Veri Madenciliği, İstanbul Üniversitesi Yayınları, 2015, <http://auzefkitap.istanbul.edu.tr/kitap/endustrimuhlt_ue/verimadenciligi.pdf> Erişim Tarihi 25 Nisan 2021.

Polat A, Sorumluluk Hukukunda Rıza, On İki Levha Yayınları, 2019.

Polater S, "Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 1-20.

Raghupathi W ve Raghupathi V, "Big Data Analytics in Healthcare: Promise and Potential", 2014, 2(3), Health Information Science and Systems, s. 1-10.

Supriyadi D, "Personal and Non-Personal Data in the Context of Big Data", 2017, Tilburg Institute for Law, Technology and Society, <http://arno.uvt.nl/show.cgi?fid=142300> Erişim Tarihi 13 Nisan 2021, s. 1-60.

Tractinsky N ve Lowengart O, "Web-Store Aesthetics in E-Retailing: A Conceptual Framework and Some Theoretical Implications", 2007, 1(1), Academy of Marketing Science Review, s. 1-18.

Turan Başara G, "Kişisel Veri İşleme Sözleşmesi", 2020, 8(16), Uyuşmazlık Mahkemesi Dergisi, s. 57-90.

Uğur N G ve Turan A H, "Üniversite Öğrencilerinin Mobil Uygulamaları Kabulü ve Kullanımı: Sakarya Üniversitesi Örneği", 2015, 6(2), İnternet Uygulamaları ve Yönetimi Dergisi, s. 63-79.

Yücedağ N, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", 2019, 1(1), Kişisel Verileri Koruma Dergisi, s. 47-63.

Wong S H R, "Which platform do our users prefer: Website or Mobile App?," 2012, 40(1), Reference Services Review, s. 103-115.