İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN KORUNMASI

Habibe Esra ER
114691020

Prof. Dr. Ahmet DENKER

İSTANBUL
2020

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN KORUNMASI

Habibe Esra ER
114691020

Prof. Dr. Ahmet DENKER

İSTANBUL
2020

Kabul ve Onay

114691020 Habibe Esra Er tarafından hazırlanan “Mobil Uygulamalarda Kişisel Verilerin Korunması / Protection of Personal Data in Mobile Applications” başlıklı bu çalışma dijital ortamda yapılan tez savunma sonucunda başarılı bulunarak aşağıdaki jüri tarafından yüksek lisans tezi olarak kabul edilmesine karar verilmiştir.

İlgili onaylar elektronik posta yolu ile alınmıştır.

Tez Danışmanı : Prof. Dr. Ahmet DENKER İstanbul Bilgi Üniversitesi

Jüri Üyeleri : Dr. Öğr. Üyesi M. Bedii KAYA İstanbul Bilgi Üniversitesi

Dr. Öğr. Üyesi Fatih AYDOĞAN İstanbul Üniversitesi

Tezin Onaylandığı Tarih: 11 Mayıs 2020

Toplam Sayfa Sayısı : 149 sayfa

Anahtar Kelimeler (Türkçe)	**Anahtar Kelimeler (İngilizce)**
1) Gizlilik	1) Privacy
2) Kişisel Veri	2) Personal Data
3) Kişisel Verilerin Korunması	3) Personal Data Protection
4) Mobil Uygulama	4) Mobile Application
5) Elektronik Haberleşme	5) Electronic Communication

ÖNSÖZ

Yüksek lisans tezi süresince desteğini esirgemeyen saygıdeğer danışman hocam Prof. Dr. Ahmet Denker'e, çalışma arkadaşlarım Hüsniye Çiçekçioğlu ve Hilal Çobanoğlu'na ve en yakın dostum Gülşah Süne'ye teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

İKİNCİ BÖLÜM

MOBİL UYGULAMALARDA İŞLENEN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YASAL DÜZENLEMELER

ÜÇÜNCÜ BÖLÜM

MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN KORUNMASI

KISALTMALAR

2002/58 Sayılı Direktif	2002/58 EC Sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına ilişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
6698 Sayılı Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu
95/46 Sayılı Direktif	95/46 EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AET	Avrupa Ekonomik Topluluğu
AİHS	Avrupa İnsan Hakları Sözleşmesi
AVKK	Avrupa Veri Koruma Kurulu
BTK	Bilgi Teknolojileri Kurumu
EHK	5809 Sayılı Elektronik Haberleşme Kanunu
EHGY	28363 sayılı Resmi Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik
FTC	Federal Ticaret Komisyonu
GPS	Küresel Konumlandırma Sistemi
GVKT	2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü
ICO	Birleşik Krallık Bilgi Komiserliği Ofisi
IEC	Uluslararası Elektroteknik Komisyonu
ISO	Uluslararası Standardizasyon Kurumu
Kurul	Kişisel Verileri Koruma Kurumu
SEC	ABD Menkul Kıymetler ve Borsa Komisyonu

TBMM	Türkiye Büyük Millet Meclisi
TCK	5237 Sayılı Türk Ceza Kanunu

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

ÖZET

Yüksek lisans tezi olarak hazırlanan bu çalışma, mobil uygulamaların kişisel verilerin korunması hukuku bakımından değerlendirilmesi amacıyla hazırlanmıştır. Mobil uygulamalar, başta akıllı telefonlar olmak üzere, akıllı tablet, akıllı evler, giyilebilir teknoloji vb. gibi cihazlarda belli işlevleri yerine getirmek için tasarlanan yazılımlar olarak tanımlanmaktadır. Bu çalışmada ağırlıklı olarak akıllı telefon ve akıllı tabletlerde kullanılan mobil uygulamalar incelenmiş, diğer mobil cihazlardaki uygulamalar çalışma kapsamına dahil edilmemiştir. Ayrıca özel nitelikli kişisel veriler, niteliği itibari ile ayrıntılı şekilde inceleme gerektirdiği için çalışmada özel nitelikli kişisel verileri işleyen uygulamalara sınırlı ölçüde yer verilmiştir.

Mobil Uygulamalarda Kişisel Verilerin Korunması Tezi ("Tez") ile "mobil uygulamalarda kişisel verilerin korunmasına yönelik sorunlar irdelenmiş, kişisel verilerin korunması mevzuatı kapsamında bu sektörde yer alan aktörlerin görev ve sorumluluklarının ne olduğuna ilişkin inceleme yapılmış ve mevzuatla uyumlu bir uygulama nasıl olmalıdır sorusuna cevap aranmıştır". Tezde herhangi bir ampirik çalışma yapılmamış olup Tez, mevcut ve taslak yasal düzenlemeler ve akademik çalışmaların incelenmesi yöntemiyle tamamlanmıştır.

Çalışma, dört bölümde sunulmuştur. Birinci bölümde, genel hatlarıyla mobil uygulama kavramının ne olduğu, bu sektörde yer alan aktörlerin işlevleri, organizasyonlar açısından mobil uygulamaların çeşitliliği, bu uygulamaların amaçları, içerikleri ve kullanıcıya temas eden özellikleri, kullanıcıların uygulamalardan beklentileri ve bu beklentilerin ne ölçüde karşılandığı anlatılmıştır.

Tezin ikinci ve üçüncü bölümünde ise kişisel verilerin korunmasına ilişkin yürürlükte bulunan ve taslak Avrupa Birliği ("AB") düzenlemeleri ile 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("6698 Sayılı Kanun") düzenlenmelerinde yer alan genel ilkeler, hukuka uygunluk sebepleri, açık rızanın unsurları, veri sorumlusu ve veri işleyen yükümlülükleri, ilgili kişilerin haklarının mobil

uygulama dünyasında nasıl uygulandığı ve sektör özelinde tarafların sorumlulukları, uygulama mağazalarının kabul kriterleri de incelenerek kişisel veri mevzuatına uyumlu bir mobil uygulamada dikkat edilmesi gereken unsurlara yer verilmiştir. Mobil uygulamaların elektronik haberleşmeye temas eden kısımları için ise AB 2002/58 Sayılı Direktif ile bu direktifi ilga edecek ve hala taslak aşamasında olan tüzük çalışması ile ülkemizde de 5809 Sayılı Elektronik Haberleşme Kanunu ("EHK") ve hala taslak aşamasında olan yönetmelik hükümlerine ve veri koruma otoritelerinin mobil uygulama özelinde verdiği karar özetlerine yer verilmiştir. Tezin dördüncü bölümünde iki tane örnek olay çalışması yapılmıştır. İlk olarak Cambridge Analytica olayı incelenmiş, olayda meydana gelen veri ihlali neticesinde mevcut hukuki korumanın yetersiz kaldığı, daha etkin veri koruma düzenlenmelerine olan ihtiyaç dile getirilmiştir. İkinci inceleme ise COVID – 19 salgın hastalığına ilişkin tedbir önlemleri kapsamında tüm dünyada aynı amaç doğrultusunda hazırlanan farklı temas takip mobil uygulamaların kişisel verilerin korunması mevzuatına uyumlulukları karşılaştırılarak tez tamamlanmıştır.

ABSTRACT

This study, which is a master thesis, has been prepared to evaluate mobile applications in terms of personal data protection law. Mobile applications are defined as a software that designed to perform certain functions especially for smart phones, smart tablets, smart homes, wearable technology, etc. In this study, mainly mobile applications used in smartphones and tablets were examined; applications in other mobile devices is not included in the scope of the study. In addition, sensitive personal data that requires detailed examination in terms of its quality, the applications that process sensitive personal data are included in the study to a limited extent.

With the Thesis of Protection of Personal Data in Mobile Applications ("Thesis"), "the problems related to the protection of personal data in mobile applications were examined, an examination was made regarding what the duty and responsibilities of the actors in this sector were within the scope of the protection of personal data legislation and an answer was sought to the question of how an application compatible with the legislation should be". No empirical studies have been made in the thesis, and the thesis has been completed with the examination of existing, draft legal regulations, and academic studies.

In the second and third parts of the Thesis, the general principles, legitimate reasons of processing, elements of explicit consent, the obligations of the data controller and data processor, how the rights of the individuals concerned are applied in the mobile application world and the responsibilities of the parties in the sector, the acceptance criteria of the application stores are examined, and the elements in the complied mobile application according to applicable and draft European Union ("EU") regulations and Protection of Personal Data Law No. 6698 ("Law No. 6698"). For the parts of mobile applications that are in touch with electronic communication, EU Directive No. 2002/58, and draft regulation that will abolish this directive , in our country the Electronic Communication Law No. 5809 ("EHK") and the provisions of the draft regulation and the summaries of the

decisions that given by the data protection authorities on mobile applications are featured. In the fourth part of the thesis, two case studies were reviewed. First, the Cambridge Analytica incident was examined and the need for more effective data protection arrangements was expressed, where the existing legal protection was insufficient as a result of the data breach occurring in the incident. In the second review, the thesis has been completed by comparing the data privacy compliance of different contact trace mobile applications developed for the same purpose all around the world within the scope of COVID - 19 epidemic measures.

GİRİŞ

Dijital çağ, bilgi çağı, teknoloji çağı gibi isimlerle de adlandırılan 21. yüzyılda, bilgi teknolojilerinin hızla gelişmesi, globalleşmenin de etkisiyle zaman ve mekan kısıtlaması olmaksızın bir çok alanda bilgiye erişimi kolaylaştırmıştır. 90'lı yıllarda itibaren internet kullanımının yaygınlaşması, kablosuz teknolojiler ve mobil telefonların da hayatımıza girmesiyle birlikte bir çok farklı sektör ortaya çıkmış özellikle iletişim ve tüketim alanındaki faaliyet çeşitliliği artışa geçmiştir. Bunların doğal sonucu olarak da, ekonomi, psiko-sosyoloji ve hukuk alanlarında yeni kavramlar, modeller ve disiplinler ortaya çıkmış ve bu yenilikler, mevzuatın da yeniden düzenlenmesini gerekli kılmıştır.

Akıllı telefonların icadı ve mobil cihazlarda internet kullanımının mümkün olması, internet hızının artması, cihaz ekranlarının büyümesi gibi faktörlerin de etkisiyle şirketler, kamu kurumları ve farklı sektörlerdeki organizasyonlar uygulamalarını internet siteleri dışına taşımaya başlamışlardır. Mobil cihazların yaygın kullanımı, bireylerin bu cihazları sürekli yanlarında taşıma ihtiyaçları, kullanıcıların istek ve ihtiyaçlarında meydana gelen artışla birlikte mobil uygulama pazarı gün geçtikçe daha farklı seçenekte uygulamaları piyasaya sunmaktadır. Mobil uygulamaların, mobil internet sitelerine nazaran kullanıcıyı hatırlayan fonksiyonlarının olması, kullanıcılara daha hızlı ve kolay erişim olanağı sunması, hatta internet bağlantısı olmaksızın kişilere çevrim dışı erişim imkanı tanıması, bu alanı gerek kullanıcılar gerekse hizmet sağlayıcılar bakımından daha cazip hale getirmiştir. Günümüzde bir çok kişi masaüstü veya dizüstü bilgisayarlar yerine sadece mobil cihazları ile internete girmeyi tercih etmektedirler. Seyahat, ulaşım, bankacılık, eğitim, eğlence, oyun, sosyal medya, harita, alışveriş, sağlık, spor, yemek, mesleki uygulamalar gibi alanlarda faaliyet gösteren çeşitli işletmeler bakımından da bu uygulamalar, hizmetin kişiye özgü sunulması, kişilere anında ulaşım sağlanabilmesi, kullanıcı alışkanlıklarının takip edilmesi ile doğru kişiye doğru ürünün iletilmesi açısından tercih sebebi olmuştur.

Teknolojik gelişmelerin, yeni iş modelleri meydana getirmesi, kişilere fayda sağlaması, hayatı kolaylaştırması bakımından önemi ve değeri tartışmasızdır. Öte yandan internetin kullanımı ile birlikte ortaya çıkan profilleme, davranış izleme teknikleri ile kişisel verilerin, mobil uygulamalarda da aynı şekilde işlenmesi hatta daha nitelikli izleme tekniklerinin kullanılabilir olmasının yardımıyla uygulamalar, veri işleme kapasitelerini daha da arttırmıştır. Hayatı kolaylaştıran yeni gelişmelere uyum sağlanması ihtiyacı karşısında teknoloji kullanımı artış gösterirken, bu artışla birlikte kişi davranışlarının izlenmesinin de sonucu olarak bireylerin kişisel verileri üzerinde hakimiyetinin bulunmadığı bir alan ortaya çıkmıştır. Tüm bunlar dikkate alındığında, teknolojik gelişmelere uyumun kaçınılmazlığı ile kişilerin özel alanına izinsiz müdahele imkanının yarattığı çelişkinin hukuki açıdan menfaatleri dengelemeye ve hakları korunmaya muhtaç bir alan doğurduğu açıktır. Hukuk kurallarının doğası gereği teknolojik gelişmeler ile aynı hızda ilerlemesi mümkün değildir. Ortaya çıkan teknolojik modellerin hukuki temelleri ile kişilerin bu konudaki haklarının korunmasına ilişkin düzenlemeler, ancak belli bir süre geçtikten sonra şekillenebilmekte veya yürürlükteki hukuki düzenlemelerin kıyası ile somut vakıalara uyarlanabilmektedir.

Kişisel verilerin hukuk düzeni tarafından korunması kavramına olan ihtiyaç, özellikle İkinci Dünya Savaşı sonrasında önem kazanmıştır. Bu koruma, esasen kişilerin ayrımcılığa uğramasını, toplum tarafından dışlanmasını önlemek üzere ortaya çıkmış ise de verinin değeri, günümüzde ekonomik açıdan bambaşka bir boyuta evrilmiştir.

Dünya tarihi boyunca toplumların kıymet verdiği, uğruna savaştığı değerler değişim göstermiştir. Sanayi devrimine kadar toprak, en önemli değerken sanayi devriminden sonra toprağın yerini enerji kaynakları, ucuz hammadde ve petrol almıştır. Yaşadığımız bilgi çağında ise artık en değerli kaynak, toprak ya da petrol

değil, bilginin ham maddesi olan veri olmuştur[1]. Dolayısıyla, ülkeler ve sermaye sahipleri, veriyi güçlü ve hakim konumda olmak için kullanmak adına her türlü gayreti göstermektedirler.

Mobil uygulamaların bir yanda haberleşme, multimedya hizmetleri sunmaya başlaması, diğer yanda pazarlama aracı olarak kullanılarak ticari faaliyetler açısından önemli bir pazar haline gelmesi ile sektör karmaşık bir yapıya dönüşmüş, mobil araç ve uygulamalar olmadan ticaret ve rekabet adeta imkansız hale gelmiştir. Piyasadaki uygulamaların, farklı yaş gruplarına hitap etmesi ve kullanım kolaylığı sunması geniş kitlelere ulaşma imkanı sağlamaktadır. Dolayısıyla uygulamalardan toplanan verilerin çeşitliliği, kalitesi, doğruluğu dikkate alındığında gerek ulusal gerekse uluslararası mevzuatta mobil uygulamalarda kişisel verilerin korunması konusunda düzenleme bulunmaması önemli bir eksikliktir. Tez, söz konusu eksikliği doldurmak adına bu konuda akademik bir çalışma yapılması amacıyla hazırlanmıştır. Tezin hazırlanmasında AB düzenlemeleri, kaynak rehberler, veri koruma otoriteleri kararları, mobil sektöre ilişkin çevirimiçi kaynaklar, yüksek lisans tezleri ile makalelerden yararlanılmıştır.

Yukarıda da izah edildiği üzere kişisel verilerin hukuk düzenlemeleri koruması altında işlenmesi gerekmektedir. Öte yandan değişen hukuk kurallarının sanayi devriminden bu yana faaliyet gösteren işletmeler ve şirketler bakımından ezber bozduğu da muhakkaktır. Hukuk düzeni, amacı gereği getirdiği kurallara uyulmamasını belirli yaptırımlara ve cezalara bağlamıştır. Nitekim kişisel verilerin korunması mevzuatına aykırılık nedeniyle veri sorumlularına uygulanan yüksek rakamlarda para cezaları dikkat çekmekte ve bu konuda zorunlu bir farkındalık yaratmaktadır. Ancak, hukuki düzenlemeler ve ağır yaptırımlara rağmen, kişisel verinin farklı hukuki kurallara tabi coğrafyalara anlık olarak ulaştığı ve muhtelif ülkelerde yer alan sistemlerde saklanabildiği çağımızda, bu

[1] Furkan Güven Taştan, Türk Sözleşme Hukuku'nda Kişisel Verilerin Korunması, Onikilevha Yay, İstanbul, Temmuz 2017, s.1, Dünya Ekonomik Forumu'nun 2011 yılında düzenlediği raporda da verinin ekonominin yeni ham maddesi olduğu tespitinde bulunulmuştur.

alanın hukuk kuralları ile eksiksiz düzenlenebileceği ve kontrol edilebileceği beklentisi oldukça tartışmaya açık olacaktır.

BİRİNCİ BÖLÜM

MOBİL UYGULAMA KAVRAMI VE UYGULAMA ALANI

1.1. TANIMI

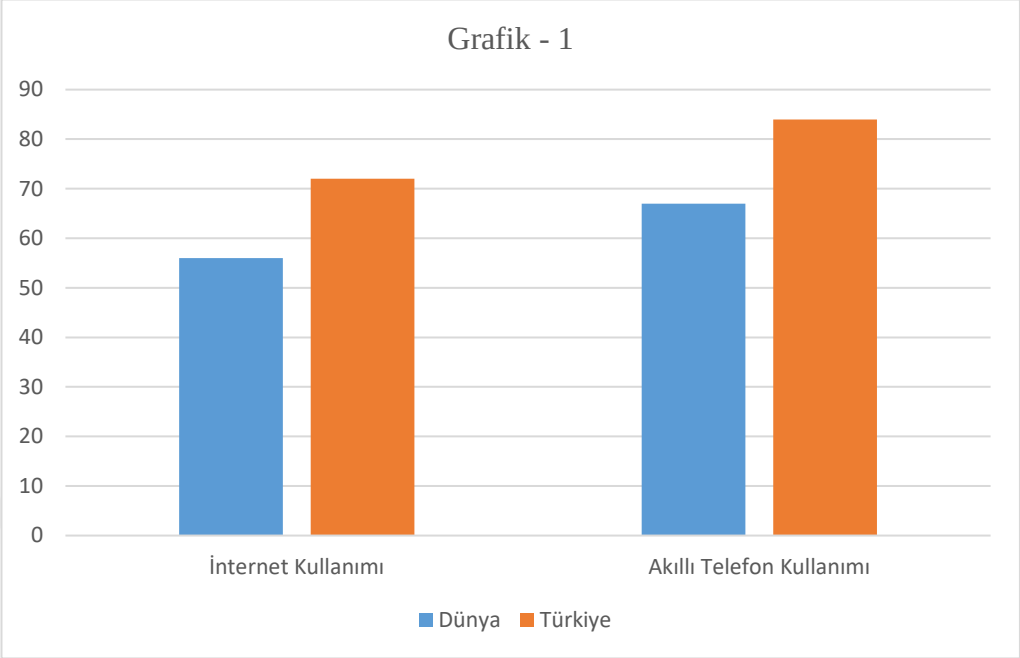
Mobil uygulama, akıllı telefon, tablet bilgisayar, akıllı ev, internet bağlantılı televizyon, giyilebilir teknoloji, gibi akıllı cihazlarda kullanılmak üzere belirli bir amaç için özel olarak kodlanarak hazırlanan yazılımlara verilen tanımdır. Teknolojik gelişmelerin ilerlemesi ile birlikte mobil cihazlar, asli fonksiyonları olan ses ve mesaj iletimi dışında mobil uygulamalar aracılığıyla bir çok farklı faaliyeti de yerine getirmeye başlamışlardır.

Uygulamalar ve donanıma ilişkin buluşların yaygınlaşması ile birlikte akıllı telefonlar sadece e-posta ve internet sitesi taraması için değil, dahili sensörleri ile birlikte bir çok farklı işlevi birarada yerine getirmeye başlamıştır[2]. Bu durum, ticari firmalar ile müşteriler arasındaki ilişkiyi de farklılaştırarak uygulama gelirlerini geçen senelere oranlara %15,5 arttırmıştır.

Aşağıdaki grafikte de görüleceği üzere Türkiye'deki internet kullanım oranı ile dünyadaki ortalama internet kullanım oranı arasında yüksek bir fark bulunmaktadır. Dünyada internet kullanım oranı %56 iken ülkemizde bu oran %72'dir. Akıllı telefon kullanımında da yerel nüfusun %84'ü akıllı telefon kullanırken bu oran dünyada %67'dir[3].

[2] Arthur, Charles, Dijital Savaşlar Apple, Google, Microsoft ve İnternet Savaşı, Türkiye İş Bankası, Kültür Yayınları, I. Basım Temmuz 2017, İstanbul, s. 250

[3] Uyar, Ahmet, Tüketicilerin Mobil Uygulamalara İlişkin Algılarının Teknoloji Kabul Modeli İle Değerlendirilmesi, İşletme Araştırmaları Dergisi Journal Of Busıness Research-Turk 2019, 11(1), 687-705, s.1, webrazzi.com, https://www.isarder.org/2019/vol.11_issue.1_article53_full_text.pdf, Erişim Tarihi : 10.10.2019



Şekil 1.1. 2019 Yılı Dünyada ve Türkiye'de İnternet ve Akıllı Telefon Kullanımı

Akıllı telefon kullanıcıların %70'i mobil uygulamaları video izlemek, %59'u gündemi takip etmek, %53'ü sosyal medya kullanmak, %36'sı ise müzik dinlemek için kullanmaktadırlar. Farklılıklar olmakla birlikte uygulamanın mobil cihaz içinde kullanımı için gerekli olan bileşenlere erişim için yükleme öncesi veya yükleme sırasında uygulamayı indiren kullanıcıdan belirli bir takım bilgi taleplerinde bulunulmaktadır. Örneğin kullanıcının fotoğraf ve konum bilgisini paylaşmayı amaçlayan bir sosyal medya uygulamasında kullanıcının fotoğraf albümüne, kamerasına ve konum bilgisine erişim için talepte bulunulması olağandır. Bu durumda onayın kullanıcıdan uygulama, cihaza indirilmeden önce talep edilmesi gereklidir. Ancak uygulamanın kullanım amacı ile ilgili olmayan mobil cihaz bileşenlerine erişim için talepte bulunulması halinde kullanıcının bilgilerinin amaç dışında toplandığına ilişkin kafalarda soru işareti uyanacaktır. Bu durumda veri sorumlusu veya veri işleyen tarafından mobil uygulama kurgulanırken veya daha sonrasında bilinçli bir kullanıcının bilgi talebine onay vermeme hakkının kolay ve rahat bir şekilde kullanacağı bir yapının oluşturulmuş olması ilgili mevzuat ve sektörel düzenlemeler açısıdan önem taşımaktadır.

1.2. MOBİL UYGULAMA SEKTÖRÜNDE YER ALAN AKTÖRLER VE FONKSİYONLARI

Mobil uygulama kullanımı ile ortaya çıkan veriler, veri eşleştirme, veri madenciliği gibi tekniklerle analiz edilerek farklı iş modellerine dönüştürülmektedir. Dolayısıyla bu alanda toplanan ve işlenen veriler üzerinden çeşitli pazarlama stratejileri ile yeni iş modelleri oluşturulduğu gibi bir çok farklı organizasyonda da verinin farklı kullanım amaçlarına hizmet ettiği yeni alanlar ortaya çıkmaktadır.

Mobil uygulamaların kolaylıkla erişilebilir olması, son kullanıcılar tarafından tercih sebebi oluştururken, büyük kitlelere kısa sürede ulaşabilme, bireysel ihtiyaç ve ilgi alanlarına yönelik doğrudan pazarlama faaliyetlerinin çok daha etkin uygulanabilmesi vs. nedenlerle de uygulamalar mobil uygulama sektörünün aktörleri açısından vazgeçilmez bir öneme ulaşmıştır. Uygulamaların sosyal medya, e-ticaret, eğlence, spor, sağlık, beslenme, bankacılık, turizm, seyehat, eğitim, kültür gibi çeşitli sektörlerde kullanılması ile tüm bu sektörlerdeki verilerden oluşan büyük veri üzerinden kullanıcı eğilimleri beslenmesi, tercihleri, alışkanlıkları vb. üzerinden profilleme yaparak kişiye özel hizmet ve ürünlerin sunulması sektörü son yıllarda ticari açıdan çok daha önemli hale getirmiştir. Bu faaliyetler çerçevesinde kişisel veri paylaşım düzeyi ve kazandığı ekonomik önem, bu konuda özel düzenlemelerin yapılmasını zorunlu kılmaktadır. Mobil uygulamalarda kişisel verilerin korunmasına ilişkin düzenlemeler çerçevesinde kimlerin hangi yükümlülükleri nasıl yerine getirileceğinin belirlenmesi bakımından öncelikle bu sektörde yer alan aktörlerin tespit edilmesi gerekmektedir. Bu noktada mobil uygulama sektöründe yer alan aktörleri aşağıdaki şekilde sıralayabiliriz:

1. Mobil uygulama geliştiriciler
2. İşletim sistemi ve cihaz üreticileri
3. Mobil uygulama mağazaları
4. Üçüncü kişi aktörler
5. Mobil uygulama kullanıcıları

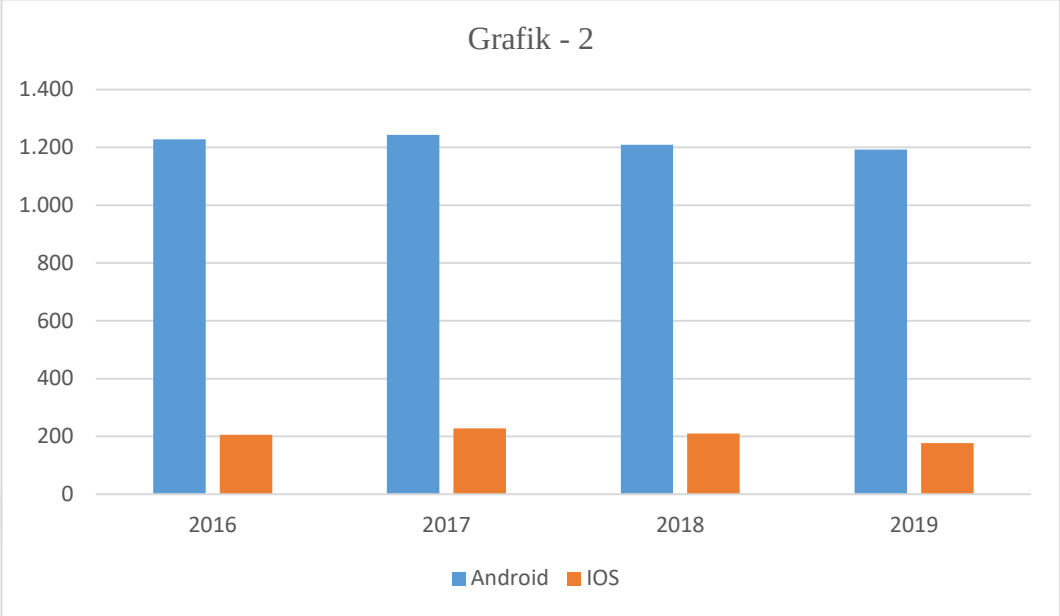
1.2.1. Mobil Uygulama Geliştiriciler

Mobil uygulama geliştiriciler, mobil cihazlar için uygulama yazılımını hazırlayıp geliştiren, üretilen uygulamanın test edilmesi, geliştirme sonrasında da uygulama satıcısı ve son kullanıcıya destek olan kişilerdir. Uygulamaların mobil cihazlara erişimi, aplikasyon program ara yüzü adı verilen işletim sistemi aracılığı mümkün olmaktadır. Ara yüz yazılımı ile mobil cihazda yer alan telefon rehber bilgisi, video, fotoğraf albümleri, mikrofon, kamera, SMS mesajları, e-posta mesajları gibi cihazın özelliklerine erişim sağlanarak cihazda yer alan sensörlere ve bilgilere ulaşılmaktadır. Mobil uygulama geliştiriciler, arayüz ile hangi uygulamada hangi kişisel verilere ulaşılacağı ve hangi kişisel verilerin işleneceği konusunda da karar veren kişiler olmaları itibariyle kişisel verilerin korunması hukuku açısından önemli aktörlerdendir.

1.2.2. İşletim Sistemi ve Cihaz Üreticileri

Taşınabilir veya masaüstü cihazlarında yer alan donanımların ve aygıtların amacına uygun bir şekilde çalışmasını sağlayan yazılımlara işletim sistemi denilmektedir. İşletim sistemi, mobil cihazlarda uygulamaların kullanılması için aracı görevi yerine getirmektedir.

Dünyada en yaygın mobil işletim sisteminden biri Google'ın sahibi olduğu ve geliştirmelerini yaptığı, en fazla Samsung, Sony ve HTC markalarında kullanılan Android işletim sistemi diğeri ise sadece Apple marka telefonlarda kullanılan IOS işletim sistemidir. Diğer işletim sistemlerinin tercih oranı ise çok düşük seviyededir.



Şekil 1.2. Dünyada Android ve IOS Kullanımı[4]

Mobil cihazlar satın alındıklarında kullanıcı tarafından yüklenmese dahi bazı standart uygulamalar yüklü halde satılmaktadır. Cihaz açılırken kayıt olunan bilgiler, cihaz tarafından otomatik olarak elde edilen bilgiler, kullanıcı uygulama indirdiğinde işletim sistemi veya cihaz tarafından işlenen bilgiler, cihaza uzaktan erişmek için elde edilen bilgiler ile cihazda yer alan bilgilerin yedeklenmesi için işlenen bilgiler, işletim sistemi ve cihaz üreticisi tarafından işlenen bilgilere örnek olarak verilebilir.

Madde 29 Çalışma Grubu, 02/2013 sayılı görüşünde, işletim sistemi ve cihaz üreticilerinin sorumluluklarına değinerek bu üreticilerin aynı zamanda uygulamalardaki kişisel veriyi işlemeye yarayan ara yüz yazılımı için de sorumlu olduklarını belirtmiştir[5]. Uygulama geliştirici, bu ara yüz yazılımına işletim sistemi ve cihaz üreticileri aracılığı ile erişim sağlamaktadırlar[6]. Bu durumda işletim

[4]https://www.statista.com/statistics/309448/global-smartphone-shipments-forecast-operating-system/ Erişim Tarihi :09.03.2020

[5] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.21

[6] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.4

sistemi ve cihaz üreticileri, hangi durumda ve ne ölçüde kişisel veriye erişime izin verileceğini belirlemek ve uygulama geliştiricinin sadece uygulamanın çalışması için gereken en az bilgiye erişimini sağlayacak şekilde bir erişim belirlemek zorundadırlar[7]. Ayrıca ilgili üreticiler, uygulama kullanımı için izin verilen erişimin basit ve etkili şekilde geri alınmasını sağlayacak bir yapının da uygulamada mevcut olduğundan emin olmalıdırlar[8]. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ("GVKT") 25. maddesinde düzenlenen "tasarımla veri koruma" [9] (privacy by design) ve "varsayılan ayarlarla veri koruma" [10] (privacy by default) ilkeleri cihaz üreticileri veya uygulama geliştiricilere daha tasarımın ilk başında veri korumasının cihaza veya uygulamaya entegre edilmesini veya varsayılan ayarlar bakımdan kişisel verilerinin korunması için gerekli olan gizlilik ayarlarının kullanıcının herhangi bir eylemde bulunmasına gerek olmadan varsayılan olarak entegre edilmesini öngörmektedir.

1.2.3. Mobil Uygulama Mağazaları

Mobil uygulamalar, satın alınan cihaz içerisinde hazır bir şekilde kullanıcıya sunulduğu gibi çeşitli amaç ve istekler doğrultusunda cihaz uygulama mağazalarından satın alınarak veya ücretsiz olarak mobil cihaza indirilerek de kullanılmaktadır. Uygulama mağazalarının sektöre girişi ilk kez 2008 yılında olmuştur[11]. Aradan geçen 11 yıldan bu yana mağazalardan uygulama indirme sayısı her geçen gün artış göstermiştir. Nitekim, mobil uygulama analiz firması olan Sensor Tower internet sitesinde yayımladığı raporda; mobil uygulama mağazalarının 2019 yılının ilk yarısında 39.7 milyar kar elde ettiğini duyurmuştur[12].

---

[7] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.11

[8] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.11

[9]Tasarımla Veri Koruma kavramına göre ürün, daha tasarım aşamasındayken veri gizliliğini koruyacak şekilde üretilmelidir. Bu kavramla birlikte kuruluşların verilerin korunmasına ilişkin teknik ve idari tedbirlerin teknolojik tasarım özelliklerine, iş politikalarına ve fiziki altyapıya entegre edilmesi ifade edilir. Taştan, s.18

[10]Varsayılan ayarlarla veri koruma ise, kullanıcının başkaca bir şey yapmasına gerek kalmaksızın kişisel verilerinin korunmasını ifade eden bir kavramdır. Bu prensip ile veri sorumluları her bir amaç için varsayılan şekilde sadece gerekli minimum veriyi işlemektedirler. Taştan, s.19

[11]Uyar, s.2

[12]https://sensortower.com/blog/ Erişim Tarihi :28.10.2019

2019 yılının ikinci yarısı itibariyle uygulama mağazalarından indirilen uygulama sayısı, Google Play mağazasında 2.46 milyon, Apple mağazasında ise 1.96 milyon olarak ölçülmüştür[13].

Uygulama satın alımları, ön ödeme şeklinde olabildiği gibi uygulama indirme sonrası alım şeklinde de olabilmektedir. Bu durumda kullanıcılardan en az ad, soyad bilgisi ile ödemeye ilişkin bilgiler elde edilmektedir. Bu kişiye özgü bilgiler daha sonra alım işlemi ve kullanıcı davranışı ile birleşerek cihaz tarafından okunabilecek hale gelebilmektedir. Mobil uygulama satıcıları, son kullanıcının uygulama indirme bilgisi, kullanma geçmişi veya benzer bilgileri de uygulama geliştiricilerine ilettiklerinde aynı şekilde veri sorumlusu olarak sorumlu tutulmaktadırlar. Mobil uygulama satıcılarının gizliliğe ilişkin kuralları mutlaka gizlilik politikalarında belirtmeleri gerekmektedir. Madde 29 Çalışma Grubu, uygulama satıcılarına, işletim sistemi üreticisi ile işbirliği içinde olarak, uygulama geliştiricileri, uygulama içerisinde son kullanıcıyı bilgilendirmeye yönelik uygulama tarafından belli bilgilere erişimi temsil eden semboller sunmaları ve bunları uygulama mağazası kataloğunda göze çarpacak şekilde görüntülenmesini sağlayacak alt yapıyı kurmaları konusunda kurallar belirlemelerini tavsiye etmektedir[14]. Uygulama mağazalarının uygulama geliştiricilere yönelik hazırladıkları kural ve politikalarda teknik ve hukuki gereklilikler belirtilmiş olup bu kriterleri kaşılamayan uygulamalar mağazaya kabul edilmemektedir.

1.2.4. Üçüncü Kişi Aktörler

Mobil uygulamanın önemli aktörlerinden biri de üçüncü kişi aktörlerdir. Bu üçüncü kişi aktörleri genellikle reklam verenler, istatistik veri analistleri ve telekomünikasyon servis sağlayıcıları oluştururlar. Özellikle birçok ücretsiz uygulama, reklam geliri ile kar elde etmektedir. Bu reklamlar ise genellikle çerezler veya başkaca benzeri yazılımlar vasıtasıyla kullanıcı davranışları doğrultusunda

[13]https: //www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ Erişim Tarihi 30.09.2019

[14]Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.12

kişiselleştirilmektedir. Reklamlar, uygulama içinde banner konulması suretiyle olabileceği gibi uygulama dışında da bir simge yardımı ile mobil masaüstüne yerleştirilebilmektedir. Uygulamalar için reklam faaliyetleri genellikle reklam ağları ve benzer yapılarca yerine getirilmektedir.

Üçüncü kişi aktörlere başka bir örnek de istatistik veri analistleri ve telekomünikasyon servis sağlayıcıları verilebilir. İstatistik veri analistleri hangi uygulamanın ne kadar indirildiği, popülerliği ve kullanılabilirliğine ilişkin verileri işlemektedir. Bu veriler gerçek bir kişi ile bağdaştırılmadığı ölçüde kişisel veri kapsamına girmemektedirler.

Şunu da önemle belirtmek gerekir ki; akıllı mobil cihazlarda kullanıcıların kişisel verilerinin işlenmesini kontrol ettikleri yazılımların yüklenmesi, masaüstü bilişim sistemlerine nazaran daha kısıtlı olmaktadır. Http çerezlerinin kullanımına alternatif olarak üçüncü kişi aktörler sıklıkla özel belirleyiciler[15] ile hedefleme yaparak kişileri tek tek veya grup olarak ayırmakta ve onlara reklam hizmeti sunmaktadır. Bu özel belirleyiciler[16], cihazın ve yazılımın kullanılması açısından zorunlu olduklarından kullanıcılar tarafından silinmesi veya değiştirilmesi mümkün olmamaktadır. Bu sebeple de üçüncü kişi aktörler son kullanıcının kontrolü olmaksızın yüklü bir miktar kişisel veriyi işleme potansiyeline sahip olduklarından bu noktada bu kişilerinin veri işlemesine yönelik sınırlarının özellikle iyi çizilmesi gerektiği açıktır.

1.2.5. Mobil Uygulama Kullanıcıları

Mobil uygulama kullanıcıları da mobil cihazları aracılığı ile gerek kendilerine ait gerekse telefon rehberine kayıtlı üçüncü kişilere ait ad, soyad, iletişim bilgisi veya fotoğraf gibi kişisel verileri saklayıp işlemektedirler. Mobil uygulama kullanıcılarının da verilerin korunması bakımından kendilerine düşen görevi yerine getirmeleri önemlidir. Kullanıcılar, cihazlarında ve mobil uygulamalarda yer alan

[15]Unique Identifier olarak tanımlanan bilgisayar yazılımlarında belirleyici olarak kullanılan bir referans numarasıdır.
[16]İşletim sistemi tarafından eklenen IMEI, IMSI MSISDN gibi ve spesifik özel belirleyiciler.

gizlilik ile ilgili politikaları inceleyerek, gizlilik tercihlerini ve ayarların gereğini yapmalı, indirdikleri uygulamaların ayarlarını kontrol ederek kendilerine düşen sorumluluğu yerine getirmelilerdir. Öte yandan 6698 Sayılı Kanun kapsamında, kullanıcıların mobil cihazlarında kendileri veya aynı konutta yaşayan aile üyeleri ile ilgili veri işleme faaliyetlerinin tamamen şahsi kullanım ve kişisel amaçlarla yapılması halinde bu işlemler yönünden kişisel verilerin korunmasına ilişkin hukuki düzenlemeler uygulama alanı bulmayacaktır[17]. Ancak kişinin hane halkı faaliyeti kapsamında kendisi veya aile üyeleri ile ilgili işlediği veriler kişisel ve faaliyet kapsamını aşıp 3. taraf kişilere ait verilere ulaşıyorsa bu durumda istisnai durum söz konusu olmayacaktır[18]. Avrupa Adalet Divanı'nın 11 Aralık 2014 tarihli kararında hırsızlıktan korunmak amacıyla evin girişine konulan kamera ile elde edilen verilerin tamamen kişisel faaliyet ve hane halkı faaliyeti kapsamında değerlendirilmeyeceğine hükmedilmiştir[19].

1.3. ORGANİZASYONLAR AÇISINDAN MOBİL UYGULAMALAR

1.3.1. Mobil Uygulamalarda Sektörel Ayrımlar

Masaüstü veya dizüstü bilgisayarlar, bilgi güvenliği açısından mobil cihaza göre daha düşük bir koruma sağladıklarından bir çok kişi, tercihini mobil cihazlardan yana yapmaktadır. Mobil cihazların yaygın bir şekilde kullanımı, kullanıcılara zaman ve mekan sınırı olmaksızın doğrudan ulaşılabilme imkanı sağlaması, uygulama kullanıcılarının bilgilerinin daha doğrulanabilir olması gibi çeşitli sebeplerle sektördeki bir çok kuruluş, kar amacı olsun olmasın kendilerine ait bir mobil uygulamaya sahip olmayı tercih etmektedirler. Bu noktada hizmetin

[17]6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un İstisnalar başlıklı 28. Maddesinin 1. Fıkrasına göre, üçüncü kişilerle paylaşılmadığı ve veri güvenliğine ilişkin yükümlülüklere uyulduğu takdirde kişisel verilerin gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi durumunda kanun hükümlerinin uygulanmayacağı düzenlenmiştir.

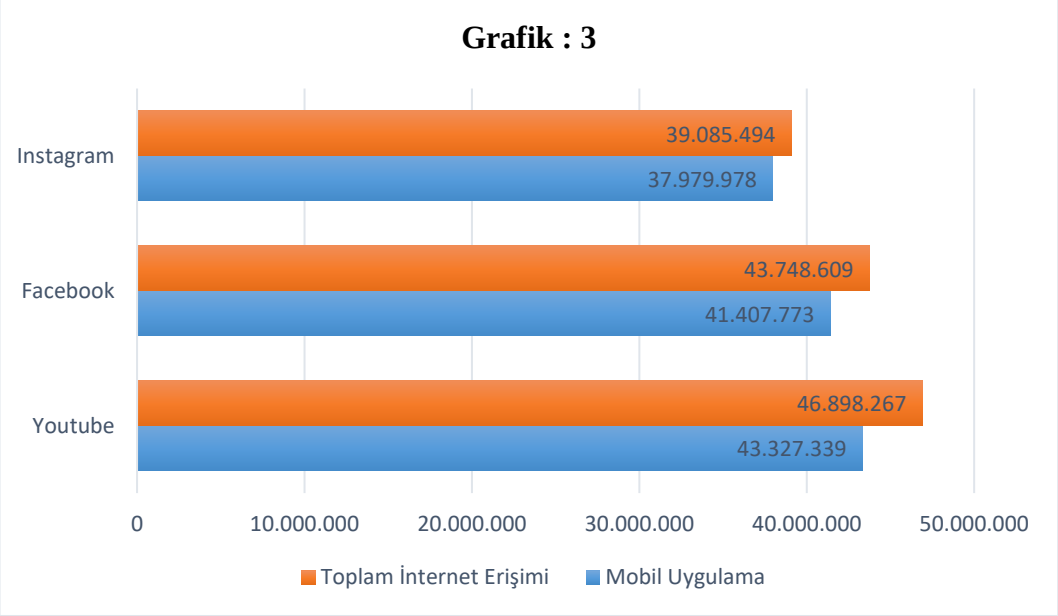
[18]Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Oniki Levha Yay, İstanbul, Ocak 2018, s.26

[19]Sezen Kama Işık, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Oniki Levha Yay, İstanbul, Ocak 2020, s.137

kapsamına bağlı olarak işlenen verilerin çeşitliliği ve ne ölçüde işlendiği de değişmektedir.

2019 yılının ilk çeyreğinde dünyada en çok indirilen mobil uygulamalar, mağazalara göre değişiklik göstermekle birlikte Apple Store'a bakılacak olursa TikTok, YouTube, Instagram, WhatsApp, Messenger, Facebook olmuştur[20]. Bu sonuçlar, mobil kullanıcıların daha çok sosyal medya ve eğlence amaçlı uygulamalara öncelik verdiklerini göstermektedir.

Mobil uygulamalar aşağıdaki grafikte görüldüğü üzere toplam internet kullanımının da büyük bir kısmını oluşturmaktadır.



Şekil 1.3. Türkiye'de Mobil Uygulama Kullanıca Sayısı[21]

1.3.1.1. Kamu Hizmeti Sağlayan Mobil Uygulamalar

Kamu hizmetleri, uzun bir süredir e-devlet adı altında elektronik ortamda da verilmeye başlamıştır. Mobil internet kullanımının artışı ile birlikte e-devlet hizmetlerinin çoğu mobil uygulamalarla da yapılacak şekilde geliştirilmiştir.

[20] https://sensortower.com/blog/top-apps-worldwide-q1-2019-downloads Erişim Tarihi :09.03.2020
[21] https://webrazzi.com/2019/10/24/turkiye-mobil-uygulama-kullanici-sayisi-gemius/ Erişim Tarihi :09.03.2020

Nitekim 2016-2019 Ulusal e-devlet Stratejisi Eylem Planında da, mevcut ve yeni geliştirilecek e-devlet hizmetlerinin öncelikli olarak mobil platformlarla uyumluluğunun sağlanması ve sosyal medyanın etkin kullanılması gerekliliği yer almaktadır[22]. Gelişmiş ülkelerde e-devlete ilişkin mobil uygulamalar, etkin ve yaygın biçimde kullanılırken gelişmekte olan ülkelerde bu oran daha düşük seviyede olmaktadır[23].

Öte yandan kamu ile etkileşimin mobil cihazlar aracılığı ile yerine getirilmesi, gerek kamu açısından gerekse vatandaş açısından avantajlı olduğu gibi dezavantajlı da olabilmektedir. Kamu hizmetlerinin elektronik alana yayılması ile bürokrasi azaltılmış, minumum belge ile zaman ve iş gücünden de tasarruf edilmiştir. Ancak ortaya çıkan her yeni gelişmede olduğu gibi mobil e-devlet hizmeti de, kişilerin köklü alışkanlıkların değiştirilmesi, güvenli alt yapı oluşturulması ve bu alt yapının korunmasına ilişkin önlemlerin alınması gibi birçok zorluk ve riski de beraberinde getirmektedir. Uygulama geliştiricisinin kamu kurumu olduğu birçok mobil uygulamaya, uygulama mağazalarından kolaylıkla erişilebilmektedir. Adalet Bakanlığı tarafından hizmete sunulan UYAP mobil mahkeme/adalet servisi, Gelir İdaresi Başkanlığı tarafından hizmete sunulan GIB mobil vergi servisi, Sağlık Bakanlığı tarafından hizmete sunulan e-nabız, İstanbul Büyükşehir Belediyesi tarafından hizmete sunulan IBB İstanbul, IBB Beyaz Masa, IBB trafik vb. gibi uygulamalar örnek verilebilir. Bu uygulamalar ile vatandaşlar herhangi bir kamu

[22]T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı, 2016, s.48, http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf Erişim Tarihi: 09.03.2020

[23]Gonca Telli Yamamoto, Mobil Yaşam ve Uygulamaları, İstanbul, 2011, https://s3.amazonaws.com/academia.edu.documents/7559182/Mobil_Yasam_ve_Uygulamalari_eBook.pdf?response-content-disposition=inline%3B%20filename%3DMobil_Yasam_ve_Uygulamalari_eBook.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191105%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191105T155638Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=1148d2bb5d6291e64f15d48476af6f6afffcb203c914c2911f50d4ea6ffeece1 s.53, Erişim Tarihi : 10.10.2019

kurumuna gitmek zorunda olmadan mobil cihazları aracılığı ile işlem yapabilmektedirler[24].

1.3.1.2. Kar Amacı Gütmeyen Mobil Uygulamalar

Kar amacı gütmeyen mobil uygulamalara, Bağımsız Sivil Toplum Örgütleri tarafından hizmete sunulan mobil uygulamalar örnek olarak verilebilir. Bu örgütler kuruluş amaçlarını gerçekleştirmek adına farklı kitlelere ulaşmak ve farkındalık yaratarak bilinirliklerini arttırmak için çalışmaktadırlar. Bu noktada mobil uygulamalar ile amaçlarına daha kolay ve hızlı bir şekilde ulaşmaktadırlar. Öte yandan örgüt üyesi olsun veya olmasın kişiler, mobil uygulamaları aracılığı ile organizasyonun faaliyetleri hakkında bilgi almakta, bağış yapmakta ve etkinlik tarihlerine ulaşmaktadırlar.

1.3.1.3. Eğitim Amaçlı Kullanılan Mobil Uygulamalar

Ülkemizdeki okullarda da yürütülmeye başlanan akıllı tahta projeleri kapsamında her öğrenciye bir tablet dağıtılması amaçlanmaktadır. Bu tablette yer alan verilerin ölçümü yapıldığında öğrencilerin gelişiminin izlenmesi ile eğitim sistemine ilişkin verilerle analizler yapılarak eğitim sisteminin geliştirilmesi yönünde daha somut adımlar atılabilecektir.

Onun dışında bilim, teknoloji, yemek pişirme, yabancı dil eğitimi, işletme, pazarlama, sağlık, yoga , müzik, fotoğrafçılık gibi binlerce kursa ücretli veya ücretsiz erişim sağlayan mobil uygulamalar da giderek popüler hale gelmektedir.

1.3.1.4. Eğlence ve İletişim Amaçlı Kullanılan Mobil Uygulamalar

Mobil uygulamalarda eğlence ve iletişim denince ilk akla gelenler sosyal medya ve sohbet uygulamaları olmaktadır. Sosyal medya uygulamalarının ücretsiz kurulumları olduğu gibi ücret karşılığı sağladıkları hizmetler de bulunmaktadır. Öte yandan en popüler sohbet uygulaması olan WhatsApp, tamamen ücretsiz olduğu ve

[24]Yamamoto, s.55

kullanıcılardan hiçbir ücret talep etmediği halde şirket, 2014 yılında Facebook şirketi tarafından 19 milyar dolar karşılığında satın alınmıştır[25]. Bu meblağın, o tarih için Türkiye'nin en büyük 20 şirketinin borsa değerinden bile daha fazla olduğu yerel basında geniş yankı bulmuştur[26]. Uygulama, hiçbir kullanıcısından ücret almadığı gibi her hangi bir reklam gelirine de sahip değildi. Buna rağmen şirketi bu kadar değerli yapan şüphesiz ki o dönem aylık aktif 1 milyar kullanıcının olması ve bu kullanıcılarının verilerinin kendisini satın alacak şirkete aktarılacak olmasıydı. Bu olay, kişisel verinin ekonomik olarak ne kadar değerli olduğunu ve verinin alınıp satılan bir varlık olduğunu gösteren çarpıcı bir örnektir.

Diğer popüler sosyal medya uygulamalarında kullanıcılar, oluşturdukları profil ile fotoğraf, video paylaşmakta veya fikirlerini, düşüncelerini dile getirmektedir. Neredeyse tüm kamu ve özel kurumları hatta siyasetçiler, ünlüler kendilerine ait sosyal medya hesaplarında paylaşım yaparak interaktif olarak diğer kullanıcılarla iletişime geçmektedirler. Hal böyle olunca da sosyal medyanın gücü ile yeni meslekler, farklı reklam modelleri ortaya çıkması kaçınılmaz olmuştur. Sosyal medyanın lider şirketleri ise daha fazla kullanıcıyı kendilerine çekmek adına sürekli yenilikler ortaya çıkarmakta ve insan psikolojisine etki ederek daha fazla kullanıcıya ulaşacak şekilde geliştirmeler yapmaktadırlar. Kullanıcıların alışkanlıkları, beğenileri, paylaştığı konum bilgileri, takip ettikleri kişiler, takipçilerinin sayısı vb. bir çok verinin toplanması ve veri madenciliği gibi teknikler ile başta pazarlama ve reklam sektörü olmak üzere bir çok alan da cazip hale gelmiş bir anlamda sosyal medyadan fayda sağlayanlar sadece şirketler olmakla kalmamış kullanıcılar da kendi yaratıcılıklarını sergileyebilecekleri hatta bundan gelir elde edebilecekleri masrafsız bir alana kavuşmuşlardır.

[25]https://pando.com/2014/02/24/whatsapp-bought-for-19-billion-what-do-its-employees-get, Erişim Tarihi : 10.10.2019

[26]https://www.cnnturk.com/fotogaleri/ekonomi/sirketler/whatsapp-turkiyenin-20-devini-gecti, Erişim Tarihi : 10.10.2019

1.3.1.5. Sağlık Hizmetlerine İlişkin Mobil Uygulamalar

Mobil sağlık uygulamaları, sağlık hizmeti sunan kişiler tarafından hastanın durumunu takip etmek amacıyla kullanıldığı gibi kişiler tarafından da sağlık verilerini yönetmek ve takip etmek amacıyla da kullanılmaktadır[27]. Sağlık ile ilgili veriler, hukuka aykırı olarak işlendiğinde diğer verilere nazaran daha ciddi zararlar doğurması bakımından özel bir korumaya muhtaçtır. Öte yandan sağlık ile ilgili gelişmelerin, araştırmaların bir çoğu veriler üzerinden olduğundan bu alandaki verinin işlenmesi toplumsal açıdan da önemlidir. Özellikle istatistiksel veriler ve veya belli verilerin bir araya getirilmesi ile okunan bazı durumlar, yeni tedavilerin veya tıp alanında yeniliklerin ortaya çıkmasına zemin hazırladığı gibi erken teşhis sağlaması bakımından da hayat kurtarmaktadır.

Sağlıkla ilgili çeşitli mobil uygulamalar mevcut olup mobil cihazlar satın alındığında otomatik yüklü uygulamalar olduğu gibi uygulama mağazalarından indirilen uygulamalar da mevcuttur. Kadınların özel dönemlerini takip edebilecekleri uygulamalar yaygın olarak kullanılmaktadır. Kişiye özel takvim yöntemi ile kişi açısından adet düzeni veya düzensizliğini kontrol edebildiği, doğurganlık dönemlerinin de yer aldığı uygulama bir çeşit doğum kontrol yöntemi olarak işlevini yerine getirdiği gibi gebe kalmak isteyenler için de kolaylık sağlamaktadır.

1.3.1.6. Gözetleme ve İzleme Amaçlı Kullanılan Casus Mobil Uygulamalar

Her ne kadar kulağa ürkütücü de gelse gözetleme ve izleme amaçlı kullanılan mobil uygulamalar bir noktada önemli bir işlevi de yerine getirmektedir. Bu uygulamalar, özellikle korunmaya muhtaç olan çocuklar ve belirli bir yaşa gelmiş veya hafıza sorunu yaşayan yaşlıların takibi bakımından son derece hayati olmaktadır. IOS işletim sistemi kullanan cihazlarda otomatik yüklü olarak gelen "Arkadaş Bul" uygulaması ile takip etmek istediğiniz telefon numarasına istek göndererek

[27]Büşra Kopmaz, Ali Arslanoğlu, Mobil Sağlık ve Akıllı Sağlık Uygulamaları, Sağlık Akademisyenleri Dergisi, 2018, s.253
https://dergipark.org.tr/en/download/article-file/633686, Erişim Tarihi : 10.10.2019

uygulamayı aktif hale getirebilmek mümkün olmaktadır. Her iki tarafın da kabulüne ihtiyaç duyan takip mobil uygulamaları kabul edilebilir olmakla birlikte yüklendiği kişinin telefonunda görünmeyen ve kişinin haberi olmaksızın başka biri tarafından izlenmesine imkan sağlayan mobil uygulamalar açısından durum aynı cihette olmayacaktır. Piyasada yer alan bu tarz ücretli uygulamalar yüklendiği cihazın konumu, gezdiği internet sitesi kayıtları ve arama kayıtları, mesajlaşmaları, tuş hafızası, sosyal medya yazışmaları gibi herşeyi takip edebildiği gibi takvim görüntüleme, ortam dinleme, ses kaydı dinleme, kullanılmasının istenilmediği internet sitesi ve uygulamaları da engelleyebilme özellikleri taşımaktadır. Uygulamanın, sadece reşit olmayan çocukları için ebeveynler ve çalışanlarına bildirilmiş olması şartıyla işverenlerce kullanılabileceği, aksi kullanımın yasalara aykırı olabileceği belirtilmiş olmakla birlikte alıcıların bu uygulamayı farklı amaçla kullanmasına bir engel bulunmamasının önemli bir gizlilik ihlali olduğu düşünülmektedir. Google Play uygulama geliştiricilere yönelik internet sitesinde hazırladığı politikasında, bu tarz casus uygulamaların mağazalarında yer almasının yasak olduğunu sadece belli kriterleri sağlayan ebeveyn/aile amacı ile kullanılan uygulamalara izin verdiğini belitrmiştir[28].

1.3.1.7. E-Ticaret Hizmeti Sunan Mobil Uygulamalar

E-ticaretin online mağazalardaki satışın gider kalemlerini önemli ölçüde azalttığı, iş gücü maliyetlerini düşürdüğü ve birçok işletmenin daha fazla kar elde etmesini sağladığı açıktır. Bunun yanında mobil kullanımın sağladığı farklılıklar ve kolaylıklar düşünüldüğünde e-ticareti mobil uygulamalara taşımak çok daha etkili olmuştur. Günümüzde rekabetin artması ile birlikte tüketicilere en hızlı ve doğru şekilde ulaşmak ve mobil uygulamanın katkılarından faydalanmak amacıyla her ticari işletmenin bir mobil uygulaması olduğu gibi Trendyol gibi sadece mobil uygulama üzerinden alışveriş yapılmasını sağlayan online alışveriş ile kar elde eden mağazalar da mevcuttur. Online alışverişi özendirici, cezbedici seçeneklerin sunulması, mağazaların açılış kapanış saatinden bağımsız olarak alışveriş yapma

[28] https://play.google.com/intl/en-US/about/privacy-security-deception/malicious-behavior/ Erişim Tarihi : 09.03.2020

imkanının tanıması, kişinin favorilerine eklediği ürünleri indirime düştüğünde kendisine bildirilmesini istemesi, özellikle indirim zamanlarında kişilerin evinde oturduğu yerde istediği ürüne ulaşabildiği, ödeme sırası beklemediği ve sanal mağaza maliyetlerinin fiziki satış kanallarına nazaran daha az olmasının avantajını kullanarak aynı ürünleri tüketicilere daha düşük fiyatlarla sunabildiği düşünüldüğünde daha da tercih edilir olmaktadır.

1.4. KULLANICILAR AÇISINDAN MOBİL UYGULAMALAR

Mobil uygulama kullanımındaki en önemli aktörlerden biri süphesiz ki cihaz kullanıcılarıdır. Günümüz yaşantısının insanları yoğun ve zamanın kısıtlı kullanıldığı bir tempoya maruz bırakması, insanların maddi ve manevi ihtiyaçlarını yer ve zaman kavramı olmaksızın gidermesini sağlayan mobil uygulamalar, hayatın vazgeçilmez parçası haline getirmektedir. Masaüstü ve dizüstü bilgisayarlar yerini mobil cihazlara bırakırken kullanıcıların mobil uygulamadan beklentileri ülkeden ülkeye değişebildiği gibi yaşa ve kullanım alanına göre de değişim gösterebilmektedir. Örneğin bazı kullanıcılar, gizlilik ve mahremiyete önem verirken başka kullanıcılarda yeni teknolojileri kullanma merakı daha ağır basmaktadır.

Diğer yanda internetin ve mobil cihazların kullanımının sosyolojik açıdan bağımlılık yarattığına ilişkin bir çok çalışma mevcuttur. Özellikle gençlerde yaygın bir şekilde mobil iletişimle birlikte sürekli bir bağlantıda kalma hali ortaya çıkmıştır.[29] 2008 yılında "nomofobi", "no mobile phobia" olarak literatüre giren bu kavram ve "Fomo", "fear of missing out" kavramı da durumun sosyal ve psikolojik açıdan önemini vurgulamaktadır.

1.4.1. İşlevsellik ve Algılanan Yararlılık

Mobil uygulamaların kişilerin hayatına katkı sağladığı tartışmasızdır. Çocukların veya hafıza kaybı yaşayan yaşlıların konumlarının takip edilmesi, araç

[29]Castells, Manuel, İletişim Gücü, 1. Baskı, Nisan 2016, İstanbul Bilgi Üniversitesi Yayınları, Castells vd., 2006, s. 13

kullanıcılarının dünyanın her yerinde navigasyon hizmetini mobil cihazlarını kullanarak bulması ile kolayca ulaşım sağlaması, seyahat ve konaklama işlemleri için rezervasyon yapılması, bilet satın alınması, özellikle çalışan insanların mesai saatleri içinde yapması gereken işlemlerine sıra beklemeden veya herhangi bir yere gitmeden yapmasına olanak tanıyan mobil bankacılık veya e-devlet uygulamaları yabancı bir dili bilmesiniz dahi günlük ihitiyaçları karşılar düzeyde iletişim imkanı sağlayan tercüme uygulamaları, havaalanlarında kullanıcıyı uçağın kalkış yapacağı kapıya ve kapı değişikliklerini, seferin gecikmesi vs. konusunda ekranlara bakmadan bilgi sağlayan uygulamalar düşünüldüğünde kişinin bir mobil uygulamayı seçmesi ve tercih etmesinin en önemli sebebinin ilk önce işlevselliği olduğuna şüphe bulunmamaktadır.

1.4.2. Kullanım Kolaylığı

Mobil uygulamaların tercih edilebilirliğine yönelik yapılan çalışmalar, bu uygulamaların kullanıcıların kolayca anlayacağı ve kullanabileceği şekilde oluşturulmasının önemli bir etkisi olduğunu göstermiştir[30]. Çok fazla işlem yapmadan uygulamadan fayda sağlanması, özellikle üyelik ve satın alma süreçlerinde kolay ve anlaşılır bir arayüzün varlığı tercih edilmeyi doğrudan etkilemektedir. Özellikle test gruplarının oluşturulması ve bu gruplarda farklı yaş ve eğitim gruplarında insanlara yer verilmesi uygulamanın farklı kitlelelere hitap ettiğinin anlaşılması açısından önemli olacaktır[31].

1.4.3. Güvenlik ve Gizlilik

Gizlilik, kişilerin kendilerine ait bilgilerin dış dünyadaki kişiler tarafından bilinmemesi olarak tanımlanırken dijital anlamda gizlilik, bilgilerin yetkisiz kişiler tarafından erişilmesini engelleyici korumayı ifade etmektedir. Bilgi güvenliği ise gizlilikle birlikte daha geniş bir anlamı içine alarak, bilginin kullanımı, ifşa

[30]Yıldırır, S. C. & Burçin, K. (2019). Mobil uygulama kullanımının benimsenmesi: teknoloji kabul modeli ile bir çalışma. KAÜİİBFD, 10(19), 22-51, s.47 https://dergipark.org.tr/en/download/article-file/749534, Erişim Tarihi : 10.10.2019

[31]Brug, Anıl Altaş, e-ticaret Satışta Tsunami Etkisi , Haziran 2019, 6. Baskı, Mediacat Digitalage, İstanbul, s.176

edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan eylemlere yönelik koruma olarak tanımlanmaktadır[32].

Kullanıcılara cezbedici şeçenekler sunan mobil uygulamalar, kullanım sırasında cihazın rehberine, kamerasına, mikrofon bileşenlerine erişim izni istemekte ve cihaz bileşenlerinden topladıkları verileri çeşitli şekillerde kullanmaktadırlar. Google Android yazılımı tarafından 2014 yılında hazırlanan raporda, mobil cihazlarda güvenliği tehdit eden alanların başında, kişisel veriler, cihaz kimlik bilgisi ve erişilebilirliğin geldiği belirtilmiştir[33]. Kişisel veriler, kar amacı güden kuruluşlar tarafından karlılıklarını arttırmak, devlet kurumları tarafından ise hizmet kalitesini arttırmak amacı gibi çeşitli amaçlarla işlenebilmektedir[34]. Özel kuruluşlara ait uygulamaların dışında kamuya ait uygulamalarda toplanan verilerinin aleyhlerine kullanılabileceği korkusu bireyleri daha fazla tedirgin etmektedir.

Diğer yanda kredi kartı bilgilerinin kullanıldığı ve yüklü miktarda ödeme yapıldığı mobil uygulamalarda kullanıcıların bilgi güvenliği beklentisi daha yüksek düzeyde ve bilinçte olmaktadır. Bu açıdan bakıldığında mobil uygulama kullanımında marka güvenirliği önemli bir kriterdir. Örneğin okyanus aşırı uçuş için uçak bileti almak isteyen bir kullanıcı herhangi bir seyahat firması veya başka bir aracı firma uygulaması kullanarak ödeme yapmak yerine markasına inandığı güvenilirliği yüksek havayolu firmasına ait mobil uygulamadan ödeme yapmayı tercih edecektir. Mobil bankacılık uygulamalarında da sistemin ve hesaplarımızdaki işlemlerin güvenirliği ve hesap sahipleri dışında kimsenin erişip işlem yapamayacağı veya başka bir şekilde erişemeyeceği şekilde tedbirlerin alınması gerekmektedir.

[32]Henkoğlu, Türkay, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara, 2015, McCumber, 2005, s.36
[33]Pradeep Kumar, Analyzing Data Leakage Using Third Party Connections in Mobile Appliacations, Master of Engineering in Information Security, May, 2015, Thapar University, s. 6
[34]Henkoğlu, s.25

Bilgi güvenliği önlemleri dışında kullanıcı zafiyeti de ciddi bir gizlilik riski oluşturmaktadır[35]. Bu noktada toplumsal farkındalığı arttıcı faaliyetlerin yapılması ve kişilerin gizlilik konusunda bilgilendirilmeleri şarttır. Kullanıcılar, emin olmadıkları sitelerdeki uygulamalar yerine güvenilir kaynaklardan uygulama indirmeli, indirdikleri uygulamanın gizlilik kurallarını inceleyerek ilgili kurallara, düzenlemelere uyulduğundan emin olmalı veya emin olmadığı uygulamaları yüklememelidir. Aynı şekilde mobil hizmeti sunan tüm kamu, özel kurum ve kuruluşların verilerinin saklandığı alanlarda doğrulanabilir güvenlik sertifikaları ve ödeme sistemlerini güncel şekilde koruyucu tedbirleri alıp almadığının kullanıcılar tarafından sorgulanması güvenliği arttıracaktır.

[35]Henkoğlu, s.26

İKİNCİ BÖLÜM

MOBİL UYGULAMALARDA İŞLENEN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YASAL DÜZENLEMELER

2.1. GENEL OLARAK

İnternet erişimi hakkı, Avrupa Konseyi tarafından 19 Nisan 2011 tarihinde Avrupa İnsan Hakları Sözleşmesi'ne ("AİHS") temel bir hak olarak eklemiş, Birleşmiş Milletler tarafından da 04 Haziran 2011 tarihinde "Temel bir insan hakkı" olarak tanımlanmıştır. Her ne kadar internet erişim hakkı, AİHS'ne taraf olan ülkemiz iç hukukumuzda temek bir hak olarak tanımlanmamaktaysa da TBMM Araştırma Komisyonu'nun Haziran 2012 tarihli raporunda; bilgiye erişimin ve internetin temel hak olarak Anayasa'da tanımlanmasına ilişkin öneride bulunmuştur[36].

İnternet erişim hakkı, temel bir hak olarak ülke mevzuatında yer almasa dahi kamunun görevi, vatandaşlarının rahat ve güvenli bir şekilde internet kullanmaları için gerekli altyapı ve tedbirleri almaktır. İnternet platformu, kişilerin görüş, düşünce ve şikâyetlerini kolay ve hızlı bir şekilde ifade edebilecekleri ve her vatandaşın her hangi bir müdahale ve sansür olmaksızın haber ve bilgi almasına imkân veren platformlardan biri haline gelmiştir. Bu noktada, kişisel verilerin korunması hakkı ile düşünceyi açıklama ve yayma özgürlüğü arasında da yakın bir ilişki bulunduğu söylenebilir[37]. Kişisel veri kavramına bireylerin düşüncelerinin de dahil olduğu düşünüldüğünde bu verilerin hem kişisel verilerin korunması hem de düşünceyi açıklama ve yayma özgürlüğü kapsamında korunması gerekmektedir[38]. Dolayısıyla tüm bu gelişmeler karşısında bireylerin bilgi güvenliğinin ve mahremiyet alanlarının korunması, gelişen teknoloji ile artan siber güvenlik

[36]TBMM Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyon Raporu, Haziran 2012 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf, Erişim Tarihi : 05.04.2019

[37]Türkmen, Sevgi Eraslan Türkmen, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, İstanbul, 2019, s.14, Küzeci, Kişisel Veriler, s.83 vd.; Akgül, a.g.e., s.80 vd.; Şimşek, a.g.e., s.146; Avcıoğlu, a.g.e., s.22

[38]Türkmen, s.14

tehditleri gerekliliği ve verinin yeni ve popüler bir ekonomik değer olarak kullanılması karşısında bu konuda yasal düzenlemeler yapılması zorunluluk haline gelmiştir.

Öte yandan kanun koyucunun öncelikli amacı, her ne kadar bireylerin mahremiyet ve güvenlik haklarının korunması olsa da kanun koyucu, gelişen teknoloji karşısında elde edilen verilerin çeşitli şekilde kullanılması ile ortaya çıkan farklı iş modellerinin geliştirilmesini engelleyici veya şirketlerin ekonomik mağduriyetine neden olacak kısıtlayıcı düzenlemeler ve yaptırım uygulamak yerine bireylerin hak ve menfaatleri ile kurum ve kuruluşların menfaatleri arasında denge kuracak şekilde hareket etmelidir.

İnternet ortamında kullanıcılara hizmet sunulan her alanda bireylere ait kişisel veriler toplanmakta, kayıt altına alınmakta, işlenmekte ve yurt içi ve yurt dışı üçüncü kişi şirketlerle paylaşılmaktadır. Bu kapsamda ülkeler, kişisel veri kullanımı, paylaşımı ve korunması bakımından kendi kişisel verileri koruma mevzuatlarını düzenlemekle birlikte uluslararası platformlarda da bazı kuruluşlar mevzuatların geliştirilmesi amacıyla çeşitli rehber ilkeler yayınlamaktadırlar.

Çevrimiçi ortam veri işleme faaliyetlerinin en sık ve en kolay şekilde yapıldığı, verinin kolaylıkla yönetilebildiği, kullanıcının haberi dahi olmadan veri erişimi, veri transferi yapılan platformlardan biri de mobil uygulamalardır. Mobil uygulamalarda verilerin toplanma ve işlenme aşaması iki farklı süreçte olmaktadır. Birinci süreç, mobil uygulama, kullanıcının cihazına indirildiğinde cihazda mevcut bilgilere erişim sağlanarak verilerin toplanması ve işlenmesi, diğer süreç ise uygulama kullanıldığı sırada kullanıcıdan belli bilgiler istenerek verilerin toplanması ve işlenmesidir.

GPS[39], kamera, parmak izi, yüz okuma gibi mobil cihazlarda yer alan bileşenlerin ortaya çıkması ile birlikte genetik verilerin kolayca işlenebilir hale gelmesi, birçok

[39] Küresel Konumlandırma Sistemi

riski beraberinde getirmiştir. Kişisel verinin internet ve bulut teknolojileri ile uluslararası platformlarda kolayca paylaşılması neticesinde birçok ülke uluslararası alanlarda kabul gören ilkeler ve içtihatlar çerçevesinde iç mevzuatlarında kişisel verilerin korunmasına ilişkin düzenlemeleri yapmak zorunda kalmıştır. Mobil uygulamalarda kişisel verilerin korunması, AB ve Türkiye'de yürürlükte bulunan ve taslak aşamasında olan kişisel verilerin korunması mevzuatı kapsamında incelenecektir.

2.2. AVRUPA BİRLİĞİ KİŞİSEL VERİLERİN KORUNMASI HUKUKU

95/46 EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi[40] ("95/46 Sayılı Direktif") 04.05.2016 tarihinde AB resmi gazetesinde yayımlanan ve 25 Mayıs 2018 yılında yürürlüğe giren GVKT ile ilga edilene kadar AB'nin kişisel verilerin korunması bakımından temel düzenlenmesi olarak kabul edilmekteydi. Direktifin üye ülke mevzuatlarına doğrudan bir etkisinin olmaması, her üye ülkenin bu direktifte yer alan düzenlemeler çerçevesinde mevzuatlarında değişiklik yapması ve yeknesaklık sağlanamaması nedeni ile GVKT kabul edilmiştir. GVKT, AB üyesi olan her ülkenin iç mevzuatına doğrudan girerek kişisel verilerin korunması mevzuatı bakımından AB üyesi ülkeler arasında bir yeknesaklık meydana getirmiştir.

Elektronik haberleşme sektöründe yer alan kişisel veriler bakımından ise 2002/58 EC Sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına ilişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi[41] ("2002/58 Sayılı Direktif") kuralları uygulama alanı bulmuştur. GVKT ile uyumlu olması hedeflenen ve 2002/58 Sayılı Direktifi ilga edecek olan

[40]Directive 95/46 /EC of the European Parliament and of the Council of the 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union Official Journal, 1995 L281

[41]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, European Union Official Journal, 2002 L201

Elektronik Haberleşme ve Gizlilik Tüzüğü ("E- Gizlilik Tüzüğü")[42] ise henüz taslak aşamasındadır.

GVKT'nün yer açısından uygulama alanı başlıklı 3. maddesinde GVKT hükümlerinin uygulama alanı belirtilmiş, bu hükümlerin veri sorumlusu veya onun adına veri işleyen kuruluşun AB sınırları içerisinde faaliyeti kapsamında kişisel veri işlenmesi halinde ve veri sorumlusunun veya onun adına veri işleyen kuruluşun AB sınırları dışında olması ancak AB sınırlarında bulunan kişilere ürün veya hizmet teklifi ya da ilgili kişinin AB sınırları içerisindeki davranışlarının gözlemlemesi ile kişisel veri işlemesi halinda uygulama alanı bulacağını düzenlemiştir[43].

Türkiye, AB üyesi bir devlet olmadığı için GVKT kuralları ülke mevzuatına uygulanabilir olmasa da yukarıda belirtilen hüküm kapsamında, AB üye ülkelerde faaliyet gösteren ve bu üye ülkede yer alan kişilere mal ve hizmet sunan veya ilgili veri sahiplerinin davranışlarını gözlemleyen kurum veya şirketlerin kişisel veri işleme faaliyetleri bakımından GVKT kurallarına uygun hareket etmesi gerekmektedir. Aksi takdirde bu şirket veya kurumlar, ilgili üye ülkelerde yer alan veri koruma otoritelerinin yaptırımına maruz kalabileceklerdir.

2.2.1. 2002/58 Sayılı Direktif

AB üye ülkelerin elektronik haberleşme sektöründe yer alan kişisel verilerin korunmasını düzenlemek ve gizlilik hakkının korunması amacıyla 2002/58 Sayılı Direktif kabul edilmiştir. Bu direktif ile haberleşmenin gizliliği esas alınarak abone veya kullanıcıların bilgilerinin toplanması ve bu bilgilere erişim konusunda önemli kurallar getirilmiştir[44]. 2002/58 Sayılı Direktif ile 95/46 Sayılı Direktif'te yer alan ilkeler elektronik haberleşme sektörü özelinde uyarlanmıştır. Direktif, 95/46 Sayılı

[42]Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010, Erişim Tarihi : 05.06.2017

[43]Çekin, s.29

[44]Leyla Keser- Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, 1. baskı, İstanbul 2014, s.33

Direktif ve GVKT'den farklı olarak tüzel kişilerin haklarını da koruma kapsamınaa almıştır.

E- Gizlilik Tüzüğü hala taslak aşamasında olduğu için mobil uygulamalar bakımından 2002/58 Sayılı Direktif'in haberleşmenin gizliliği başlıklı 5.maddesi uygulama alanı bulacaktır[45]. Bu maddede direktif, üye ülkelere, elektronik haberleşme şebekelerinin bilgiyi muhafaza etmek veya kullanıcı ya da abonenin terminal cihazında yer alan bilgiye erişimini sağlama amacı ile kullanılmasını sadece ilgili kullanıcı ya da abonenin 95/46 Sayılı Direktif uyarınca veri işlemenin amacını da kapsayacak şekilde açık ve kapsamlı bir şekilde bilgilendirmiş olması ve veri sorumlusu tarafından bu veri işleme faaliyetini reddetme hakkının tanınması şartına bağlamalarını tavsiye etmektedir.

Madde 29 Çalışma Grubu görüşünde, 2002/58 Sayılı Direktif'in birçok maddesinin sadece AB üye ülkelerde yer alan kamuya açık elektronik haberleşme hizmetleri ve kamu haberleşme şebekesi servis sağlayıcılarına uygulanırken 5. maddenin 3. bendi ile bu direktifin akıllı cihazlardan bilgiyi okuyan veya saklayan niteliği ne olursa olsun özel veya kamusal, bireysel programcı veya büyük şirketler, veri sorumlusu, veri işleyen veya üçüncü kişi her kuruma uygulanacağının açıkça belirtildiğine yer vermiştir[46].

Madde 29 Çalışma Grubu aynı görüşün devamında, GVKT'de sadece kişisel verilerin koruma alanı bulduğunu, 2002/58 Sayılı Direktif'in bu maddesi ile akıllı cihazlarda saklanan ve erişilen her türlü veri ve bilgi için de rıza verilmesi gerektiğini[47], bu maddedeki rıza gerekliliğinin hizmet sağlayıcının nerde olduğuna bakılmaksızın Avrupa Ekonomik Topluluğu'nda ("AET") yaşayan tüm bireyler için sunulan hizmetlere uygulandığı, bu bağlamda mobil uygulamalar bakımından uygulama geliştiricilerin 95/46 Sayılı Direktif ve 2002/58 Sayılı Direktif

[45]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.7
[46]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.7
[47]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.7

hükümlerinin emredici nitelikte olduğunu bilmeleri, bu hakların devredilemeyeceği ve bu haklardan feragat de edilemeyeceğini belirtmiştir[48]. AET'unda yaşayan bireylerin haklarını koruma altına alan düzenlemelerin tüm dünyaya karşı emredici olması, AET'na hizmet sunmak isteyen her kurum ve kuruluşun da bu kurallara uymak zorunda olmasının global ölçekte kişisel verilerin ve mahremiyetin korunmasına ilişkin koruyucu hükümlere uygun hareket edilmesi konusunda zorunluluk yarattığı açıktır.

2.2.2. 2002/58 Sayılı Direktifi İlga Edecek Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunmasına İlişkin E- Gizlilik Tüzüğü Taslağı

Elektronik haberleşme sektöründe gelişen teknolojiler karşısında ortaya çıkan veri işleme faaliyetleri ile birlikte yeni tekniklerle iş modellerinin geliştirilmesi ve bu veri işleme faaliyetlerinin önem arz etmesi ile GVKT'nün getirdiği yenilikler karşısında 2009 ve 2013 yıllarında değişiklik yapılan 2012/58 Sayılı Direktif eksik ve yetersiz kalmıştır.

Elektronik haberleşme hizmetleri bakımından bu sektörde yer alan tüm aktörlerden hizmet alan kullanıcıların gizliliklerini GVKT ile getirilen yeniliklerle uyumlu olacak şekilde daha yüksek seviyede korumak ve güvenliği arttırmak amacıyla tüzük çalışmalarına başlandığı, E-Gizlilik Tüzüğü taslak metnin gerekçeler başlıklı 1. maddesinde de düzenlenmiştir. E-Gizlilik Tüzüğü taslağında 2002/58 EC Sayılı Direktifle paralel ve GVKT'nden farklı olarak sadece gerçek kişiler değil ticari sır niteliğinde olan veya ekonomik değeri olan özel nitelikli veriye sahip olan tüzel kişiler de korumadan yararlanabilmekte ve veri tanımını da daha genişleterek kişisel veri niteliğinde olan elektronik haberleşme verisini de koruma altına almaktadır.

E-Gizlilik Tüzüğü taslağının amaçlarından biri de elektronik haberleşme sektöründe yer alan klasik telekomünikasyon operatörlerinin dışında ortaya çıkan

[48]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.8

ve esas hizmetlerinin yanı sıra elektronik haberleşme hizmeti de sunan Facebook Messenger, WhatsApp, Skype gibi yeni aktörlerin de gizlilik kurallarına uygun hareket ettiğinden emin olmak ve tüzük hükümlerinin üye ülkeler mevzuatına ayrıca bir işlem yapmadan doğrudan etki etmesi sebebiyle AB sınırları içerisinde yer alan kişi ve kuruluşların elektronik haberleşme konusunda yeknesak bir korumadan yararlanmalarını sağlamaktır[49].

Bununla birlikte Madde 29 Çalışma Grubu, E-Gizlilik Tüzüğü taslağı hakkındaki 04 Nisan 2017 tarih ve 01/2017 sayılı görüşünde, dört ana kaygısını dile getirmiştir. Bunlar, cihazın konumunun izlenmesi[50], içerik ve meta verinin analiz amaçlı kullanılmasına izin verilmesine ilişkin şartlar, cihazın ve yazılımın varsayılan ayarları ve izleme duvarları konularında toplanmaktadır.

E-Gizlilik Tüzüğü taslağının başlangıç kısmının 5. paragrafında tüzük hükümlerinin GVKT kapsamındaki korumadan daha düşük seviyede bir koruma sağlamayacağı hususu özellikle vurgulanmıştır. Bununla birlikte Madde 29 Çalışma Grubu, taslağın bu haliyle GVKT'de yer alan korumadan daha düşük bir seviyede koruma sağladığı görüşünde olup taslak tüzüğün, GVKT ile aynı veya daha yüksek seviyede koruma getirmesini önermektedir[51].

2.2.3. Avrupa Birliği 2016/679 Sayılı Genel Veri Koruma Tüzüğü

95/46 Sayılı Direktif zaman içerisinde gelişen teknoloji ve veri kullanımının çok farklı alanlarda yaygınlaşması sonucunda yetersiz kalmış ve direktiflerin hukuki nitelikleri itibariyle çerçeve niteliğinde olmaları, üye ülkelerin iç hukuklarına doğrudan etki etmemesi sebebiyle üye ülkelerde aynı konularda farklı hukuki düzenlemelerin ortaya çıkmasına neden olmuştur. Hem üye ülkeler arasındaki

[49]https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation, Erişim Tarihi 06.12.2017

[50]Alışveriş merkezlerinde veya havalimanlarından ücretsiz wifii erişim noktalarına erişim sağlanarak cihazın izlenmesi. Örneğin bir alışveriş merkezinde kişinin hangi mağazalara girdiği, oralarda ne kadar vakit harcadığı , binada ne kadar kaldığı, binaya nerden girip nerden çıktığı gibi bilgilerin toplanması.

[51]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.3

hukuki düzenlemeleri yeknesak hale getirmek hem de daha etkin bir koruma getirmek için üye ülkelerin iç hukuklarına ayrıca bir işlem yapılmaksızın doğrudan etki edecek tüzük şeklinde bir düzenleme yapılması ihtiyacı doğmuştur.

Bu doğrultuda AB'de gelişen teknoloji ve toplumsal ihtiyaçlar karşısında üye ülkelerde veri korunmasına ilişkin farklı uygulanma biçimlerini ortadan kaldırmak ve tüm üye ülkeler arasında yeknesak bir düzenleme yapmak amacıyla 2012 yıllarının başında başlatılan yeni bir tüzük çalışması, 14 Nisan 2016 tarihinde kabul edilmiş ve 04.05.2016 tarihinde AB resmi gazetesinde yayımlanmış, 25 Mayıs 2018 tarihi itibari ile 95/46 Sayılı Direktif ilga edilerek yürürlüğe girmiştir.

2.2.3.1. GVKT'ün Getirdiği Yenilikler

GVKT'nün 95/46 Sayılı Direktif'ten farklı konularda yenilikler getirmiştir**.** GVKT'ün, AB hukukuna tabi olmayan ancak AB üye ülke vatandaşlarına mal ve hizmet vermeyi hedefleyen ve onların kişisel verilerini işleyen kuruluşlara da uygulanması, veri sorumlusu ile birlikte veriyi işleyen herhangi bir kurum veya kişinin de sorumlu olması[52], kişisel verisinin hukuka aykırı işlenmesi sebebiyle zarara uğrayan kişiye tazminat talep hakkı tanınması, rıza kavramının daha ayrıntılı olarak tanımlanması, çocuklara özgü koruma getirilmesi ve çocukların verilerinin işlenmesinin ebeveynlerinin rızaları ile mümkün olabilmesi, unutulma hakkı ile verisi işlenen kişinin verilerinin silinmesini talep etme hakkına sahip olması, tasarımla veri koruma[53] ve varsayılan ayarlarla veri koruma[54] kavramlarının tanımlanması, kişisel verilerin işlenmesi faaliyetinin kişilerin temel hak ve hürriyetlerini ihlal etme riski taşıdığı durumlarda veri koruma etki analizinin[55] yapılmasının zorunlu tutulması, hesap verilebilirlik ilkesi gereğince hukuka aykırı veri işlenmesi durumunda veri işleyenler durumu hemen veri sorumlularına onlar

[52]Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Çalışma Raporu 6, Ayşenur Akıncı, Haziran 2017 http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf Erişim Tarihi, 11.11.2017

[53]Taştan, s.18

[54]Taştan, s.19

[55]Data Protection Impact Assessment

da denetleyici ilgili veri koruma otoritesine bildirmekle yükümlü tutulması, veri koruma otoritesine ihlal halinde bunu gerçekleştiren kuruma idari para cezası yaptırımı uygulaması söz konusu yeniliklere örnek olarak gösterilebilir.

2.2.4. Avrupa Veri Koruma Kurulu (Madde 29 Çalışma Grubu) Görüşleri

25 Mayıs 2018 tarihinde GVKT'nin yürürlüğe girmesi ile görevini Avrupa Veri Koruma Kurulu'na[56] ("AVKK") bırakan Madde 29 Çalışma Grubu, bu tarihe kadar 95/46 Sayılı Direktif'in 29. maddesi ile kurulan veri mahremiyeti ve korunması ile ilgili tavsiye niteliğinde görüş veren ve AB bünyesinde danışma kurulu olarak görev yapan bağımsız bir organdı. Görevleri, 95/46 Sayılı Direktif'in 30. maddesinde ve 2002/58 Sayılı Direktif'in 15. maddesinde tanımlanan Madde 29 Çalışma Grubu'nun görüşleri, AB üye devletler için kesin ve bağlayıcı olmamakla birlikte mevcut ve muhtemel durumlar bakımından çerçeve oluşturması ve tavsiye vermesi bakımında önem arz eden bir nitelikteydi.

Teknolojinin ve bilişim sektörünün hızlı bir şekilde ilerlemesi ile birlikte mobil uygulamalar, kişilerin yemek, e-ticaret, sağlık, eğlence, oyun, bankacılık, ulaşım, sesli ve görüntülü iletişim, seyahat, e-devlet gibi binlerce farklı seçeneğe rahat ve kolay bir şekilde erişmesini sağlayarak gittikçe artan bir hızla tercih edilen bir platform olmuştur. Hukuk düzenlemelerinin teknolojik gelişmeler karşısında aynı hızla ilerleyememesi, ortaya çıkan yeni kavramlar, yeni tanımlarla birlikte mobil uygulama alanında yer alan aktörlerin, verileri toplama, kullanma ve işleme faaliyetlerinde yer alan riskleri ve bu risklere ilişkin kurallara yabancı olmaları mobil uygulama açısından bir çalışma yapılmasını zorunlu tutmuştur. Bu kapsamda en ayrıntılı ilk değerlendirme, Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü ile olmuştur. Bu görüşte, Madde 29 Çalışma Grubu, uygulamaların yazılım aşamasında ve akıllı

[56] European Data Protection Board (EDPB), GVKT ile kurulan ve Brüksel'de faaliyet gösteren veri koruma kurallarının Avrupa Birliği genelinde tutarlı bir şekilde uygulanmasına katkıda bulunan ve AB'nin veri koruma otoriteleri arasında işbirliğini destekleyen bağımsız bir Avrupa organıdır. EDPB, ulusal veri koruma otoritelerinin ve Avrupa Veri Koruma Denetçisinin (EDPS) temsilcilerinden oluşur.

cihazlarda kullanılması sırasında kişisel verilerin işlenmesi ile ilgili yasal çerçeveyi açıklığa kavuşturmak, rıza gereklilikleri ile amaçla sınırlılık ve ölçülülük ilkelerine vurgu yaparak son kullanıcıyı doğru bir şekilde bilgilendirme ile özellikle çocuklar hakkındaki verinin adil bir şekilde işlenmesi için yeterli güvenlik önlemlerinin alınması konusunda değerlendirmeler yapmıştır.

2.3. TÜRKİYE KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Türkiye, her ne kadar Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına İlişkin 108 Sayılı Sözleşme ve 181 Sayılı Ek Protokol'e taraf olsa da bu anlaşmayı iç hukukta onaylayacak kanun düzenlemesi olan 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("6698 Sayılı Kanun") yürürlüğe girene kadar geçen sürede, kişisel verilerin korunması, Türkiye'de ilk kez 2004 yılında "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" ile gündeme gelmiştir[57].

12.09.2010 tarihli Anayasa değişikliği ile birlikte Özel Hayatın Gizliliği başlıklı 20. Maddesine ek fıkra olarak herkesin kendisi ile ilgili kişisel verilerinin korunmasını isteme hakkını sahip olacağı düzenlenerek bu hak temel bir insan hakkı olarak düzenlenmiştir. Kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği de Anayasa ile güvence altına alınmıştır[58].

5237 Sayılı Türk Ceza Kanunu'nda 134. ve devamı maddelerinde kişisel verilerin hukuka aykırı işlenmesine yönelik düzenlemelere yer verilmiştir. Bu kapsamda kişilerin özel hayatının gizliliğini ihlal edenlerin cezalandırılacağı, gizliliğin görüntü ve seslerin kayda alınması suretiyle ihlal edilmesi halinde cezanın arttırılacağı, kişisel verileri hukuka aykırı olarak kaydeden kişilerin cezalandırılacağı söz konusu verilerin özel nitelikli veriler olması halinde cezanın yarı oranında attırılacağı, kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin eyleminin cezalandırılacağı, bu kişinin kamu

[57] Taştan, s.21
[58] Taştan, s.21

görevlisi olması halinde verilen cezanın arttılacağı düzenlenmiştir. Ayrıca kaydedilen verilerin belirlenen süre içinde silinmemesi durumunda da ceza verileceği düzenlenmiştir.

2.3.1. 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun

6698 Sayılı Kanun ile öncelikli olarak kişisel verilerin işlenmesinin belli bir disiplin altına alınarak bireylerin mahremiyet ve gizlilik hakkının korunması, kişinin bilgi güvenliğinin korunmasını ve kişisel veri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları esasların düzenlenmesi amaçlamaktadır. 6698 Sayılı Kanun daha çok 95/46 Sayılı Direktif esas alarak hazırlanmış olmasına rağmen GVKT'da yer alan tazminat hakkı, idari para cezası gibi yenilikler de 6698 Sayılı Kanunda yer almıştır.

Kanun koyucu, GVKT düzenlemesine paralel olarak sadece gerçek kişilere uygulanan düzenlemeler içermektedir, tüzel kişiler 6698 Sayılı Kanun'un kapsamında değildir.

2.3.1.1. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

6698 Sayılı Kanun'un 7. maddesinin 3. fıkrası ile 22. maddesinin 1. fıkrasının e bendine dayanılarak Kişisel Verileri Koruma Kurulu ("Kurul") tarafından hazırlanan ve 28.10.2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile kişisel verilerin silinmesi yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esaslar belirlenerek[59] veri sorumluları ve veri işleyenler tarafından uyulması gereken yükümlülükler düzenlenmiştir. Kurul tarafından yayımlanan rehberde ise kişisel verilerin silinmesi, silme işleminin süreci ve yöntemleri ile kişisel verilerin yok edilmesi ve buna ilişkin yöntemler açıklanmıştır.

[59]28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazetede yayınlanmıştır.

2.3.1.2. Veri Sorumluları Sicili Hakkında Yönetmelik

6698 Sayılı Kanunun 16. maddesinin 5. fıkrası ile 22. maddesinin 1. fıkrasının d ve e bentlerine dayanılarak hazırlanan ve 30.12.2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanarak 01.01.2018 tarihinde yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmelik ile veri sorumluları sicili oluşturulması, idaresi ile veri sorumluları siciline yapılması öngörülen kayıtlara ilişkin usul ve esaslar belirlenmiştir[60]. 6698 Sayılı Kanun'da veri sorumlusuna getirilen yükümlülüklere ilişkin olarak veri sorumluları siciline kayıt yükümlülüğü bulunan veri sorumlularının kişisel veri işleme envanteri ve kişisel veri saklama ve imha politikası hazırlaması gerektiği düzenlenmiştir. Ayrıca aynı yönetmeliğin 4. maddesinde kişisel veri işleme envanteri tanımı yapılarak envanterde yer alması gereken hususlar da belirtilmiştir.

2.3.2. 5809 Sayılı Elektronik Haberleşme Kanunu ve İlgili Mevzuat

2.3.2.1. 5809 Sayılı Elektronik Haberleşme Kanunu

5809 Sayılı Elektronik Haberleşme Kanunu ("EHK"), elektronik haberleşme sektörü bakımından en temel düzenleme olup bu sektöre ilişkin kişisel verilerin korunması ile ilgili hükümler içermektedir[61]. Bilgi güvenliği ve haberleşme gizliliğin gözetilmesi ilkesi, elektronik haberleşme hizmetinde yer alan bir ilke olarak kanun ile koruma altına alınmıştır. Bu konuda düzenleme yapma yetkisi, Bilgi Teknolojileri ve İletişim Kurumu'na ("BTK") verilmiş, EHK 6. maddesinde abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak BTK'nın görevleri arasında sayılmıştır.

Aynı şekilde EHK 55. maddesine göre de BTK izin vermedikçe abone veya kullanıcıların kimlik ve iletişim bilgilerinin veya cihazların teşhisine yarayan

[60] 30.12.2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanmış ve 01.01.2018 tarihinde yürürlüğe girmiştir.

[61] Ayözger, Çiğdem Ayözger, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, Beta Yay, İstanbul, 2016, s. 98

elektronik kimlik bilgilerinin yeniden oluşturulamayacağı, değiştirilemeyeceği, kopyalanarak çoğaltılamayacağı veya herhangi bir amaçla dağıtılamayacağı düzenlenmiştir. 56. maddede abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gerecin yetkisiz ve izinsiz olarak kopyalanamayacağı, muhafaza edilemeyeceği, dağıtılamayacağı, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamayacağı kanun ile koruma altına alınmıştır[62].

EHK'nun elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme konusunda BTK'ya yetki verilmesini düzenleyen 51. maddesi, Anayasa Mahkemesi tarafından kişisel verilerin korunması hakkında kanun yürürlüğe girmediği ve Türkiye Cumhuriyeti Anayasası 20. maddesi kapsamında özel hayatın gizliliğinin sınırlandırılmasına ilişkin hükümlerin kanuni düzenleme ile konulabileceği ve henüz kanuni bir düzenleme yok iken, yürütme organına bu hususta yetki verilmesinin hukuka aykırı olduğu gerekçesi ile iptal edilmiştir[63]. İptal kararından sonra elektronik haberleşme sektöründe kişisel verilerin korunmasına ilişkin genel ilkeler iptal edilen madde metnine işlenmiştir[64].

6698 Sayılı Kanun'dan farklı olarak bu maddede, elektronik haberleşme ve ilgili trafik verisinin de gizliliğinin esas olduğu ilgili mevzuat ve yargı kararlarının öngördüğü durumlar dışında haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasaklandığı düzenlenmiştir.

2.3.2.2. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik ve Yönetmeliği İlga Edecek Yönetmelik Taslağı

EHK'nun 4, 6, 12 ve 51. maddelerine dayanılarak BTK tarafından hazırlanan ve 24.07.2012 tarih ve 28363 sayılı Resmi Gazete'de yayımlanan Elektronik

[62] Ayözger, s.107
[63] Anayasa Mahkemesi E. 2013/122, K. 2014/74, T. 09.04.2014, R.G. 29072, Y.T. 26.07.2014,
[64] Ayözger, s.107

Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik **("EHGY")** ile 2002/58 Sayılı Direktifle uyumlu olarak gerçek kişilerin yanı sıra tüzel kişilerin de verilerinin de korunacağı hüküm altın alınmıştır[65]. Ancak dayanak kanunun ilgili maddesi Anayasa Mahkemesi tarafından iptal edilince yönetmeliğin geçersiz olmaması için Kanunun ilgili maddesi yeniden düzenlenmiştir.

6698 Sayılı Kanun'un yürürlüğe girmesinden sonra ve kişisel verilerin korunması ile ilgili olarak ortaya çıkan yeni gelişmeler de dikkate alınarak yeni bir taslak yönetmelik düzenlenmesi arayışına gidilmiştir. BTK'nın 07.08.2017 tarihli ve 2017/1K-THD/239 sayılı Kararı ile EHK'nın 51.maddesi hükümlerinin uygulanmasına ilişkin hususların netleştirilmesi ve ikincil hususların düzenlenmesi amacıyla hazırlanan taslak metin, EHGY 'in, BTK Teşkilât Yönetmeliği'nin "Görüş alınması ve değerIendirilmesi" başlıklı 44. maddesinin 1. fıkrası uyarınca kamuoyu görüşü alınmak üzere 17 Ağustos 2017 tarihinde internet sitesinde kamuoyunun görüşünün alınabilmesi amacıyla paylaşılmıştır[66].

EHGY taslağı öncelikle EHK'nun yanı sıra 6698 Sayılı Kanun'u da dayanak almış, yeni tanımlar eklenerek 6698 Sayılı Kanun'ula uyumlu olacak şekilde daha ayrıntılı olarak düzenlenmiştir. Ayrıca EHGY'te yer alan haberleşmenin içeriğine ilişkin verilerin saklanmasının yönetmeliğin kapsamı dışında olduğu hükmü taslak metinden kaldırılmıştır.

Özellikle rıza yerine açık rıza tanımı yapılarak rıza tanımı genişletilmiş ve 6698 Sayılı Kanun'a uyumlu hale getirilmiştir. Konum verisi tanımı daha genişletilmiş, konum, trafik verisi ve ilgili diğer bilgiyi kapsayan veri tanımı ise taslak metinde elektronik haberleşme verisi olarak değiştirilmiştir. Buna göre elektronik haberleşme verisi, elektronik haberleşme hizmeti alanların ses, görüntü, kısa mesaj ve benzeri verileri ile taslak yönetmeliğin saklanacak elektronik haberleşme veri

[65] Taştan, s.29

[66] http://www.kbd.org.tr/s/2389/i/KBD_EH-KisiselVeriler-20170807-239-Karar.pdf, Erişim Tarihi : 08.12.2018

kategorileri başlıklı 11. maddesinde[67] kategorize edilen veriler olarak tanımlanarak geniş bir veri tanımı yapılmıştır. Buna ilişkin gerekçede, EHK'nun elektronik haberleşme sektörüne özgü olarak işletmecilerde oluşan kişisel elektronik haberleşme verilerinin düzenlenmesini öngördüğü düşünüldüğü bu sebeple de kişisel veri tanımı yerine kişisel elektronik haberleşme verisi tanımı yapıldığı yer almıştır[68]. Ayrıca 6698 Sayılı Kişisel verilerin Korunması Hakkındaki Kanunda yer alan ilgilinin hakları maddesi taslağa abonenin hakları olarak eklenmiştir.

[67]Madde 11– (1) Bu Yönetmelik kapsamında işletmeciler tarafından aşağıda belirtilen kategorilerdeki elektronik haberleşme verileri saklanır. a) Elektronik Haberleşmenin takibi ve kaynağının tanımlanması için: 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere haberleşmenin başlatıldığı hatta ait telefon numarası, abonenin adı ve adresi, hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgi. 2) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, abonenin/kullanıcının adı ve adresi. b) Elektronik Haberleşmenin sonlandırılacağı noktayı belirlemek için: 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin sonlandırıldığı/sonlandırılacağı numara veya numaralar, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi. 2) Elektronik posta ve internet telefonu ile ilgili olarak; elektronik posta alıcılarına ait kullanıcı kimliği, internet telefonu ile aranan alıcılara ait kullanıcı kimliği veya telefon numarası, internet telefonu veya elektronik posta alıcılarının adı ve adresi. c) Elektronik Haberleşmenin tarihi, zamanı ve süresini belirlemek için: 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin başlangıç ile bitiş tarih ve zamanı. 2) İnternet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; internet erişimi ile ilgili oturum açma, kapatma tarihi ve zamanı, tahsis edilen dinamik veya statik IP adresi, NAT kullanılan şebekelerde IP adresi yanında port bilgisi, abone/kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili oturum açma ile kapatma tarihi ve zamanı. ç) Elektronik Haberleşmenin türünü tanımlamak için: 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak kullanılan elektronik haberleşme hizmeti. 2) Elektronik posta ve internet telefonu ile ilgili olarak kullanılan internet hizmeti. d) Kullanıcıların elektronik haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için: 1) Sabit telefon hizmetiyle ilgili olarak haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları. 2) Mobil telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları, haberleşmenin başlatıldığı ve/veya sonlandırıldığı tarafa ait IMSI ve IMEI numaraları; abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği. 3) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; çevirmeli ağ erişimi için arayan telefon numarası, sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer nokta. e) İlgili mevzuatın öngördüğü hallerde mobil haberleşme cihazının konumunu tespit etmek için; haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sürede hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veri, hücre adresi ve hücre kimliğinin o adrese atanma ve kaldırılma tarihleri.

[68] http://www.kbd.org.tr/s/2389/i/KBD_EH-KisiselVeriler-20170807-239-Karar.pdf, Erişim Tarihi : 08.12.2018

ÜÇÜNCÜ BÖLÜM

MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN KORUNMASI

3.1. GENEL OLARAK

Mobil uygulama alanında birden fazla aktör yer aldığından öncelikle bu aktörlerin rollerini ve görevlerini tanımlamak ve mobil uygulamalarda verilere temas eden kişilerin hangilerinin veri sorumlusu hangilerinin veri işleyen sıfatına haiz olduğunu belirlemek, yasal sorumlulukların çerçevesinin çizilmesi açısından önem arz etmektedir. Her halükarda cihazın üretimi, dağıtımı veya işletimi aşamasında veri sorumlusu olarak kabul edilen kişi veya kişiler yasal zorunluluklara uygun hareket etmek zorundadır.

Madde 29 Çalışma Grubu, uygulama geliştiriciler, uygulama mağazaları, işletim sistemi ve cihaz üreticileri ve üçüncü kişi aktörlere, veri sorumlusu ve/veya veri işleyen olarak kendilerine düşen sorumlulukları yerine getirmek adına tasarımla veri koruma ve varsayılan ayarlarla veri koruma prensibi ile hareket etmelerinin yanı sıra veri minizasyonu ilkesi kapsamında etkili kısıtlayıcı önlemler alarak mevcut veya muhtemel veri koruma riskleri ile ilgili denetimler yapmasını tavsiye etmektedir[69].

3.2. MOBİL VERİ TOPLAMA KANALLARI

Mobil platformlarda veri toplama ve veri yönetme faaliyeti, masaüstü, dizüstü bilgisayarlar gibi çevrimiçi ve çevrimdışı platformlara nazaran farklı teknik altyapı modelleri ile desteklenmekte ve bu konuda gün geçtikçe yeni iş modelleri oluşturulmaktadır. Bu farklılık, aynı zamanda mobil verilerin niteliğini, kalitesini ve önemini de beraberinde getirerek mobil alandaki verilerin daha güvenli yöntemlerle korunmasını da zorunlu kılmaktadır.

[69]Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü,s.11

Mobil cihaza birçok farklı kanaldan veri aktarılmakta, bu kaynakların başında ise cihaz ve işletim sistemi, sensör ve bileşenler, mobil uygulamalar, kablosuz ağ ve bluetooth erişimi, bulut teknolojisi, ses iletişimi, haberleşme hizmeti sağlayan operatörler, kullanıcının kendisi yer almaktadır.

3.2.1. Cihaz ve İşletim Sistemi

Akıllı cihazlar, işletim sistemleri ile birlikte kullanılmakta ve cihazın kendisinde olan konum bilgisi, ağ ayarları, IP adresi bilgileri, cihaz ve kişi belirleyicileri IMEI[70], IMSI[71], UDID[72], MAC[73], telefon numarası gibi bilgileri varsayılan olarak işlemektedirler. Bunun yanı sıra cihaz depolama alanında, telefon numarası, veri sahibinin kimliği, telefonun kimliği, telefonun adı[74], kredi kartı ve ödeme verileri, arama kayıtları, uygulama kullanırken kullanıcı tarafından üretilen telefon rehberi, notlar, SMS veya anlık mesajlaşmalar, gezinme geçmişi, e-posta, toplum bilgilendirme servisi kimlik doğrulama bilgileri, resim ve videolar, biometrik, yüz tanıma ve parmak izi özellikleri gibi bir çok farklı veri saklanmakta ve işlenmektedir[75]. Bu veriler, cihaz sahibi ile ilişkili olabileceği gibi cihaz sahibinin telefon rehberinde kayıtlı üçüncü şahsa ait bir veri de olabilir. Bu noktada mobil cihaz ve işletim sistemi, verinin depolandığı ana yer olması bakımından veriye erişim açısından da önemli bir kaynaktır. Cihaz ve İşletim sisteminin cihazın kullanım süresi boyunca ve kullanım sonrasında dahi veri gizliliğini sağlayacak tedbirleri alması önemlidir. İşletim sistemi ile cihazda yüklü olan uygulamaların cihazdaki hangi verilere eriştiğini görmek ve kullanıcının erişim izinlerini dilediği gibi yönetebileceği ortam sunması önemlidir. IOS ve Android işletim sistemlerinde ayarlar kısmında cihazda yüklü olan uygulamalar listelenmekte ve hangi uygulamanın hangi izinlere sahip olduğu görülmektedir. Kullanıcı bu panelde hangi

[70]Uluslararası mobil cihaz kimlik no
[71]Uluslararası mobil abone kimlik no
[72]Cihaz belirleyici
[73]Media Access Control, cihazın internet ağındaki teşhisine imkan tanıyan numarasıdır.
[74]Kullanıcıların telefonlarına verdikleri isimler.
[75]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.8

uygulamanın hangi verilerine eriştiğini görerek erişim konusunda kontrol hakkına sahip olacaktır.

3.2.2. Sensör ve Bileşenler

Sensörler, akıllı cihaz içerisinde ölçüm, yönlendirme gibi birden fazla işlevi yerine getirmek için veri toplama yapan bazı durumlarda yazılım tabanlı da olan donanımlardır. Sağlık, güvenlik, kolaylık, üretkenlik ve sürdürülebilirlik gibi birçok alanda dönüşümsel iyileştirmeler getirmeyi vaat eden sensörlerin çeşidi ve sayısı akıllı telefon, tablet bilgisayarlar olmak üzere giyilebilir teknoloji, akıllı evler gibi platformlarda gittikçe yaygınlaşmaktadır. Sensörlerin farklı cihazlarla iletişime geçerek nesnelerin interneti[76] gibi yeni hizmetler ve iş modelleri de artış göstermektedir[77]. Bazı durumlarda bu iletişime geçme durumundan kullanıcının bilgisi dahi olmamaktadır. En basit şekilde açıklamak gerekirse sensörlerden elde edilen veriler ile kullanıcının yürüyüş yapma, koşma ve sabit durma durumları tespit edilebilir olmakta, acil servisi arayan kişilerin konum verisi ile kaçıncı katta oldukları verisine[78] dahi erişilebilmektedir. Nesnelerin interneti mobil cihazlarda toplanan verilere dayanarak kullanıcının alışkanlıkları, veya faaliyetlerine karşılık

[76] İlk Olarak Kevin Ashton tarafından 1991 yılında yapılan bir sunumda kullanılmış bir kavram olan Nesnelerin İnterneti (IOT) birbiriyle ilişkili bilgi işlem cihazları, mekanik ve dijital makineler, nesneler, hayvanlar veya benzersiz tanımlayıcılar (UID'ler) ile sağlanan insanlara ve insandan ağa gerek duymadan bir ağ üzerinden veri aktarabilen sistemlerin tümünü ifade eder.

[77] Jacob Kröger, Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things, IFIP International Internet of Things Conference, 2018 https://link.springer.com/chapter/10.1007/978-3-030-15651-0_13 Erişim Tarihi : 09.03.2020

[78] New York Columbia Üniversitesi'nden William Falcon ve Henning Schulzrinne, GPS, sinyal gücü ve atmosferik basıncı birleştirerek - birçok akıllı telefonun şu anda içerdiği barometreyi kullanarak – arayan kişinin ne kadar yükseklikte olduğunu belirleyebilen Sensory adlı bir uygulama keşfetmişlerdir. Birçok akıllı telefon, deniz seviyesinden yüksekliklerini tespit edebiliyor. Katlar arasındaki mesafe binadan binaya önemli ölçüde değiştiğinden bu tespit sadece rakımı verirken doğrudan kat numarasına dönüşmemektedir.. Bu sorunu çözmek için Falcon ve Schulzrinne, belirli binaların farklı katlarını tekrar tekrar ziyaret eden gönüllüleri izleyerek elde ettikleri hareket verilerini belirli rakımlarda kümeleyerek farklı katları ortaya çıkarmıştır. Falcon, Rockefeller Center da dahil olmak üzere beş New York binasında 63 rastgele katı ziyaret ederek uygulamayı test etmiş ve testlerin yüzde 91'inde sistem iki katın içinde doğrulanmıştır. Sydney'deki New South Wales Üniversitesi'nden Binghao Li ve meslektaşları da kablosuz ağ sinyallerini kullanarak kat konumunu tahmin eden bir sistem geliştirmişlerdir. https://www.newscientist.com/article/2152366-phone-sensors-can-save-lives-by-revealing-what-floor-you-are-on/#ixzz6Cd03Cm00 Erişim Tarihi : 09.03.2020

gelen verilerin kombinasyonuna ve analizine dayanarak hizmetlerini sunar. Kamera, mikrofon ve GPS gibi navigasyon sistemleri mevcut işletim sistemleri tarafından ancak kullanıcının açık rıza vermesi ile kullanılabilirken ivmeölçerler, jiroskoplar ve barometreler gibi göze çarpmayan sensörler bu kapsamda daha az korunmaktadırlar. Sensörlerden elde edilen verinin içerik ve konum verisi olduğu, 13-14 Ekim 2014 yılında Balaclava, Mauritius'da yapılan Uluslararası Veri Koruma ve Gizlilik Komiserleri Konferansında da kabul edilmiştir. Konferansta, sensörlerden toplanan verinin miktar, kalite ve hassasiyeti dikkate alındığında tanımlanabilirliğin ve eşleştirmenin daha büyük olduğu büyük verinin korunması ve tanımlanabilirliğinin zorluğu karşısında bu verilerin kişisel veri olarak korunmasını, şeffaflık ilkesi ve uluslarası gizlilik prensiplerine uygun şekilde hareket edilmesine ilişkin kararlar alınmıştır[79].

Tablo 1.1. En Yaygın Akıllı Cihaz Sensörleri[80]

Sensör Tipi	**İşlevi**
İvmeölçer	Titreşim, döndürme hareketi algılama, hız ölçümü
Jiroskop	Adım sayma, yön tespiti veya ölçümü
Isı Ölçer	Oda/havanın ısısının ölçümü
Manyetik Ölçer	Alan yoğunluğu, mesafe, hız, akım algılama ve konumlandırma
GPS	Konum bulma, enlem boylam bilgisi, yükseklik
Işık Sensörü	Ortam aydınlatma seviye ölçümü
Barometre	Hava basıncı, deniz seviyesi yükseklik ölçümü
Yakınlık	Cihaza nesne yakınlaştığında algılama
Kamera	Görüntü ve video kaydedici
Mikrofon	Ses kaydedici

[79] Kröger, s.148
[80] Kröger, s.150

3.2.3. Kablosuz Ağ ve Bluetooth Erişimi

Bluetooth, benzer teknolojiyi kullanan diğer cihazlar arasında kablosuz bağlantı sağlayarak veri alışverişi sağlayan bir teknolojidir. Bu teknoloji ile cihazlar arasında her türlü veri alışverişi mümkün olmaktadır.

Kullanıcılar ücretsiz kablosuz bağlantı sunan mağaza, kafe, restoran, avm alanlarında bu hizmetten faydalanmak amacıyla hizmet şartlarını kabul ederek hizmet sağlayıcının kendi cihazlarındaki bir çok veriyi kullanmalarına da izin vermiş olmaktadırlar. Kablosuz ağ bağlantısı ile ilgili diğer bir sorun da bu bağlantı ile mobil cihazın izlenebiliyor olmasıdır[81]. Wifi izleme olarak tanımlanan bu durum, kişilerin mobil cihazlarından gelen sinyal ile izlenmesi anlamına gelir. Mobil cihazlar, kablosuz erişim noktasına bağlanmak için sürekli olarak sinyal iletir. Bu noktada telefonun MAC adresini içeren sensör, telefondan gelen sinyalleri aldığında telefonu diğer cihazlardan ayırt edilebilir hale getirir. Sensör, MAC adresini diğer verilerle, yani cihazın kayıtlı sinyal gücü, cihazın konumu, ölçümün tarihi ve saati ile birlikte işler. Veri analisti, bu veriler doğrultusunda sensör kapsamındaki cihaz sayısı ve insanların davranışları hakkında bilgi alabilir. Ticari şirketler, bu şekilde belli mekanlarda alışveriş davranışı ve yürüyüş akışları hakkında ekonomik veriler üretebilmektedir.

Kullanıcılar wifi izleme durumunda kullanıcıdan birçok kez opt out[82] yapması beklenemez[83]. Bu tarz yapılan izleme faaliyetleri için istisna getirilerek uygun güvenlik tedbirleri alınmasının sağlanması, gerekli teknik ve organizasyonel önlemler alınarak verinin herhangi bir ölçüm ve karar için işlenmemesi, ayrıca opt-

[81] ABD'de faaliyet gösteren alışveriş mağazasının, alışveriş yapanları izlemek için Euclid Analytics olarak bilinen bir hizmet kullandığı ortaya çıkmış, bu hizmet ile ücretsiz kablosuz ağ aracılığıyla, alışveriş yapanların hangi departmanları ziyaret ettiğini ve orada ne kadar zaman geçirdiklerini belirlenebilir olmuştur. Forbes 100'den fazla perakendeci bu hizmetten yararlandığını bildirmiştir. https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare Erişim Tarihi : 10.02.2020

[82] Kullanıcının işlemin yapılmaması için bunun açık bir şekilde harekette bulunarak ifade edilmesi

[83] Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) s.19

out seçeneğinin olması ve saklanan veriler için süre sınırlamaları olması gerekmektedir.

3.2.4. Bulut Bilişim

Bulut bilişim, bilişim kaynaklarına bir ağ üzerinden erişilmesi olarak tanımlanmaktadır[84]. Bu teknolojide verinin gönderildiği yer, firma ağının dışında bir alan olduğundan burada bulunan ve işlenen kişisel verilerin güvenliği için ayrı bir değerlendirme yapılması gerekmektedir. Bulut hizmeti sağlayıcının yurt dışında bulunması halinde bu durumda yurt dışına veri aktarımına ilişkin kurallar devreye girecektir.

3.2.5. Mobil Uygulamalar

Mobil uygulamalar, bazı durumlarda uygulamanın işlevini yerine getirmek bazı durumlarda farklı amaçlarla cihazda yer alan verilere erişim isterler. Bunların en başında konum, albüm, rehber, kamera, mikrofon, takvim, SMS, arama geçmişi vb. örnekler verilebilir. Cihazın ayarlarında cihazda yüklü uygulamaların hangi verilere eriştiği, kullanıcı tarafından erişim kontrolü yapılmaktadır.

3.3. MOBİL UYGULAMA VE BÜYÜK VERİ İLİŞKİSİ

Kabul görmüş net bir tanım olmamakla birlikte genel itibariyle büyük verinin veri yaşam döngüsünde yer alan verilerin toplanıp analiz edilmesi ile oluşan yüksek hacimli veriler olduğu söylenebilir[85]. Büyük veri genellikle verinin gerçek zamanlı olması, farklı kaynaklardan elden edilmesi, büyük hacimli veri kümeleriyle ilgili olması ve kullanımının değer yaratması ile tanımlanmaktadır[86]. Bir çok işletme,

[84] ICO, Guidance on the use of Cloud Computing, s.3,

[85] TEPAV Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, İstanbul Bilgi Üniversitesi, 2014, s.5 https://www.tepav.org.tr/upload/files/1421853130-9.Turkiyede_Kisisel_Verilerin_Korunmasinin_Ekonomik_ve_Hukuki_Analizi.pdf , Erişim tarihi : 04.10.2019

[86] ICO, Big Data, artificial intelligence, machine learning and data protection, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf s.6 Erişim tarihi : 05.10.2019

veri işleme sürecinde büyük hacimli verileri toplayıp, işleyen ve analiz eden teknolojilere sahiptir[87]. Büyük veri uygulamaları, en basit şekilde insan davranışlarının anlaşılıp tahmin edilmek suretiyle yönlendirilmesi için kullanılmaktadır. Büyük veri içerisinde yer alan veriler anonimleştirilse dahi gerçek kişi ile ilişkilendirilebildikleri için kişisel verilerin korunması mevzuatına tabi olmaktadırlar.

Büyük veride çevrim içi platformlar dışında, radyo frekansı ve sensör teknolojisinin artmasıyla çeşitli kaynaklardan anlamlı veya anlamsız veri toplanmaktadır[88]. Büyük veri içerisinde toplanan verilerin bir kısmı, kullanıcı tarafından paylaşılan örneğin alışveriş sitesinden ürün alması, sosyal medyada paylaşım yapılması, sesli mesaj gönderilmesi gibi veri sahibi tarafından bilinen veriler oluştururken bir kısmını ise veri sahibinin haberi dahi olmadan toplanan üçüncü taraf çerezler, CCTV kayıtları, sensörden elde edilen veriler oluşturmaktadır[89].

Mobil uygulamalar, kablosuz ağ, bluetooth gibi çeşitli ağ arayüzleri aracılığı ile aynı kullanıcıya ait olsun olmasın başka akıllı cihazlarla iletişime geçerek veri alışverişi yaptığı[90] gibi cihazda yer alan sensörlerden elde edilen verileri işleyerek veri üretmekte, toplanan bu verilerin değerlendirilmesi sonrasında veriyi yine gerçek zamanlı olarak kullanıcıya ulaştırmaktadırlar. Tüm bu veriler büyük veri alanın içine dâhil olmaktadır. Bu sebeple de mobil uygulamaların, veriyi gerçek zamanlı olarak toplayabilmesinin, değerlendirebilmesinin ve paylaşabilmesinin, büyük verinin oluşturulmasına katkı sağlamasının yanı sıra mobil uygulamalar, büyük verinin hem üreticisi hem de tüketicisi konumuna dönüşmektedirler. Büyük verinin önemi sektörler açısından farklılık göstermekle birlikte genel olarak pazar

[87] Işık, s.178
[88] Şehriban İpek Aşıkoğlu, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Onikilevha Yay, İstanbul, Kasım 2018, s.21
[89] Aşıkoğlu, s.139
[90] EDPS Guidelines On The Protection Of Personal Data Processed By Mobile Applications Provided By European Union Institutions s.3 https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf Erişim tarihi : 05.10.2019

çalışmalarını arttırmak, hizmet iyileştirmek, müşteri bağlılığını sağlamak için kullanılmaktadır.

GVKT'nin başlangıç maddesinin 71. paragrafında "çevrimiçi kredinin otomatik olarak reddedilmesi veya herhangi bir insan dahili olmaksızın e-işe alım uygulamaları" gibi otomatik karar alma mekanizmalarına örnek verilmiştir. GVKT, her ne kadar otomatik karar alma ve profil oluşturma mekanizmalarını engellemiyor olsa da bireylere otomatik karar alma mekanizmalarına tabi olmama hakkı tanınmıştır. GVKT ayrıca veri sorumlulularına profilleme faaliyetleri için uygun matematiksel veya istatistiksel prosedürler hazırlama ve etnik köken, siyasi görüşler, din veya inançlar, sendika üyeliği, genetik veya sağlık durumu veya cinsel yönelim gibi konularda ayrımcılık yapılmasını engelleyici önlemler alma yükümlülüğü getirmektedir[91]. Buna göre veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzeri şekilde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunmaktadır[92]. 6698 sayılı Kanun'da ise bu durum, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonuç çıkmasına itiraz etme hakkı olarak düzenlenmiştir. Büyük veride verinin işleme amacının işlemin sonucu olarak çıkması amaçla sınırlılık ve şeffaflık ilkesine de uygun olmamaktadır.

3.4. MOBİL UYGULAMALARDA İŞLENEN VERİLER VE NİTELİKLERİ

6698 Sayılı Kanun'da kişisel verilere ilişkin genel bir tanım yapılmakla birlikte niteliği itibari ile daha özel koruma gerektiren veriler için 6698 Sayılı Kanunu'nun 6. maddesinde "Özel Nitelikli Kişisel Veriler" olarak ayrı bir veri tanımı yapılmaktadır. Elektronik haberleşme sektöründe yer alan trafik verisi, konum

[91]ICO, Big Data, artificial intelligence, machine learning and data protection, s.21 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Erişim Tarihi : 10.02.2020

[92] Işık, s.179

verisi gibi veri türleri ise herhangi bir kişi ile ilişkilendirildiği ölçüde kişisel veri olarak değerlendirilebilecektir[93].

Elektronik Haberleşme Sektöründe kişisel verilerin işlenmesi, tüketicilerin bu hizmeti almak için işletmecilerle paylaştıkları bilgiler ile bu hizmeti kullanırken üretilen verilerin toplanması, kaydedilmesi, değiştirilmesi, silinmesi ve üçüncü kişilere aktarılmasını içermektedir. E-Gizlilik Tüzüğü taslağının giriş bölümünün 1. maddesinde elektronik haberleşme kavramının içine arama ve internet erişiminin yanı sıra anlık mesaj uygulamaları, e-posta, internet aramaları ve sosyal medya aracılığı ile haberleşme içeriklerinin de girmesi mobil uygulamaların elektronik haberleşme açısından kullanıldığı dikkate alındığında isabetli bir düzenleme olmuştur.

3.4.1. Kişisel Veriler

6698 Sayılı Kanun, GVKT ve diğer uluslararası düzenlemeler birlikte değerlendirildiğinde kişisel veri, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veri"* olarak tanımlanmıştır. Bu şekilde bir tanımlama ile kişisel veri kavramına, kişinin kimlik bilgileri, iletişim bilgileri, fiziksel özellikleri, finans bilgileri, öğrenim durumuna kadar bir çok bilgi girmektedir[94].

6698 sayılı Kanun ile GVKT düzenlemelerinde yer alan kişisel veri tanımında sadece gerçek kişiye ait veriler yer almakta, tüzel kişilere ait veriler, kişisel verilerin korunmasına dahil edilmemektedir. Ancak gerek 2002/58 Sayılı Direktif gerekse EHK ve E-Gizlilik Tüzük taslağında hem gerçek hem de tüzel kişilere ait elektronik haberleşme cihazlarında yer alan ve bu servislerde işlenen her türlü veri gizlilik kapsamına alınarak bu verilerin korunmalarına ilişkin düzenlemeler yapılmıştır.

[93]BTK, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Osman Şahin, Bilişim Uzmanlığı Tezi, Haziran 2011, Ankara s.6 http://afyonluoglu.org/PublicWebFiles/ReportsTR/Uzmanlik_Tez/BTK/siber/2011%20Haziran%20Elektronik%20Haberle%C5%9Fme%20Sekt%C3%B6r%C3%BC%20ve%20Ki%C5%9Fisel%20Veriler.PDF Erişim Tarihi : 08.08.2018

[94]Aşıkoğlu, s.5

Öte yandan tüzel kişilere sağlanan korumanın, 2002/58 Sayılı Direktifin başlangıç bölümünün 12. paragrafında, sadece abone kavramı içinde olan tüzel kişilerle sınırlı olduğu ve bu korumanın o tarihte yürürlükte olan 95/46 Sayılı Direktif'i kapsayacak şekilde yorumlanmayacağı özellikle belirtmiştir[95]. Aynı şekilde direktifin 24. paragrafında, elektronik haberleşme şebekeleri kullanıcılarının terminal ekipmanları ve bu ekipmanlar üzerinde saklanan herhangi bir bilginin kullanıcının korunması gereken özel hayatının bir parçasının olduğunun İnsan Hakları ve Temel özgürlükler hakkındaki Avrupa Konvansiyonunda kabul edildiği belirtilmiş[96] ve sadece kişisel veri değil her türlü verinin korunması amaçlanmıştır.

Madde 29 Çalışma Grubu'nun 02/2013 nolu görüşünde, uygulama geliştirici veya üçüncü kişi tarafından cihaz altyapısı ile harici arayüz aracılığı ile son kullanıcının haberi olmadan eş zamanlı olarak farklı verilerin de cihazda toplanıp işlenebileceği veya aktarılabileceği yer almıştır. Görüşün devamında, bu verilerin herhangi bir kişiyle ilgili olması ve doğrudan veya dolaylı olarak veri sorumlusuna veya üçüncü kişiye karşı belli ve belirlenebilir olması halinde bu verilerin kişisel veri olduğu belirtilmiştir[97]. Dolayısıyla kişisel verilere ilişkin korunmadan yararlanmak için verilerin belli ve belirlenebilir olması en temel kriter olmaktadır.

3.4.2. Özel Nitelikli Kişisel Veriler

6698 Sayılı Kanun'un 6. maddesinde tanımlanan özel nitelikli kişisel veriler, içeriklerinin ifşa edilmesi ile kişinin utanç duymasına, kişisel ve sosyal olarak zarar görmesine ve ekonomik açıdan kayıp yaşamasına neden olma ihtimallerine sahip olmaları nedeniyle daha fazla korunması gereken kişisel verilerdir. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi 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

[95]Aşıkoğlu, s.15
[96]Hayrünnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yay, Ankara, Ekim 2009, s. 247
[97]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.8

verilerinin özel nitelikli kişisel veriler olduğu belirtilmiş ve bu verilerin işlenmesi özel şartlara tabi tutulmuştur. GVKT'de yer alan tanımda; dernek ve vakıf üyelikleri, ceza mahkumiyeti, güvenlik tedbirleri ile kılık kıyafet ile ilgili veriler kapsam dışında tutulmuştur.

Biometrik verilere ilişkin GVKT'de ayrı bir tanım yapılmıştır. Buna göre; biyometrik veri, yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir. GVKT'nün giriş bölümünün 51. paragrafında da biyometrik verilere ilişkin açıklamalara yer verilerek, fotoğrafların işlenmesinin biyometrik veri olarak nitelendirilemeyeceği, sadece verinin o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olduğu ölçüde biyometrik veri olarak kabul edileceğine yer verilmiştir.

6698 Sayılı Kanun'un 6. maddesinin 2. fıkrasında özel nitelikli kişisel verilerin sadece açık rıza ile işlenebileceği düzenlenmiştir. Bu kapsamda veri sahibinin açık rızasının varlığı, özel nitelikli kişisel verilerin sınırsız bir şekilde işlenebileceği anlamına da gelmemektedir. Nitekim Kurul'un spor tesisine giriş esnasında el ve parmak izinin taranması suretiyle kişilerin kimlik doğrulaması yapmasının ölçülülük ilkesi ve veri minimizasyonu ilkelerine aykırı olduğuna ilişkin verdiği kararda; amaç için gerekli olmayan veri işleme faaliyetinden kaçınılması gerektiği, kişinin rızası alınsa dahi rızanın aşırı miktarda veri toplanmasını meşrulaştırmayacağı, benzer şekilde Madde 29 Çalışma Grubu tarafından hazırlanan Biyometrik Teknoloji Geliştirmeleri konulu görüşte yer alan örnekte de spor salonuna sadece üyelerin girişini sağlamak için müşterlerin parmak izinin depolanarak işlenmesi, kulübe erişimi kolaylaştırma ihtiyacı ile orantısız olarak değerlendirildiği bu uygulama yerine daha basit yöntemlerin kullanılarak da aynı ihtiyacın karşılanacağı yer almaktadır[98].

[98] Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Kararı

Özel nitelikli verilerin açık rıza olmaksızın işlenebileceği haller ise maddenin devamında sınırlı olarak sayılmıştır. Bu kapsamda; sağlık ve cinsel hayat dışındaki özel nitelikteki kişisel veriler sadece kanunlarda öngörülen hallerde açık rıza aranmaksızın işlenebilecekken, sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir.

Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler ise Kurul tarafından alınan 31.01.2018 tarih ve 2018/10 sayılı kararda yer almıştır[99].

[99]Kurul'un 31.01.2018 tarih ve 2018/10 sayılı kararı ile Kanunun 22 nci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir: 1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi, 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi, b) Gizlilik sözleşmelerinin yapılması, c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması, ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi, d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması, 3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi, b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması, c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması, ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması, d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması, e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması, 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması, b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi, 5- Özel nitelikli kişisel veriler aktarılacaksa a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması, b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması, c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi, ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir. 6- Yukarıda belirtilen önlemlerin yanı sıra

3.4.2.1.Sağlık Kategorisindeki Mobil Uygulamalar

Kişilerin sağlık durumuna ilişkin bilgi veren veriler, sağlık verisi olarak kabul edilirken kişinin beslenme ve egzersiz alışkanlıkları tek başına sağlık verisi değildir[100]. Ancak bu veriler, belirli bir periyotta ya da kişinin sağlık durumuna ilişkin bir sonuç çıkartmak amacıyla işlendiği takdirde sağlık verisi olarak kabul edilecektir[101].

App Store'da, sağlık kategorisinde yer alan ve sağlıklı yaşam ile ilgili uygulamalara yönelik ek kurallar düzenlenmiştir. Örneğin, uygulamaların, klinik sağlık kayıtları arayüzü, sağlık kiti arayüzü, hareket ve egzersiz, hareket bozukluğu arayüzleri veya sağlıkla ilgili insan denek araştırmaları dahil olmak üzere sağlık ve tıbbi araştırma bağlamında toplanan verileri, veri sahibinin açık rızası alınmak kaydıyla sağlık yönetimini iyileştirme ve sağlık araştırması amacı ile işlenebilirken verilerin bu amaçlar dışında reklam, pazarlama, kullanıcı temelli veri madenciliği amacıyla kullanılması veya üçüncü taraflarla paylaşılması yasaklanmıştır. Bununla birlikte, App Store, bu tarz uygulamalarda sadece kullanıcının kendisine yarar sağlamak için uygulamanın avantaj sağlayan kuruluş tarafından sunulması ve verilerin başka bir üçüncü tarafla paylaşılmaması koşuluyla işlenmesine izin vermiştir. Sigorta şirketinin, kendisi tarafından sunulan mobil uygulamasında kullanıcıya indirimli sigorta primi sağlamak amacıyla kullanıcının sağlık veya egzersiz verilerini işlemesi buna örnek olarak verilebilir. Her halükarda veri sorumlusu uygulama geliştirici, kişisel sağlık bilgilerini iCloud'da saklamayacağı kurallar arasındadır.

App Store'da sağlıkla ilgili denek araştırması yapan uygulamalara ilişkin ayrı kısıtlamalar yer almakta mağaza, uygulama geliştiriciye bu araştırmaya katılan katılımcılara veya reşit olmayanların ebeveyn veya vasilerinden alınacak rızanın

Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.

[100]Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yay, İstanbul 2019 s.111

[101] Dülger, s.111

öncesinde kişilere araştırmanın niteliği, amacı ve süresi; risk ve faydaları; verilerin gizliliği ve işlenmesi hakkında bilgiler, üçüncü taraflarla herhangi bir paylaşım dahil; katılımcı soruları için bir irtibat noktası; ve rızanın geri alınma sürecine ilişkin bilgilendirilme yapmasını şart koşmaktadır. Bu tarz uygulamaların, bağımsız bir etik inceleme kurulundan onay alması gerektiği de ayrıca belirtilmiştir.

Sağlık uygulamaları ile biometrik veri toplayan uygulamalar, biometrik veriler ile sağlık verileri gibi özel nitelikte kişisel veriler işlediği gibi birçok uygulama konum verisi gibi işlendiğinde dolaylı olarak din bilgisi gibi özel nitelikli veri elde edilen veriler de işleyebilmektedir. Nitekim bu verilerin bir araya getirilip kullanıcı profili oluşturulması, kişinin temel haklarına zarar verecek riskleri de beraberinde getirebilmektedir. Bu sebeple mobil uygulamalarda özel nitelikli kişisel verilerin işlenmesi durumunda ilgili ulusal ve uluslararası mevzuat kapsamında yeterli önlemlerin alınması gerekmektedir.

3.4.3. Elektronik Haberleşme Verisi

Elektronik haberleşme sektöründe toplanan ve işlenen kişisel veriler için, yürürlükte bulunan ulusal veya uluslararası mevzuatta herhangi bir özel veri tanımı yapılmamıştır. EHGY'i değiştirecek taslak metin[102] hem elektronik haberleşme verisi tanımı hem de kişisel elektronik haberleşme verisi tanımı yapılmıştır. Aynı şekilde E-Gizlilik Tüzüğü taslağında da ilk kez bu tanıma yer verilmiştir.

BTK tarafından 07.08.2017 tarihinde kamuoyunun görüşüne sunulan taslak EHGY teklifinin tanımlar ve kısaltmalar maddesinin 3. maddesinde Elektronik Haberleşme Verisi, elektronik haberleşme hizmeti alan kişilere ait ses, görüntü, kısa mesaj ve benzeri veriler ile, haberleşmenin takibi ve kaynağının tanımlanması, haberleşmenin sonlandırılacağı noktayı, haberleşmenin tarihi, zamanı ve süresini belirlemek, haberleşmenin türünü, kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için gerekli veriler olarak tanımlanmıştır.

[102]http://www.kbd.org.tr/s/2389/i/KBD_EH-KisiselVeriler-20170807-239-Karar.pdf, Erişim Tarihi : 08.12.2018

Ayrıca aynı maddenin son paragrafında da BTK tarafından gerekli görülmesi halinde bu madde kapsamı dışında da veri kategorilerinin oluşturulacağı düzenlenerek elektronik haberleşme verisi bakımından oldukça kapsamlı ve geniş bir veri tanımı yapılmıştır. Aynı şekilde tanımlar kısmında kişisel elektronik haberleşme verisi tanımı yapılarak kimliği belli veya belirlenebilir gerçek kişiye ilişkin haberleşme verisi, trafik verisi ve konum verisinin bu tanıma girdiği düzenlenmiştir. Bu şekilde de kişisel verilerin özellikli bir tanımı yapılarak kişisel elektronik haberleşme verisi adı altında özel bir veri tanımı yapılması hedeflenmiştir.

Kişisel elektronik haberleşme verisi, sadece gerçek kişilere ait verileri kapsamaktadır. Her ne kadar tüzel kişi adına abonelik ihdas edilse de elektronik haberleşme verisi, trafik verisi ve konum verisinin bu hizmeti alan gerçek kişiye ait olması gerekçesi ile bu veri tanımında tüzel kişi kapsam dışına çıkarılmıştır.

E- Gizlilik Tüzüğü taslağında da 2002/58 Sayılı Direktiften farklı şekilde elektronik haberleşme verisi tanımı yapılmıştır. Bu veri tanımı ise taslağın tanımlar başlıklı 4. maddesinde tanımlanmıştır. Buna göre, elektronik haberleşme verisi, elektronik haberleşme içerik verisi ve elektronik haberleşme meta verisinden oluşmaktadır. Elektronik haberleşme içeriği, elektronik haberleşme hizmetleri sırasında gönderilen veya alınan mesaj, ses, videolar, resimler ve ses verileri gibi veriler olarak tanımlanırken elektronik haberleşme meta verisi ise iletişimin kaynağı ve gönderileceği yeri izlemek ve belirlemek amacıyla kullanılan elektronik haberleşme hizmet sağlayıcıları tarafından sunulan hizmetin içeriğinde cihazda ortaya çıkan ve haberleşmenin tarihi, zamanı, süresi ve haberleşme tipi ile ilgili veriler dahil olmak üzere elektronik haberleşme içeriğinin iletim, dağıtım veya alışverişi amacıyla elektronik haberleşme ağı içerisinde işlenen veriler olarak tanımlanmıştır.

Madde 29 Çalışma Grubu, 01/2017 sayılı görüşünde, E-Gizlilik Tüzüğü taslağının başlangıç bölümünün 4. paragrafında yer alan elektronik haberleşme verisinin kişisel veri içerebileceği ifadesini eleştirmiş bu verilerin büyük kısmında kişisel

veri olduğu gibi özel nitelikte olan veriler de bulunduğu bu sebeple paragraftaki ifadenin verilerin kişisel veri içerebileceği şeklinde değil verilerin genellikle kişisel veri olduğu şeklinde düzeltilmesi gerektiğini belirtmiştir[103]. Nitekim EHGY'in taslak metninin kamuoyuna sunulan değişiklik teklifinde kişisel elektronik haberleşme verisi tanımı yapılarak daha sağlıklı bir tanım yapılmıştır. Yönetmeliğin yürürlüğe girmesiyle bu tanım, taslak tüzük bakımından ülkemiz açısından da olsa Madde 29 Çalışma Grubu'nun endişelerini gidermiş olacaktır.

3.4.3.1. Elektronik Haberleşme Metaverisi

Elektronik haberleşme metaverisi, E-Gizlilik Tüzüğü taslağının 4. maddesinin c bendinde tanımlanmıştır. Buna göre elektronik haberleşme metaverisi; iletişimin kaynağı ve gönderileceği yeri izlemek ve belirlemek amacıyla kullanılan veriler, elektronik haberleşme hizmet sağlayıcıları tarafından sunulan hizmet içeriğinde cihazda ortaya çıkan ve haberleşmenin tarihi, zamanı, süresi ve haberleşme tipi ile ilgili veriler dahil olmak üzere elektronik haberleşme içeriğinin iletim, dağıtım veya alışverişi amacıyla elektronik haberleşme ağı içerisinde işlenen verilerdir.

Ancak bu çok dar bir tanımdır. Özellikle yukarıda tanımlanan verilerin elektronik haberleşme ağı tarafından işlenmesi ile sınırlı tutulması ile OTT servisi[104] tarafından işlenen veriler kapsam dışına bırakılmaktadır. Madde 29 Çalışma Grubu 01/2017 sayılı görüşünde, metaveri tanımının tüm işlenen veriler olarak değiştirilmesi gerektiğini belirtmiştir[105].

E-Gizlilik Tüzüğü taslağının 6. maddesinde metaveri ve elektronik haberleşme içeriği ile ilgili farklı seviyede korumalar öngörülmüştür. Madde 29 Çalışma Grubu

[103]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.27

[104]BEREC (Body of European Regulators for Electronic Communications) 2016 Ocak tarihli OTT Hizmetleri ile ilgili raporunda, OTT Hizmetlerini "internet şebekesi üzerinden son kullanıcıya sunulan içerik veya servis veya uygulama" olarak tanımlamaktadır. OTT, belli bir hizmeti değil bir tedarik metodu olarak internet şebekesi üzerinden bir tedarik hizmeti sunmaktadır. Örnek olarak; Viber, Skype, Tango, Whats app gibi uygulamalar üzerinden ve internet şebekesi üzerinden veri iletimine imkan sağlayarak ses, sms/mms ve görüntü hizmeti sunulması.

[105]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.16

01/2017 sayılı görüşünde bu madde ile ilgili ayrıntılı değerlendirme yaparak her iki kategorideki verilerin de hassas nitelikte olduklarından bu ayrımı desteklememekte ve bu iki veri çeşidinin de aynı koruma seviyesine sahip olmaları gerektiği görüşünü savunmaktadır. Hem metaverinin hem de içerik verilerinin alıcı ve gönderici olan son kullanıcıların rızası olmadan işlenmemesi gerektiği de tekrar vurgulanmıştır. Amaçla bağlı olarak değişmekle birlikte eğer sadece o amaç için gerekli ve elzemse bazı veri işlemelerin rıza aranmaksızın gerçekleştirilmesine izin verilmiştir. Örneğin hizmet sağlayıcıların elektronik haberleşme verilerini hem metaveri hem de içerik verisini haberleşmenin iletimini sağlamak için gerektirmesi ve gereklilik süresi boyunca bu amaçla ve elektronik haberleşme ağları ve servislerinin güvenliğini sağlama ve düzeltme için gerekli olması veya haberleşmenin iletiminde teknik arıza veya hataların tespiti için gerektirdiği süre boyunca işleyebileceklerini düzenlenmiştir. Metaverinin elektronik haberleşme hizmetlerinin faturalandırma, ara bağlantı ödeme hesaplaması, dolandırıcılığın veya herhangi bir istismar durumunun tespiti ve durdurulması halleri veya abonelik işlemleri için gerekli olması halinde işlenebileceği düzenlenmiştir.

Madde 29 Çalışma Grubu 01/2017 sayılı görüşünde, kullanıcı tarafından özellikle talep edilen örneğin arama veya anahtar kelime indeksleme işlevselliği, sanal asistan, konuşma metni motorları ve çeviri gibi hizmetlerin kullanıcıya sunulması amacıyla elektronik haberleşme verilerinin işlenmesinin mümkün hale getirilmesini önermektedir. Görüşün devamında bu kullanımın, sadece hanehalkı ve kişinin işle ilgili kullanımı ile ilgili verilerin analiz edilmesi açısından tüzüğün kapsamı dışına bırakılmasını tavsiye etmektedir[106].

3.4.3.2. Konum Verileri

Konum verisi, EHGY'in tanımlar ve kısaltmalar başlıklı 3. maddesinde, "*kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme aracılığı ile işlenen belirli veri"* olarak tanımlanmıştır. 2002/58 Sayılı Direktif'in

[106]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.13

2. maddesinin c bendinde de benzer şekilde tanmlanmıştır. Ancak bu tanımlar mobil uygulamalarda işlenen konum verileri açısından yetersiz kalmakta, uygulamanın kullanımı için gerekli olan veya gerekli olmasa dahi farklı amaçlarla işlenen konum verilerine ilişkin korumayı açıkta bırakmaktadır.

E-Gizlilik Tüzüğü taslağının başlangıç kısmının 17. paragrafında, elektronik haberleşme hizmetleri kapsamında olmayan konum verilerinden bahsedilmiş ancak bu verilerin akıllı cihazlardaki GPS işlevselliğindeki verileri kullanan uygulamalar yoluyla toplanan konum verileri, kablosuz ağ sinyali ile oluşturulan konum verileri, navigasyon asistanları üzerinden toplanan konum verileri veya başka yollarla üretilen konum verileri olup olmadığı tam olarak açıklanmamıştır.

Ayrıca konum verileri her ne kadar özel nitelikli kişisel veri kategorisinde yer almasa da bu veri ile örneğin sürekli belli dönemlerde ibadethaneye gidilmesi ile dolaylı olarak özel nitelikli kişisel veri işlenmesi mümkün olabilmektedir.

3.4.3.2.1 Konum Verilerinin İşlenmesi

2002/58 Sayılı Direktif'in ,9. maddesinin 1. bendinde; konum verilerinin yalnızca anonimleştirildikleri veya katma değerli hizmetin sunulması için gerekli ölçüde ve süre ile sınırlı olarak abone veya kullanıcıların rızası ile işlenebilecekleri ifade edilmiştir[107].

EHK'nun 51. maddesinin 8. fıkrasına göre, işletmeciler, konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlamak zorundadırlar. Aynı fıkranın devamında trafik ve konum verileri ile kişisel verilerin abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebileceği de hüküm altına alınmıştır.

Veri sorumluları, sadece belli hallerin varlığında örneğin belirli konumdaki müşterilerin sayısı istatiksel olarak hesaplanırken veya bekleme süresinin

[107] Ayözger, s.157

görüntülenmesi için ilgili kişinin rızası olmaksızın konum verisi işleyebilir. Diğer yanda işlenen konum verisi her ne kadar istatistik amaçlarıyla kullanılıyorsa da bu bilgi ile kişilerin konum bilgileri ile davranışsal alışkanlıkları ortaya çıkarılmaktadır. Bazı durumlarda örneğin ibadethaneler veya sağlık merkezlerine gidildiğinde buradaki konum bilgisi ile özel nitelikli kişisel veri bilgisini açığa çıkabildiğinden bu ayrımın doğru bir şekilde yapılması önem arz etmektedir.

Bununla birlikte, her iki örnekte de, istatistiksel amaç yerine getirildiğinde verilerin silinmesi veya anonim hale getirilmesi gerekecektir. Mağaza gibi belirli bir konuma gelen ziyaretçilerin cihazlarının MAC adresleri cihazlara kalıcı bir şekilde depolanmadan derhal anonimleştirilmeli ve teknik olarak yeniden tanımlanabilme olanağının devre dışı bırakılması gerekmektedir.

Kullanıcıların, elektronik haberleşme servis sağlayıcıları tarafından iletişimin kullanıcıya aktarılması için veya navigasyon hizmetinden yararlanmak için gerekli konum verilerinin işlenmesini reddetme imkanları bulunmamaktadır. Madde 29 Çalışma Grubu'nun akıllı chazlardaki konum hizmetlerine ilişkin görüşünde, akıllı cihazlarda kural olarak konum verilerini işleyen servislerin kapalı olması ve her işleme faaliyetinde açık rıza alınması gerektiği tavsiye edilmiştir[108].

RFID[109] veya diğer teknolojilerle kişinin açık rızası veya yargı kararı olmadan konumunun izlenmesi bazı ülkelerde yasaklanmıştır[110]. Şirket tarafından çalışanlara tahsis edilen veya iş için kullanılması gereken araç izleme cihazlarında yer alan uygulama aracılığıyla konum verisinin işlenmesi de çalışan davranışlarının izlenmesi anlamına geldiğinden bu faaliyet öncesi mutlaka veri koruma etki analizi ve denge testi yapılması, çalışanların bu konuda aydınlatılması, her halükarda çalışanın özel kullanımına tahsis edilen araçlarda çalışanın kontrol edebileceği bir

[108]Madde 29 Çalışma Grubu'nun 16 Mayıs 2011 tarih ve 13/2011 sayılı "Akıllı mobil cihazlarda coğrafi konum hizmetleri" hakkındaki görüşü, s.16

[109] Radyo Frekansı ile Tanımlama teknolojisi, radyo frekansı kullanarak nesneleri tekil ve otomatik olarak tanıma yöntemidir.

[110] Determan s.184

gizlilik yöntemi belirlenerek izleme faaliyetinin mesai saatleri dışında durdurulmasına imkan verilmelidir..

3.4.3.3. Trafik Verileri

EHGY, 2002/58 Sayılı Direktifte düzenlenen trafik verileri tanımını almış ve trafik verilerini, "*bir elektronik haberleşme şebekesi üzerinden haberleşmenin iletilmesi veya bunun faturalandırılması amacıyla işlenmiş her türlü veri"* olarak tanımlamıştır. Bu anlamda haberleşmenin yapılması amacıyla bir mobil telefonun abonesi tarafından yapılan aramanın tarih ve saatine ilişkin veriler, trafik verisidir[111]. Trafik verileri ile elektronik haberleşmenin ne kadar sürdüğü, elektronik haberleşme ağına zarar veren durumların ve bu durumlarda işletmecinin kim olduğunun tespiti yapılabilmektedir.

EHK 51. maddesinin 7. fıkrasında trafik verilerinin; trafiğin yönetimi, ara bağlantı, faturalama, usulsüzlük, dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile ara bağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işleneceği ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanacağı düzenlenmiştir. Aynı maddenin devamında trafik verileri ile konum verilerinin açık rıza ile veya anonim hale getirilerek katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenebileceği düzenlenmektedir.

[111] Öngün, A. Çiğdem Ayözger Öngün, Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, Beta Yay, İstanbul, Ocak 2019, s.162,

3.5. MOBİL UYGULAMALARDA VERİ SORUMLUSU VE VERİ İŞLEYEN KAVRAMI VE SORUMLULUKLARI

3.5.1. Veri Sorumlusu

Veri Sorumlusu, 6698 Sayılı Kanunun 3.maddesinin 1. bendinde kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. 6698 Sayılı Kanunun veri güvenliğine ilişkin yükümlülükleri düzenleyen 12. maddesinde de veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu düzenlenmiştir.

Veri sorumlusu, gerek 6698 Sayılı Kanun gerekse GVKT 5. maddesinde yer alan ilkeler doğrultusunda veri işlemenin dışında ayrıca tasarımla veri koruma ve varsayılan olarak veri koruma konusunda gerekli tedbirlerin alınması ve mevzuata uygun veri işlemenin gerçekleştirilmesi bakımından sorumludur.

Özellikle gelişen teknoloji ile kişi hak ve özgürlükleri bakımından önemli tehlikeler meydana getiren veri işleme faaliyetlerinde veri sorumlusu kişisel verilerin işlenmesine ilişkin etkin değerlendirme yapmak durumundadır. GVKT 35.maddesinde düzenlenen veri koruma etki analizi ile öngörülen veri işleme faaliyetinin güvenlik önlemleri de dahil sistemli bir şekilde açıklanarak veri işlemenin gerekliliği ve amacı ile orantılı bir değerlendirme yapılması ve verisi işlenen kişinin hakkının korunmasına yönelik önlemlerin alınması gereklidir. Ayrıca GVKT'dan farklı olarak 6698 Sayılı Kanun'un 16. maddesinin 2. fıkrasına göre veri sorumluları, veri sorumluları siciline kaydolmak zorundadır.

Mobil uygulamalarda da veri sorumlusu, mobil uygulama ile hangi verilerin toplanacağını, verilerin toplanma amacını, kimlere ait verilerin toplanacağını, toplanan verilerin paylaşılıp paylaşılmayacağını, paylaşılacaksa kimlerle paylaşılacağını, verilerin ne kadar süre ile saklanacağı ve veri sahiplerinin sahip

olduğu haklarını ne şekilde kullanacakları konusunda karar verme yetkisine sahip olan kişiler olarak tanımlanmaktadır. Veri sorumlusu bazı konularda karar alma yetkisini veri işleyene de bırakabilmektedir. Bu durumda uygulama geliştirici veri sorumlusu olabileceği gibi uygulama geliştiriciye bu şekilde hizmet vermesi yönünde talimatta bulunan esas uygulama sahibi kişi, kuruluşlar da veri sorumlusu olabilecektir.

3.5.2. Veri İşleyen

Veri işleyen, 6698 sayılı kanunun 3.maddesinin ğ. bendinde veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır. Ayrıca bir gerçek veya tüzel kişi aynı anda hem veri sorumlusu hem de veri işleyen olabilmektedir[112]. 6698 sayılı Kanun gerekçesinde veri işleyenin, veri sorumlusu tarafından verilen talimatlar çerçevesinde kişisel verileri işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı gerçek veya tüzel kişiler de olabileceği ifade edilmektedir 6698 Sayılı Kanun'un 12. maddesinin 2. fıkrasında veri sorumlusunun veri işleyenlerle birlikte müştereken sorumlu olduğu düzenlenmiştir. GVKT'de veri koruma hukukundan sorumlulukları bakımından veri sorumlusu ile birlikte sorumlu tutmuştur. GVKT'de de veri işleyenler veri sorumlusu ile birlikte gerekli tedbirleri almakla yükümlü kılınmış ve kendilerine veri ihlallerinde bildirim yükümlülüğü yüklemiştir. Veri Sorumlusu ile veri işleyen arasındaki ilişkinin sınırları ve kapsamının belirlendiği üzere yazılı bir sözleşme yapılması gerekmektedir[113].

Uygulama geliştiriciler bazı durumlarda veri sorumlusu sıfatıyla hareket ederken bazı durumlarda veri işleyen olarak hareket etmektedirler. Örneğin mobil uygulama ihtiyacı olan herhangi bir işletme, bu yazılımın hazırlanması için sözleşme ile başka bir işletmeden yazılım hizmeti alabilir. Bu durumda uygulama yazılımı yapan kişi uygulama içinde gerekli teknik iyileştirme ve güncellemelerin yapmak için ilgili veri sorumlusu adına ve onun talimatları ile veri işlediğinde veri işleyen olarak

[112] Taştan, s.68
[113] Aşıkoğlu, s73, Lambert, s.238

hareket eder. Diğer yanda uygulama yazılımını geliştiren kişi ile uygulama sahibinin aynı olduğu durumda uygulama geliştirici veri sorumlusu olarak kabul edilecektir. Dolayısıyla veri sorumlusu ve veri işleyen ayrımının her bir uygulama açısından ayrı ayrı değerlendirilmesi gerektiği açıktır.

3.5.3. İşletim Sistemi ve Cihaz üreticileri

İşletim sistemi ve cihaz üreticileri, öncelikli olarak mobil cihazın daha rahat ve kolay çalışması veya işletim sisteminin güvenliği, cihazın işlevlerini yerine getirmesi gibi sebeplerle kendi amaçları doğrultusunda kişisel veri işlediği ölçüde veri sorumlusu olarak kabul edilecektir. Herhangi bir uygulama cihazın konum bilgisine ulaşılmak istendiğinde uygulama, cihazın işletim sistemini kullanmak zorundadır. İşletim sisteminin buna izin vermesi için de kişisel veriyi toplaması şarttır. Başka bir örnek ise işletim sisteminin kendi bileşenlerini güncellemek adına kişisel veri işlemesidir. İşletim sistemi ve cihaz üreticileri, araçlar, ayarlar ve başvuru materyalleri oluşturma konusunda minimum standartları ve uygulama geliştiriciler arasındaki en iyi pratikleri belirlemek konusunda önemli bir yere sahiptirler.

Uygulamalar tarafından kişisel veriye erişim ve işleme faaliyeti, arayüz yazılım hazırlama sınıfları, uygun kontroller ve güvenlik koruma metotları ile yönetilmektedir. İşletim Sistemi ve cihaz üreticileri, kişisel veriye erişime izin veren metot ve fonksiyonların birbirinden ayrı rıza talepleri içermeyi amaçlayan özelliklerin dâhil olduğundan emin olmalıdır. Aynı şekilde kişisel veriye erişimi hariç tutmak veya limitlemek için düşük seviye fonksiyonları veya üstün gelen kontroller ve güvenlik korumalarını arayüze dahil edecek aksiyonlar almalı, cihaz içine açık denetleme izi geliştirmeli, böylelikle son kullanıcılar açık bir şekilde hangi uygulamanın kendi kişisel verilerine eriştiklerini görebiliyor olmalılardır.

Mobil uygulama sektöründe yer alan aktörlerin hepsi güvenlik açığına yakalanmadan önce zamanında güvenlik zafiyetine cevap verecek tedbirleri almalıdır. İşletim sistemi ve cihaz üreticileri uygulama geliştiricilerle birlikte son kullanıcılara düzenli güvenlik güncellemeleri hakkında ne kadar bir zaman

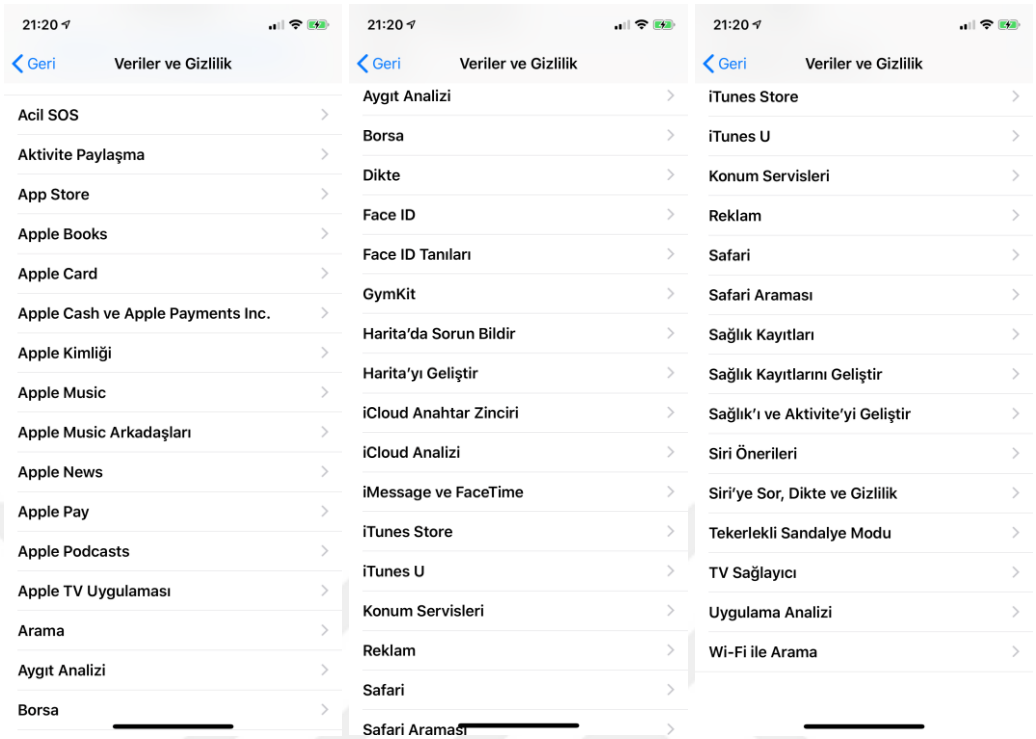
bekleyecekleri hakkında ön bilgi sunmalı ayrıca güvenlik konusunda yapılacak bir düzeltme için güncelleme gerekiyorsa bu konuda kullanıcılara hemen bilgi vermelidirler.

Çalışmanın ilk bölümünde mobil cihazlarda yaygın şekilde kullanılan işletim sistemlerinin Android ve IOS işletim sistemi olduğundan bahsedilmiştir.

Android işletim sistemi, farklı markalara ait mobil cihazlarda kullanılmakta iken, IOS işletim sistemi ise sadece Apple marka cihazlarda kullanılmaktadır.

Android işletim sistemi kullanan cihazın ayarlar ve gizlilik sekmesinde cihaz sahibi markanın işlediği verilerin işlenmesine ilişkin bilgilendirme, ayrı bir gizlilik politikası ile sunulurken, Google şirketine ait Android işletim sistemi ve Google Play mağazası ise tüm veri işleme faaliyetlerine yer veren tek bir gizlilik politikasına referans yapmaktadır. Bu şekilde torba bir bilgilendirme ise verinin toplandığı her kanalda veri sahibine bilgilendirme yapılması kuralına aykırılık teşkil etmektedir. IOS işletim sisteminin uygulama mağazası ise App Store'dur. Bu durumda cihaz ve işletim sistemi üreticisi ve uygulama mağazası tek bir veri sorumlusu tarafından yönetilmektedir.

Apple marka cihazlarda, işletim sistemine ait uygulamaların kullanıcıların hangi kişisel verilerinin hangi amaçlarla nasıl işlendiği hakkında bilgilendirme metinleri, cihazın gizlilik ayarlarında alfabetik olarak ayrı ayrı kullanıcının incelenmesine sunulmuş olup ilgili sayfalara erişildiğinde ise ayrıca Apple markasının genel gizlilik politikasına da atıf yapılmaktadır.



Şekil 3.1. Apple Marka Cihazlarda, İşletim Sistemine Ait Uygulamaların Kullanıcıların Hangi Kişisel Verilerinin Hangi Amaçlarla Nasıl İşlendiği Hakkında Bilgilendirme Metinleri

Örnek olarak Apple Kimliği'ne ilişkin bilgilendirme metnine tıklandığında, metinde bu uygulamanın işlevi hakkında bilgi verildiği, cihazda yer alan rehber, takvim, fotoğraf, belge, sağlık ve aktivite ve diğer uygulama verilerini içeren belirli verilerin kullanıcı adına saklanıp yedeklenmesi için Apple ile paylaşıldığı, daha iyi hizmet ve destek sağlamak amacıyla Apple kimliği ile ilişkilendirildiği, bu kimlik ile Icloud, App Store, Itunes store, Imessage ve Facetime gibi Apple servislerine ve tüm aygıtlar ile ağ üzerindeki içeriklere erişmek için kullanıldığı gibi bilgiler yer almaktadır. Metnin devamında hizmetin işlevi, verilerin hangi amaçla işlendiği gibi bilgiler yer almaktadır.

3.5.4. Uygulama Mağazaları

Uygulama mağazaları, uygulama geliştiricileri tasarladıkları uygulama yazılımlarında hangi bilginin ne şekilde ve hangi amaçlarla işleneceğine ilişkin

kuralları belirlemeleri için yönlendirdikleri gibi özellikle Apple Kimliği ve Google hesabı gibi mağazalarda hesap oluştururken kişisel veri işlerler. Uygulama mağazaları hangi verilerin işleneceğini ve veri işleme amaçlarını belirledikleri doğrultuda veri sorumlusudurlar.

Apple Store'un mobil cihazda yer alan kişisel verilerin işlenmesine ilişkin kullanıcılara yönelik hazırlanan bilgilendirme metni incelendiğinde;

1) kişisel bilgilerin mağazadan satın alınan, indirilen veya güncellenmesi istenen içerikleri sağlamak amacıyla,

2) hesap bilgilerinin özelleştirilmiş reklam, kişiselleştirilmiş öneriler sunmak amacıyla,

3) gelen ve giden telefon aramaları ile e-postaların yaklaşık sayısı, cihazın nasıl kullanıldığı bilgilerinin, dolandırıcılığı belirleme ve önlemek amacıyla,

4) satın alınan ve indirilen uygulama bilgilerinin mağazayı geliştirmek adına işlendiği,

reklam ve kişiselleştirilmiş önerileri almak istemeyen kullanıcılar için opt-out seçeneklerinin sunulduğu, hangi durumlarda hangi kategorideki verilerin üçüncü taraflarla paylaşıldığı toplanan verilerin ne kadar süre ile saklandığı gibi bilgiler yer almaktadır.

Diğer yandan uygulama mağazalarının mağazalarında kabul ettikleri uygulamalar açısından da sorumlulukları vardır. Özellikle App Store, her uygulamayı mağazasına kabul etmediği gibi mağazasına kabul edeceği uygulamalar için detaylı bir inceleme süreci başlatmaktadır. Ayrıca her iki mağazanın da uygulama geliştiricilere yönelik hazırladıkları politikalar mevcut olup bu politikaları kendi internet sitelerinde yayınlamaktadırlar.

3.5.5. Mobil Uygulama Geliştiriciler

Mobil uygulama geliştiriciler, mobil cihazlar için uygulama yazılımı hazırlayıp, geliştiren yazılımcılardır. Uygulama geliştirici, mobil uygulama yazılımını kendi adına hazırlayıp, kişisel verileri kendi amaçları doğrultusunda işlediği bir senaryoda veri sorumlusu iken uygulamayı başka bir veri sorumlusu adına hazırlayıp veriyi başkası adına işlediği, verinin işlenme amaçlarını belirlemediği bir durumda ise veri işleyen sıfatına haiz olacaktır.

Bu iki durumda da uygulama geliştirici uygulamasını kullanıcılarla buluşturmak istediği platformun belirlediği kurallara uymak zorunda olduğu gibi uygulamasını en başından itibaren tasarımla veri koruma prensibi çerçevesinde hazırlamalıdır.

3.5.5.1. Uygulama Mağazaları Gereklilikleri

Uygulama geliştiriciler, uygulamalarını Google Play veya App Store'da yer almasını istediklerinde mağazaların belirlediği kriterleri karşılamaları gerektiği gibi uygulamanın kişisel verilerin korunması mevzuatına uyumlu olması da uygulamaların mağazalara kabul sürecinde önemli bir rol oynamaktadır[114]. Google, 2017 yılında Gizlilik Politikası bulunmayan uygulamaları, Google Play Store'dan kaldıracaklarını açıklamış[115], App Store ise 2018 yılında, mağazada yer almak isteyen uygulamaların gizlilik politikası sunmalarını, mağazada yer alan mevcut uygulamalar açısından ise gizlilik politikalarını güncellemelerini zorunlu tutmuştur.

Apple'ın internet sitesinde, App Store'da yer alan uygulamalara ilişkin gizlilik kriterlerinden birkaçından bahsedilmiştir[116]. Bunlar; gizlilik kurallarının

[114]Pedro, Filipa Carmo, Privacy in the Smartphone Age A study on the privacy and data protection risks and violations of mobile applications, Master thesis in Law and Technology, s. 11 http://arno.uvt.nl/show.cgi?fid=142089 Erişim tarihi :05.10.2019

[115] ENISA, Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR, s.19

[116] Apple, uygulama yazılımcı topluluğu için Apple Developer isimli yeni bir mobil uygulama ortaya koyarak, uygulamada, etkinlik haberlerinin yanı sıra tasarım ve teknik konular hakkında makaleler, videolar, yazılım haberleri ve güncellemeler gibi önemli kaynaklara da yer verilecek. Bunların yanı sıra uygulamanın, yazılımcıların Apple Developer programına kaydolması ve üyeliğini sürdürmesi için de bir yöntem olarak sunulmuştur.

ihlal edildiği fark edilen bir uygulamada, uygulama geliştiricinin sorunu gidermesinin zorunlu kılındığı, sorun giderilmediği takdirde uygulamanın App Store'dan çıkarıldığı, cihaza yüklenen uygulamaların verilere erişim için izin almasının zorunlu tutulduğu ve bu izinlerin kullanıcı tarafından değiştirilebildiği bir yapının kurulduğu, işletim sisteminin yeni sürümlerinde konum verisine yalnızca uygulamanın kullanıldığı zaman erişilebileceği, uygulamaların cihazda bulunan belli başlı veri türlerine erişilemeyeceği ve her halükarda uygulamanın cihazdaki verilerin tümüne tam erişim istemesinin mümkün olmadığıdır[117]. Bu noktada uygulama mağazasının gizlilikle ilgili olarak veri erişiminde sadece belli kriterlere sahip uygulamaları mağazasına kabul ettiğini, uygulamaların cihazdaki verilere erişimini kullanıcı iznine tabi tuttuğu ve hiçbir şekilde tüm verilere erişime izin vermediği anlaşılmaktadır.

Apple'ın internet sitesinde uygulama geliştiriciler için teknik gereklilikler, testler[118], programlama rehberi, işletim sistemi saklama rehberi, tasarım rehberi, marka ve pazarlama rehberleri gibi geliştiricilerin incelemesine sunulan rehber ve bilgilendirmeler yer almaktadır. Başvurudan önce uygulama geliştiricilerin güvenlik, performans, işletim, tasarım, hukuki başlıklar altında yer alan diğer gereklilikleri de tamamlamaları beklenmektedir[119].

Google Play uygulama geliştirici politikasında yer alan gereklilikler ise kullanıcı verisi, izinler, cihaz ve ağ suistimali, kötü niyetli davranış, yanıltıcı davranış, yanlış sunum başlıkları altında yer almaktadır[120].

Uygulama geliştirici, bir uygulama yazılımı tasarlamadan önce verinin nerede saklanacağı kararını vermelidir. Bazı durumlarda kullanıcının verisi mobil cihazda saklanmakta iken bazı durumlarda veriler başka bir sunucuda da

https://webrazzi.com/2019/11/19/apple-yazilimci-toplulugu-icin-yeni-bir-mobil-uygulama-yayinladi/ Erişim Tarihi : 08.12.2019

[117] https://www.apple.com/tr/privacy/features/ Erişim Tarihi : 08.02.2020

[118] https://developer.apple.com/app-store/review/guidelines/#before-you-submit Erişim Tarihi : 08.02.2020

[119] https://developer.apple.com/app-store/review/guidelines Erişim Tarihi : 08.02.2020

[120] https://developer.apple.com/app-store/review/guidelines/#data-collection-and-storage Erişim Tarihi : 08.02.2020

saklanabilmektedir. Bu durumda kişisel veriler, hizmet sağlayıcının sistemine aktarılıyor veya kopyalanıyordur. Cihaz üzerinde depolama ve işleme, son kullanıcının verisini kontrol etmesi açısında büyük bir avantaj sağladığı gibi cihaz dışında veri depolanması ise cihazın çalınması veya kayıp olması halinde bilgilerin geri getirilmesi bakımında önemli olmaktadır[121].

Uygulama geliştirici, her iki mağazanın kriterlerinden de anlaşılacağı gibi, kişisel veri korunması ihlalleri konusunda mevzuatla uyumlu gerekliliklere uygun hareket etmeli ve kullanıcıları uyarıcı tedbirleri aktif bir şekilde almalıdır. Madde 29 Çalışma Grubu'nun 02/2013 sayılı görüşünde uygulama geliştiricilerin kişisel verilerin korunması bakımından hangi tedbirleri alarak nasıl hareket etmesi gerektiğine ilişkin yönlendirmeler yer almaktadır. Bunlardan bazıları; kötü niyetli uygulamaların yayılmasını engelleyici, uygulamanın kolaylıkla cihaza yüklenmesi veya kaldırılmasının yapılabileceği güvenlik dostu platformlar tasarlamak[122], verinin istem dışı transferlerine ilişkin uygulama kontrollerini yapmak, etkin güvenlik yama yönetimi stratejisi belirlemek, düzenli güvenlik sistemi denetimleri yapmak, uygulamanın sadece kullanıcıya düzgün bir şekilde ulaşmasına yardımcı olarak kadar veriye erişime izin vermek, varsayılan ayarlarla veri koruması ilkesini prensip olarak belirlemek, kişisel verilere yetkisiz erişimi hem aktarım hem de saklama aşamasında koruyacak önlemleri almaktır.

Bu noktada uygulama geliştiricilerin, kullanıcı kimliği tespiti ve doğrulama onayına ilişkin kullanacakları metotları dikkatli bir şekilde seçmeleri gerekir. Cihaza endeksli belirleyiciler yerine geçici cihaz belirleyici kullanarak mobil uygulama tasarım aşamasında IMEI ve MAC adresleri gibi bir kişiye belirlenebilir özel belirleyiciler yerine rastgele GUI[123] belirleyiciler üretmeli ve bu GUI belirleyiciler ile de herhangi bir cihazla ililişkilendirilme sağlanmamalıdır[124]. Uygulama

[121] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü

[122] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüş

[123]Graphical User Interface.

[124]Mangset, Peder Lind Mangset, Analysis of Mobile Application's Compliance with the General Data Protection Regulation (GDPR), 2018, s.15,

geliştiriciler kullanıcı doğrulaması yapılırken kullanıcı adı ve şifre yönetimine özel önem vermeli ve gizlilik dostu kullanıcı doğrulama mekanizmaları dikkate almalıdır.

3.5.5.2. Veri Kullanımı ve Veri Erişimi

Her iki mağazanın kişisel verilerin gizliliğine ilişkin belirledikleri standartlar ve hukuki gereklilikler karşılaştırıldığında; Google Play ve App Store, uygulamaların kullanıcıların uygulamayı indirmeden önce inceleyebilecekleri ve uygulama içinde kolayca erişilebilecek bir alanda gizlilik politikasına yer vermelerini şart koştuğu anlaşılacaktır. App Store, geliştiricilerin hazırladıkları gizlilik politikasında veri saklama, silme politikasına, kullanıcı tarafından verilen açık rızanın geri alınma yöntemine yer verilmesini de belirtmişken Google Play politika içeriğini bu ölçekte detaylandırmamıştır.

Uygulamaların cihazda yer alan veri ve sensörlere erişim izinlerine ilişkin ayrıntılı açıklama, her iki mağazanın ilgili politikasında yer almaktadır. Google Play, kişisel veri olarak nitelendirilmeyen veya gizlilik politikasında yer almayan verilere erişilmesini de ihlal olarak değerlendirmekte uygulamanın amaçları dışında her hangi bir veriye erişmeyecek yapı kurgulamasını talep etmektedir. App Store'un belirlediği kurallar çerçevesinde uygulama, kullanıcıdan erişim izni almadan önce veriye neden erişmek istediğini açıklayacak, kullanıcının verdiği erişim iznini geri almak için kolay erişilebilir bir yöntem belirleyecek, kullanıcıları gereksiz veri erişimine izin vermeye zorlamayacak, izin vermeyen kullanıcı için "örneğin, bir kullanıcının konum paylaşmayı reddetmesi karşısında manuel olarak adres girme olanağı sunulması" gibi alternatif çözümler sağlayacaktır[125].

Apple internet sitesinde uygulama izin erişimlerinin[126] nasıl olmasın gerektiğine ilişkin sistemin izin isteği uyarısı için özel metin hazırlanması ve metnin kısa ve

https://pdfs.semanticscholar.org/d91a/38b5e24177a0b24c184b9c8b4a14ec99eb5e.pdf, Erişim Tarihi : 10.10.2019

[125] https://developer.apple.com/app-store/review/guidelines/#legal Erişim Tarihi : 08.02.2020

[126]https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy/requesting_access_to_protected_resources Erişim Tarihi : 08.02.2020

açık olması, insanların kendilerini baskı altında hissetmeyeceği bir üslupta olması gerektiği belirtilmiştir[127].

Tablo 3.1. Apple İnternet Sitesinde Uygulama İzin Erişimleri

Doğru	Uygulama, gece boyunca horlama sesleri tespit etmek için sesinizi kaydeder.
Yanlış	Daha iyi bir deneyim için mikrofon erişimi gerekir.
Yanlış	Mikrofon erişimini açın.

3.5.5.3. Kullanıcı Tarafından Oluşturulan İçerik

Kullanıcı tarafından içerik oluşturma, uygulamaların kullanıcıları tarafından video, görsel veya metin içeriklerini uygulamaya ait platformlarda kendi istekleri doğrultusunda yayınlamaları anlamına gelmektedir. Bu içeriğe sahip uygulamalar, içeriğin kullanıcı tarafından rastgele oluşturulduğu göz önüne alındığında fikri mülkiyet ihlali, şiddet, hakaret, tehdit gibi çeşitli riskleri de beraberinde getirmektedir. Bu içeriklerin kötüye kullanımını önlemek için, kullanıcı tarafından oluşturulan içeriğe veya sosyal ağ hizmetlerine sahip uygulamaların içermesi gereken unsurlar uygulama mağazaları politikasında belirtilmiştir. Bunlardan bazıları, sakıncalı içeriğin uygulamaya gönderilmesini filtrelemek için bir yöntem belirlenmesi, rahatsız edici içeriklerin bildirilmesine ilişkin şikayet mekanizması, ilgili kullanıcıları hizmetten engelleme imkanı, kullanıcıların uygulama geliştiriciye kolayca ulaşabilmesi iletişim bilgilerinin yayınlanmasıdır.

3.5.5.4. Çocuklara Yönelik Uygulamalar

6698 Sayılı Kanun'da çocuklara ait kişisel verilerin korunmasına ilişkin özel düzenlemeler mevcut değilse de GVKT'de çocuk verilerinin işlenmesine ilişkin

[127]https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/ Erişim Tarihi : 08.02.2020

özellikle açık rızanın geçerliliğine ilişkin özel düzenlemeler mevcuttur. Çocuklara yönelik hizmetlerde, 16 yaşından küçük çocukların ancak yasal temsilcisinin onayı ile rızalarının geçerli olacağı düzenlenerek veri sorumlusuna da bu konuda yeterli teknik alt yapıyı sağlama sorumluluğu yüklenmiştir[128]. Uygulama mağazaları, çocuklara yönelik mobil uygulamalarda reklam faaliyeti veya kullanıcı profilleri oluşturmaya ilişkin sınırlama ve yasaklamalar getirmektedir.

App Store uygulama mağazasında yer almak isteyen çocuklara yönelik mobil uygulamaların çocuk kategorisinde sunulmasının talep edilmesi halinde geliştiricinin çocuklara özel belirlenmiş kurallar çerçevesinde hareket etmesi gerekmektedir. Söz konusu uygulamanın daha sonra çocuk kategorisinden ayrılması bu kurallara uygun hareket etmesi yükümlülüğünü ortadan kaldırmamaktadır. Çocuklar için daha güvenli bir deneyim sağlamak adına, uygulama geliştiriciden çocukların kişisel verilerinin toplanmasıyla ilgili mevzuatları inceleyerek, mevzuat çerçevesinde hareket etmesi, uygulama içerisinde ebeveyn kapısı[129] olmadıkça uygulamada satın alma bağlantısına yer vermemesi, kişisel verilerin veya cihaz bilgilerinin üçüncü taraflarla paylaşılmaması, uygulamada cihaz kimliği veya çocuklara ait kişisel veri, cihaz konumu gibi verilerin dışındaki veriler işlendiğinde sadece üçüncü taraf analiz veya üçüncü taraf reklamlara izin vermesi beklenmektedir.

Mağaza ayrıca uygulama meta verilerinde uygulamanın ana kitlesinin çocuk olduğu anlamına gelen uygulama adı, alt başlık, simge, ekran görüntüleri veya açıklamada bu anlama gelecek terimlerin sadece çocuk kategorisindeki uygulamalar için kullanılması gerektiği ve çocuk kategorisinde olmayan uygulamalarda bu ifadelere yer verilmemesi gerektiğini kural olarak belirtmiştir.

Google Play'in çocuklara yönelik uygulama geliştiricilere ilişkin politikasında da benzer kısıtlamalar mevcuttur. Google Play mağazasında yer almak isteyen

[128] Çekin, s.63

[129] Ebeveyn kapıları, çocuklara yönelik uygulamalarda çocukların ticari bir faaliyete katılmasını veya bir uygulamadan web sitelerine, sosyal ağlara veya diğer uygulamalara ebeveynleri veya velileri bilmeden bağlantılarıları takip etmelerini önlemek için uygulanan bir metoddur. Ebeveyn kapısı, işleme devam etmek için yetişkin düzeyinde birinin tamamlaması gereken görev sunar.

uygulamanın hedef kitlesi çocuklar olduğunda mağazanın internet sitesine yer alan Aile Politikası Gereksinimleri[130] başlığı altındaki gereksinimlerin yerine getirilmesi gerekemektedir. Bu gereksinimleri yerine getirmeyen uygulamalar kaldırılmakta veya kullanımı askıya alınmaktadır.

Bu gereksinimlere örnek olarak; uygulama içeriğinin çocuklara uygun olması, çocuklara reklam görüntülemek için yalnızca Google Play sertifikalı reklam ağların kullanılması, gösterilen reklamların ilgi alanına dayalı reklamcılık veya yeniden pazarlama içermemesi, yürürlükteki tüm yasal düzenlemelere ve endüstri standartlarına uygunluğun sağlanması, uygulamaların çocuklara yönelik hizmetlerde kullanımı onaylanmamış herhangi bir arayüz[131] veya SDK[132] içermemesi verilebilir.

Mağaza, çocuklara yönelik uygulama içeriğinde yalnızca yetişkinler için uygun olan oyun tanıtmak, alkol, tütün veya kontrollü maddelerin kullanımını çekici hale getiren, kumar, bahis, çocuklar için uygun olmayan şiddet, kan veya şok edici içerik barındıran, arkadaşlık hizmeti sunan veya cinsel veya evlilikle ilgili tavsiyeler sunan, içerik olarak çocuklara uygun olmayan reklam gösterilmesine izin veren uygulamaları ihlal olarak örneklendirmiş bu tarz içeriklerin olması halinde uygulamanın mağazadan kaldırılacağını belirtmiştir.

3.5.6. Üçüncü Kişi Aktörler

Reklam ağları, istatistik uzmanları ve elektronik haberleşme hizmeti sağlayıcılar, gibi mobil uygulama sektöründe yer alan üçüncü kişi aktörler de kişisel veriyi kendi amaçları için toplayıp işledikleri ölçüde veri sorumlusudurlar.

---

[130] https://play.google.com/about/families/#!?zippy_activeEl=families-policy#families-policy Erişim Tarihi : 08.02.2020

[131] Google Oturum Açma (veya bir Google Hesabı ile ilişkili verilere erişen başka herhangi bir Google API Hizmeti), Google Play Oyunlar Hizmetleri ve kimlik doğrulama ve yetkilendirme için OAuth teknolojisini kullanan herhangi bir diğer API Hizmeti dahildir

[132] Software Development Kit, mobil uygulama geliştirme sürecinde entegrasyon için uygulanan bu kitler, bir takım bilgileri kişinin isteği dışında üçüncü taraflarla paylaşabilmektedir. Berber s.131,

Uygulama geliştiricilerle karşılaştırınca üçüncü kişi aktörler iki farklı tipte olmaktadırlar. Birinci tiptekiler, uygulama geliştiriciye yönelik işlemde bulunurken örneğin uygulama içinde istatistik bilgi verdiği durumda kendi amaçları için değil sadece uygulama geliştirici adına ve onun talimatları çerçevesinde hareket ettiklerinde bu kişiler, veri işleyen sıfatına haiz olacaklardır. İkinci tip üçüncü kişiler ise uygulama aracılığı ile ilave bir hizmet sunmak amacıyla bilgi toplayan kurumlardır. Bu durumda uygulama geliştirici, kişiselleştirilmiş öneriler için kendi amacı doğrultusunda kişisel bilgi topladığı takdirde veri sorumlusu olarak hareket etmekte ve veri sorumlusunun uymakla yükümlü olduğu yasal düzenlemelere uymak zorundadır.

3.kişi reklam verenler, uygulama içerisinde kullanıcının önceki tarama ilgi alanlarına dayalı reklam sunmak için kişisel verileri işlediğinde veri sorumlusudur. Diğer yanda uygulama geliştiricinin kullanıcılara hangi kişisel verilerin toplanacağı, nasıl kullanılacağı, kimler tarafından ve kullanıcıların hangi kontrolü kullanabileceği konusunda bilgi verme yükümlülüğü devam edecektir[133].

E-Gizlilik Tüzüğü taslağının 10. maddesi, kullanıcının cihazındaki veriye erişim, verinin saklanması veya hali hazırda elde edilmiş verinin işlenmesi kurallarını belirlemek konularda kullanıcılara seçim hakkı sunulmasını zorunlu tutmaktadır. Bu seçim hakkı, uygulamanın indirilmesi sürecinde kullanıcının üçüncü kişi aktörler tarafından izlenmesini engellemek bakımından önemlidir. Maddede, uygulama indirildiği sırada kullanıcıya gizlilik ayarları hakkında bilgi verilmesi ve indirme işleminin ancak kullanıcı ilgili ayarlara açık rıza verdiğinde takdirde devam edilmesinin alt yapısının hazırlanması gerektiğini düzenlemiştir.

EHK'da işletmeciler yetkilendirme[134] çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten

[133]ICO, Privacy in mobile apps Guidance for App Developers, s.6, https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf Erişim Tarihi : 08.02.2020

[134] EHK 3. Madde, Elektronik haberleşme hizmetlerinin sunulması ve/veya elektronik haberleşme şebekesi sağlanmasını teminen şirketlerin, Kurum nezdinde kayıtlanmasını veya kayıtlanmasıyla

şirketler olarak tanımlanmış EHK 12. maddesinin 2. fıkrasının d bendinde; işletmecilerin hak ve yükümlülükleri arasında kişisel veri ve gizliliğin sağlanması belirtilmiştir[135]. Haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamaları amacıyla elektronik haberleşme şebekelerinin kullanılması, işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir denilerek işletmecilere bilgilendirme ve açık rıza alma yükümlülüğü yüklenmiştir. Aynı maddenin devamında da işletmecilerin şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alacaklarını düzenlemiştir.

EHK 51. maddesi 11. maddesinde, tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir denilmektedir.

3.5.7.Kullanıcılar

Bazı mobil cihazlarda şifre yerine parmak izi, yüz tanımlama sistemi gibi biometrik veriler kullanılmaktadır. Apple marka mobil cihazda Face ID olarak tanımlanan yüz tanıma sistemi ile taranan biometrik veri şifrelenerek cihazda saklanmakta ve hiçbir şekilde bulut ortamı veya başka bir yere yedeklenmemektedir. Bu durumda uygulama veya cihaz bu veriye erişemediği gibi veri üzerinde tek hakimiyet kullanıcıya ait olmaktadır. Bu durumda Face ID işleminde kullanıcının veri

birlikte bu şirketlere elektronik haberleşme hizmetlerine özel, belirli hak ve yükümlülükler verilmesini, ifade eder.

[135] Ayözger, s.107

sorumlusu cihaz ve işletim sistemi üreticisinin veri işleyen olduğundan bahsedilebilecektir.

ICO tarafından yayımlanan rehberde kullanıcının mobil cihaz içerisinde not almasına ve bunları cihaza kaydetmesine izin veren uygulamalarda kullanıcının kişisel veri işleme faaliyetini yerine getirmesi ile bu verilerin kullanıcının kontrolünde olması sebebi ile kullanıcının veri sorumlusu olduğundan bahsedilebileceği belirtilmiştir[136].

3.5.8. Mobil Uygulamaların Pazarlama Amacıyla Kullanımı

Akıllı mobil cihazların kullanımı ile eş zamanlı olarak tüketicilerin mobil ticaret kullanım isteklerinin de artması ile birlikte şirketler mobil ticaret için ayırdıkları pazarlama bütçelerini büyük oranlarda arttırmışlardır[137]. Mobil uygulamaların doğrudan satışa imkan tanıması ile birlikte kullanıcı beğeni, ilgi ve alışkanlıklarının takip edilmesi, kullanıcının cihaz konum bilgilerinin göz önüne alınması, mevcut pazarın demografik olarak ölçülmesi vb. verilerin analiz edilmesi ile doğru kişiye doğru mesajın doğru zamanda iletilmesine olanak sağlamaktadır[138].

Mobil uygulamalar, kullanıcılarının verilerini işleyerek kişiye özel hazırlanan kampanyalar ile kullanıcıların davranışlarına uygun pazarlama faaliyetini muhatabına doğrudan ulaşmasına imkan sağlamaktadır. Örneğin bir alışveriş uygulamasında kullanıcı, çocuk ürünlerini inceliyorsa bu durumda bu kullanıcının diğer verileri de birleştirilerek bir profil oluşturulmaktadır. Kullanıcının profiline uygun bildirimlerin yapılması ile kişinin pazarlaması yapılan ürünü tercih etmesi ihtimali çok daha yüksek olacaktır.

---

[136]ICO, Privacy in mobile apps Guidance for App Developers, s.5, https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf Erişim Tarihi : 08.12.2018

[137]Gülhan Yenilmez, Algılanan Deneyimsel Değer Ve Akış Deneyiminin Mağaza Memnuniyeti Ve Satın Alma Niyeti Üzerindeki Etkileri: Çevrimiçi, Fiziksel Ve Mobil Mağaza Kanallarının Karşılaştırılması, Osmaniye Korkut Ata Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı**,**Yüksek Lisans Tezi, 2019,s.141

[138]Uyar,

Ticari rekabetin gün geçtikçe arttığı bir dünyada firmalar, müşteri sadakati sağlamak, müşterilere özel kişiselleştirmiş hizmetler sunmak için mobil cihazları kendi amaçları doğrultusunda kullanılması için yeni teknolojiler ortaya çıkmaktadır. Mobil cihazların günün her saatinde kullanıcılarla iletişim kurulmasına olanak sağlaması, uygulama çeşitliliğin artması ve interaktif ve konum bazlı uygulamalar aracılığı ile kişilerin sürekli erişilebilir olması, mobil cihazları reklam aracı haline getirmektedir.

3.5.8.1. Doğrudan Pazarlama Faaliyetleri

Doğrudan pazarlama, pazarlama faaliyetlerinin arada hiçbir şirket, kurum veya aracı olmaksızın doğrudan kişi ile iletişime geçilerek yapılması anlamına gelmektedir. Doğrudan pazarlama faaliyetleri, her türlü elektronik kanalla yapılabildiğinden kullanıcısının doğrudan indirdiği mobil uygulamalar bakımından özel bir önem arz etmektedir. Her ne kadar 6698 Sayılı Kanunda doğrudan pazarlama faaliyeti ile ilgili olarak özel bir düzenleme mevcut değilse de 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'nda ticari elektronik iletilerin ancak kullanıcılardan onay alındıktan sonra gönderilebileceği yani opt in[139] bir onay beyanı ile doğrudan pazarlama faaliyeti yapılabileceği aynı şekilde verilen onayın her zaman hiçbir gerekçe göstermeden kolay ve ücretsiz bir şekilde geri alınmasının sağlanmasına yönelik alt yapının yapılması gerektiği düzenlenmiştir.

2002/58 Sayılı Direktif'in 13. maddesinin 3. fıkrasında üye ülkelerin, ilgili abonelerin rızası dışında veya önceden rıza vermiş olsalar da artık bu mesajları almak istememeleri halinde ücretsiz olarak doğrudan pazarlama amacıyla haberleşmeye izin verilmemesini sağlayacak uygun önlemleri alması gerektiği düzenlenmiştir[140]. E- Gizlilik Tüzüğü taslağında hali hazırda doğrudan pazarlama faaliyetine rıza vermiş kullanıcıların daha fazla pazarlama iletişimi almamak için verdikleri rızaları geri alma hakkı kolaylığı sağlanması gerektiği düzenlenmiş ise de GVKT de düzenlendiği gibi rızanın kolay ve ücretsiz geri alınması hakkından

[139] Kullanıcının ancak açık bir şekilde izin vererek işlemin yapılması
[140] Özdemir, s.69

bahsedilmemiştir. Bu durum Madde 29 Çalışma Grubu tarafından tutarlılığı sağlamaması ve kullanıcıların mahremiyetinin korunmasını iyileştirmek için, rızanın geri alınması konusunun açık olmaması bakımından eleştirilmektedir [141] .

Gerçek veya tüzel kişiler, tarafından bir ürünün satılması ya da bir hizmetin sağlanması sırasında aboneye ait elektronik iletişim bilgilerinin elde edilmesi halinde, söz konusu kişiler kendi ürünlerinin ya da hizmetlerinin doğrudan pazarlanması amacıyla iletişim bilgilerini kullanabilirler. Ancak, iletilerin haberleşmenin her aşamasında abone tarafından basit ve ücretsiz bir işlemle reddedilebilir olmasına imkân tanınmalıdır.

3.5.8.2. Mobil Pazarlamanın Özellikleri

Mobil cihazlarının taşınabilir olma özelliği sayesinde insanların sürekli elinin altında olması bu noktada mobil cihazların mobil pazarlama ile kullanılmasına olanak sağlamaktadır. Mobil pazarlamanın unsurları aşağıdaki tabloda gösterilmiştir[142].

Tablo 3.2. Mobil Pazarlamanın Unsurları

Ulaşılabilirlik	Lokalizasyon	Kişiselleştirme	Ölçülebilirlik	Hızlı Ulaşım

Mobil pazarlamanın geleneksel pazarlamaya nazaran daha düşük maliyetli olması, hedef kitleye doğrudan ulaşılabilirlik sağlaması ve müşterilerden anında geri bildirim alınabilmesi işletmecilerin bu pazarlama biçimini daha fazla tercih etmelerine neden olmuştur[143]. Mobil pazarlamanın en önemli diğer bir özelliği ise kullanıcının ihtiyaçları ve istekleri doğrultusunda kişiye özel kampanya ve fırsatlar sunulmasına olanak sağlamasıdır.

[141]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.22

[142]Sert, Aybike, Cep Telefonu Kullanıcılarının Mobil Reklamlara Karşı Tutumlarını Etkileyen Faktörler Üzerine Bir Araştırma, İstanbul Arel Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı/İşletme Yönetimi Programı,Yüksek Lisans Tezi, İstanbul, 2012, s.19

[143]Sert, s. 65

3.5.8.3. Konum Tabanlı Servisler

Mobil cihazın konumu ile kullanıcılara konum tabanlı hizmetler sunulmaktadır[144]. Kullanıcının mevcut konumlarına yakın mağazalara özel reklamların iletilmesi, bir bina içerisinde kişiyi aradığı yere yönlendirme, konum tabanlı rehberlik hizmeti, bir mağaza ya da depo içerisinde ürünlerinin yerinin tespiti bu hizmetlere örnek olarak verilebilir[145]. Bunun sonucu olarak kullanıcıda alışveriş algısı yaratılması sağlanarak ilgili indirim veya kampanya müşteriye doğrudan ulaştırılmaktadır. Öte yandan kullanıcının mağazanın yakınından her geçtiğinde bu bildirimlere maruz kalmasının kullanıcıda olumsuz bir etki de yaratabileceği dikkate alınarak bu bildirimlerin belirli aralıklarla yapılmasına olanak tanıyan algoritmalar yapılması sağlanmalıdır.

Harita hizmeti, wifi konumlandırma hizmeti, akıllı ev sistemleri, akıllı taşımacılık gibi mobil uygulamalardaki konum hizmetlerinin yalnızca uygulama tarafından sağlanan özellikler ve hizmetlerle doğrudan alakalı olduğunda kullanılması, mobil uygulamaların gerekli olmadıkça konum erişimi istememesi, konum tabanlı arayüzler, konum verilerini toplamadan, aktarmadan veya kullanmadan önce kullanıcıdan onay alınması gerekmektedir. Uygulama, konum hizmetleri kullanıyorsa, uygulamada bu hizmetin amacı açıklanmış olmalıdır.

3.5.8.4. Çevrimiçi Davranışsal Reklamcılık

Kullanıcının herhangi bir internet sitesi veya mobil uygulamada gezindiği sırada çerez adı verilen küçük metin dosyaları, kullanıcının cihazının belleğine veya harddiskine yerleştirilir. Bu metinler içerisinde kullanıcının IP adresi, tarayıcı bilgisi gibi bilgiler saklanmaktadır[146]. Pratikte çerezler, internet geliştiriciler

[144] Haris Kurtagic,Tüketicilerin Mobil Pazarlama Uygulamalarını Kabullenmelerinde Etkili Olan Faktörler: Balkan Ülkelerindeki Üniversite Öğrencileri Üzerine Bir Araştırma, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İşletmecilik Anabilim Dalı Yüksek Lisans Tezi, 2019, s.41

[145] Işıl Karabey, Wi-Fi Tabanlı Parmak İzi Yöntemi Kullanarak İç Ortam Konumlandırma, Atatürk Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 2015,s.3

[146] Taştan, s.80

tarafından kişilerin aynı siteye veya uygulamaya giriş yaptıklarında kullanıcı adı ve şifrelerini tekrar girmek istemedikleri takdirde kullanıcıları tanıyarak bazı işlemlerin daha hızlı gerçekleştirilmesini sağlamak amacını yerine getirir.

Çevrimiçi davranışsal reklamcılık ise kullanıcının çevrimiçi faaliyetlerinin çerezler yardımıyla izlenmesi ile oluşturulan profili hedefleyen ve kullanıcıya özel içerik ve reklam hizmeti sunan bir teknolojidir.

Bir internet sayfası veya mobil uygulama genellikle hem internet sitesinin kendisinden hem de harici öğelerden alınmış birçok unsur içerir. Bir izleme çerezi, kullanıcı bir sosyal paylaşım ağı sitesini ziyaret ettiğinde yerleştirilmiş olabilir. Çerezler ID numarası ile belli bir kişi ile özdeşleştirildiğinden kişisel veri olarak kabul edilmektedir. Bu sosyal paylaşım sitesi, söz konusu kullanıcı aynı sosyal paylaşım sitesi ile etkileşim içinde olan başka bir web sitesini ziyaret ettiğinde üçüncü kişi aktör de olabilir. Madde 29 Çalışma Grubunun, Çevrimiçi Davranışsal Reklamcılık konulu görüşünde de, çerezlerin kişisel verilerin işlenmesine ilişkin kurallara tabi olarak işlenebileceği, çerezler hakkındaki bilgilendirmenin kolaylıkla erişilebilir ve görünür olması gerektiği, uyarının veri işlemeden önce kullanıcıya gösterilmesi hususlarına vurgu yapılmıştır[147]. Kural olarak Kişinin önceden opt-in açık rızası ile bilgilendirilmiş olması halinde işlenebilecekken 2002/58 Sayılı Direktif'in ilgili düzenlemesinde de tek bir amacın varlığı ve açıkça bir gereklilik olması halinde çerezlere ilişkin rıza aranmayacaktır[148].

Mobil cihazlarda yer alan internet tarayıcılar tarafından işlenen çerezlere ilişkin bilgilendirme ve opt-in seçenekleri tarayıcı ayarlarından yapılmaktayken mobil uygulama içerisinde işlenen çerezler ise farklı şekillerde uygulamaya entegre edilebilmektedir. Yazılım geliştirme kiti olarak tanımlanan SDK ile uygulama geliştiriciler belirli işletim sistemleri için uygulama oluşturmak veya uygulamalarına işlevsellik katmak amacıyla hazır bir araç setinden

[147] Madde 29 Çalışma Grubu 'nun 22 Haziran 2010 tarih ve 02/2010 sayılı "Çevrimiçi Davranışsal Reklamcılık" hakkındaki görüşü, s.19
[148] Öngün, s.247

faydalanmaktadırlar. Örneğin uygulama geliştirici Android platformda çalışabilecek bir uygulama yaratmak için Android SDK'dan faydalanabilecektir.

Analitik SDK'lar kullanıcıların ilişkili mobil uygulamalarla etkileşimi hakkında belirli verileri izlemesine ve ölçmesine olanak tanır. SDK aracılığı ile yapılan izleme ve ölçmeye ilişkin bilgilendirme de mobil uygulamanın gizlilik politikasında yer almalı ve kullanıcılara opt-out seçeneği sunulmalıdır. Analitik SDK'lar, kaç tane kullanıcının uygulamayı kullandığı, uygulamada çalışan oturum sayısı ve her oturumun ne kadar sürdüğü, bu kullanıcıların dünyanın hangi ülkesinden uygulamaya giriş yaptıkları, belirli uygulama özelliklerinin kaç kez kullanıldığı, uygulamayı çalıştıran işletim sistemleri ve cihazlar, kullanıcılar tarafından uygulamalarda harcanan para miktarı ve bir uygulamanın kaç kez çöktüğü dahil olmak üzere uygulama kullanımı hakkında bilgi toplar[149].

Cihazın değiştirilemez belirleyici özelliklerin oluşturan, örneğin IME numarası, telekomünikasyon numarası vs. gibi verilerin işlenmesi zorunlu olması sebebiyle bu verilerin işlenmesi için kullanıcıdan rıza alınması söz konusu olmayacağından bu bilgilerin ilgi alanına dayalı davranışsal reklamcılık ve/veya istatistik için kullanılmaması gerekir[150]. Bilgiye erişim hakkı da dahil olmak üzere, ifade özgürlüğü gibi temel hakların kullanımında internetin temel önemi göz önüne alındığında, kişilerin çevrimiçi içeriğe erişme yeteneği, cihazların ve internet siteleri uygulamalarındaki hareketlerin izlenmesine bağlı olmamalıdır.

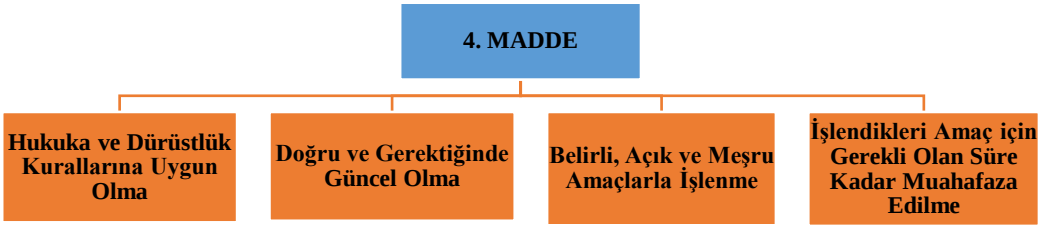
3.6. MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN İŞLENMESİ

Kişisel verilerin korunmasının temelinde, kişisel verilerin işlenmesine hakim olan uluslararası alanda kabul görmüş bazı ilkeler bulunmaktadır. AB düzenlemeleri ile uyumlu olarak 6698 sayılı Kanun'un 4. maddesinde bu ilkeler aşağıdaki şekilde gösterilmektedir;

---

[149] https://www.termsfeed.com/blog/privacy-policy-analytics-sdk/ Erişim Tarihi : 15.03.2020

[150] Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.13



Şekil 3.2. 6698 Sayılı Kanun'un 4. Maddesinde Bulunan İlkeler

GVKT'nde 95/46 Sayılı Direktif'ten farklı olarak bu ilkelere uyulmaması halinde veri sorumlusunun sorumlu olacağına ilişkin "hesap verilebilirlik" ilkesi tesis edilmiştir. 6698 Sayılı Kanun'da bu ilkeye yer verilmemiştir ancak ilgili kanunun 4. maddesine aykırı olarak veri işlemesi halinde kanunun 11/ğ maddesi kapsamında veri sorumlusundan zararını talep edilebileceği düzenlenmiştir[151].

3.6.1. Mobil Uygulamalarda Kişisel Veri İşlenmesinde Hukuka ve Dürüstlük Kurallarına Uygun Olma

Kişisel verilerin işlenmesine yönelik düzenlemelerde yer alan birinci ilke, kişisel verilerin hukuka ve dürüstlük kuralına uygun şekilde işlenmesidir[152]. Bu ilke, kişisel verilerin işlenme sürecinin başından sonuna kadar başta 6698 Sayılı Kanun olmak üzere diğer hukuki düzenlemeler doğrultusunda gerçekeştirilmesi anlamına gelir. Kişisel veriler işlenirken mutlaka hukuki bir temele dayanması gerekir. 6698 Sayılı Kanun'un 5. maddesinde kişisel verilerin açık rıza olmadan işlenemeyeceği devamında ise açık rıza gerektirmeyen haller tek tek sayılarak bunlardan birinin varlığı halinde işlenebileceği düzenlenmiştir. Diğer yandan kişisel verilerin meşru bir sebep olmaksızın bireyler aleyhine sonuçlar doğuracak şekilde kullanılmaması, kişisel verilerin işlenmesinde şeffaflığın ilke edinilmesi ve kişilerin bu bağlamda bilgilendirilmesi, kişisel verilerin, bireylerin makul beklentileri ve öngörüleri doğrultusunda işlenmesi gerekir [153].

[151] Taştan, s. 45
[152] Ayözger, s.124, Küzeci, Kişisel Veriler, s.196
[153] https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/ Erişim Tarihi : 08.12.2019

3.6.2. Doğru ve Gerektiğinde Güncel Olma

Bu ilke, kişisel verileri işlenen kişilerin verilerinin gerçeğe uygun olarak işlenmesini ifade eder. Kişilere, verilerinin gerçeğe uygun olarak işlendiğini kontrol etme ve dönem dönem verilerinin güncelliğini sağlama imkanının verilmesi gerekmektedir. 6698 Sayılı Kanun'un 11. maddesinin d bendinde düzenlenen "kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme" hakkı da bu ilke ile ilgilidir[154]. Bu ilkenin uygulanması için veri sorumlusu kişisel verileri toplarken ve işlerken verilerin doğru ve güncel olduğuna ilişkin gerekli tedbirleri alması ve ilgili kişiye bunları doğrulama ve güncelleme imkanı sağlaması gerekmektedir.

3.6.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi esas olup kişisel verilerin bir gün lazım olur diye saklanması kabul edilemez[155]. İleride ortaya çıkması muhtemel bir amaç için kişisel verilerin işlenmesi bu ilkeye aykırılık teşkil edecektir. Bu ilke doğrultusunda veri sorumlusuna veri işleme amacını kesin ve açık bir şekilde belirleme yükümlülüğü getirilmiştir. Veri sorumlusu belirlediği amaç dışında veri işlediği takdirde sorumlu olacaktır. Aynı şekilde kişisel veriler işlenirken de kişinin belirli, açık ve meşru bir amaç için rıza verdiği varsayılır. Bu nedenle amacın sonradan değişmesi halinde kişisel verisi işlenen kişiden bu kapsamda kişiye karşı aydınlatma yükümlülüğü yerine getirilerek yeniden rıza alınması gerekecektir[156].

3.6.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Bu ilke ile kişisel verilerin sadece işleme amacı ile bağlantılı olarak sınırlı ve ölçülü işlenebileceği belirtilmiştir. İşleme amacı ile ilgili olmayan veya amacın gerçekleştirilmesi için ihtiyaç duyulmayan kişisel verilerin işlenmesi bu ilkeye

[154] Taştan, s.47
[155] Taştan, s. 48, Küzeci, s.198
[156] Taştan, s.48

aykırılık teşkil edecektir. Ayrıca bu ilke kapsamında amacın gerçekleştirilmesi için minimum verinin işlenmesi gerekmektedir. Bu ilke Unutulma Hakkı ile de yakından ilgilidir. Bu hak ile kişisel verilerin durumun gerektirdiği ölçüde ve en kısa süreliğine depolanmasını ihtiva etmektedir[157]. Kullanıcıların verilerinin nasıl işleneceği konusunda veri sorumlusu ve veri işleyene güvenmesi açısından önemli bir ilkedir. Bu durumda kullanıcı hangi tür verisinin işleneceği konusunda bilgilendirilerek vermiş olduğu rızayı sadece o amaçla işleneceğini anlayarak bilinçli bir şekilde vermiş olacaktır. Bilgilendirilme ve kullanıcı kontrolü bu ilkenin iki önemli unsurudur. Bu ilke sebebi ile hangi verilerin işleneceğinin iyi ve normal bir insanın anlayacağı şekilde açık ve teknik terimlerden uzak olarak tanımlanması şarttır. Bu ilke ile uygulama geliştiricilerden kullanıcılardan veri toplamadan önce yapılacak işin niteliğini ve amacını iyi belirlemeleri beklenmektedir. Kişisel veri ancak hukuka uygun olarak kanunun belirlediği ölçüde işlenebilir bu yüzden işleme amacının veri işlenmesinden önce belirtilmiş olması şarttır.

Ancak bu ilke, veri işleme durumlarındaki ani değişikliklerde uygulanmamaktadır. Örneğin, bir uygulama ilk versiyonunda kullanıcıların birbirlerine e-posta göndermelerine izin vermekteyken uygulama geliştirici iş modelini değiştirerek e-posta adreslerini başka bir uygulamanın telefon numarası ile birleştirdiği takdirde bu durumda ilgili veri sorumlusu tek tek ilgili tüm kullanıcılara ulaşarak ve onlardan şüpheye mahal vermeyecek açıklıkta rızasını almak zorunda kalacaktır[158].

Ölçülü ve sınırlı veri işleme ilkesi gereğince de uygulama geliştirici uygulamanın gereği gibi işlemesi için hangi verilerin ne sıklıkla işlenmesi gerektiği konusunda bilgili olmalıdır.

Uygulamalar, cihazlarda yer alan sensörlere de erişim sağlamaktadırlar bu sebeple de SMS göndermek, fotoğraflara erişim ve tüm adres rehberi de dahil olmak üzere birden fazla işlem yapabilmektedirler. Birçok uygulama mağazası otomatik

[157] Taştan, s.49

[158] Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.17

güncelleşmeyi desteklediğinden kullanıcının dahili olmaksızın veya çok az aksiyonda bulunduğu şekilde yeni özellikleri entegre edebilmektedir [159].

3.6.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilme

Bu ilkeye göre kişisel veriler sadece işlenme amacı kadar veya mevzuatta belirtilen süre için muhafaza edilmeli işlenme amacı ortadan kalktıktan sonra kişisel veriler artık saklanmamalıdır. Veri sorumlusu, bu ilke gereğince gerekli olan sürenin bitiminde verileri silmeli, yok etmeli ya da anonim hale getirmelidir. Ayrıca 6698 Sayılı Kanunun 16. maddesi uyarınca veri sorumluları, sicile kayıt başvurusunda bulunurken kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi de belirtilmelidir.

3.7. MOBİL UYGULAMALARDA AÇIK RIZA ALINMASI

Açık Rıza, kişisel verilerin işlenmesinde en temel hukuka uygunluk sebebi olduğu gibi hukuka aykırı bir kişisel veri işlenmesini de hukuka uygun hale getirmektedir. Ancak açık rızanın varlığı, kişisel verilerin serbestçe ve sınırsız bir şekilde işlenebileceği anlamına da gelmemektedir. Veri işleme faaliyetinde başka bir hukuka uygunluk sebebi olması halinde açık rızaya başvurulması ilgili kişileri aldatmaya ve yanıltmaya sebep olabilecektir[160]. Nitekim Kurul tarafından verilen bir kararda; diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği, bu durumun 6698 Sayılı Kanun'un 4. maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil etmesi nedeniyle veri sorumlusu aleyhine idari yaptırım kararı uygulanmasına karar verilmiştir[161].

[159]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.17
[160] Baysal s.128
[161] https://kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi

6698 sayılı Kanun'unda yer alan tanıma göre geçerli bir açık rızanın varlığından söz edebilmek için rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür irade ile açıklanması gerekmektedir.

3.7.1. Belirli Bir Konuya İlişkin Olma

Rızanın belirli bir konuya ilişkin olması, belirli ve açık amaçlar için işlenme ilkesiyle uyumlu olarak işleme konusuna ilişkin kapsamın net bir şekilde belirtilmesini ifade eder.

Bu durumda, kişinin "kişisel verilerimin işlenmesini kabul ediyorum" şeklinde vereceği genel bir beyanda açık rızanın varlığından söz edilemez. Yapılan her bir ayrı veri toplama ve/veya işleme faaliyeti için kullanıcılardan ayrı ayrı rıza alınması gerekmektedir. İlgili mobil uygulama, cihaza indirilmeden ve/veya cihazdan veri alımı gerçekleştirilmeden önce mobil uygulamada hangi verilerin işleneceği kullanıcıya ayrı ayrı belirtilerek her biri için ayrı rızanın alınması gerekecektir. Özellikle reklam verenler tarafından kullanıcı davranışlarını izlemek ve profilleme yapmak için cihaza aktarılan yazılımlar söz konusu olduğunda cihaz işletim ayarlarının varsayılan olarak bu tür izlemelere ancak kullanıcı izin verdiğinde izin verecek yapıda oluşturulması gerekmektedir**.** Örnek olarak yakınlardaki restoran bilgisi veren bir uygulamanın kullanılması için konum bilgisinin alınması için uygulama mutlaka kullanıcının açık rızasını alacaktır. Bu açık rıza, uygulamanın indirilmesi esnasında kullanıcıdan sorulacağı gibi cihazın konum servisine erişme sırasında da sorulabilir. Burada açık rızanın belirli bir konuya ilişkin olması uygulamanın sadece yakınlardaki restoranları önermesi ile amacı ile limitli olmasını ifade eder. Bu rızanın verilmesi, uygulamaya konum bilgisini toplamaya devam etme hakkını vermeyecektir. Uygulama buna ilişkin bir bilgi toplamaya devam etmek isterse bu toplama için de kullanıcıdan ayrı bir rıza alacaktır [162].

[162] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.15

3.7.2. Bilgilendirmeye Dayanma

Bilgilendirmeye dayanma, kişinin verisinin işlenmesi ile ilgili olarak kişinin kolayca erişebileceği bir platformda açık ve anlaşılır bir şekilde bilgilendirilmesini ifade etmektedir**.**

Katmanlı bilgilendirme yöntemi, mobil uygulamalarda etkili olarak kullanılabilir. Bu durumda önemli kısımlar ilk görünen kısımda konunun ayrıntılı açıklaması da linke tıklanarak kapsamlı olarak okunacak şekilde bir bildirim hazırlanabilir. Bilgi, rahat ve görünür şekilde erişilebilir olmalıdır. Belli kategorilerdeki kişisel veriler işlendiğinde içeriksel eş zamanlı bilgi[163] ikonlar aracılığı sağlanabilir örneğin konum ve biometrik veriler işlendiğinde mobil cihazda görünecek bir ikon ile kişinin ilgili verisinin işlendiğini anlamasını sağlayacak belli önlemler alınabilir[164].

Geçerli bir bilgilendirmeden söz edebilmek için anlaşılabilirlik ve erişilebilirlik unsurlarının mevcut olması şarttır. Anlaşılabilirlik, yapılan bilgilendirmenin basit sade, teknik terimlerden uzak ortalama kullanıcının anlayabileceği bir dilde kaleme alınmış olmasını ifade eder. Erişilebilirlik ise bilginin, kullanıcı tarafından doğrudan, kolayca elde edilebilir ve görünür olmasıdır. Örneğin mobil uygulamalarda ekran görüntüsünün küçük olması uygulama indirilmeden önce ve/veya indirilme sonrasında kullanıcıyı bilgilendirecek metnin boyutunun büyük puntolarla ve rahatça görünür olması gerekmektedir. Anlam karmaşasını önlemek adına bilgilendirmenin mutlaka kişisel verinin işlenmesinden önce yapılması gerekir. Eğer uygulama indirme esnasında veri işleme söz konusu olacaksa bu durumda bilgilendirmenin indirmeden önce yapılması şarttır.

Madde 29 Çalışma Grubu, EHGT taslağının internet sitesi tarayıcılarına, kullanıcılara cihazlarıyla yapılan müdahaleleri kontrol etmelerine imkân verecek bir seçenek sunduklarından emin olmak için Do Not Track Standardı (“DNT”) gibi teknik mekanizmaları uygulamak zorunda bırakmasını ve bu şekilde kullanıcı

[163] Contextual real-time information
[164] EDPS Guidelines On The Protection Of Personal Data Processed By Mobile Applications Provided By European Union Institutions,

tarafından yapılan DNT seçiminin mobil uygulama içerisindeki tüm veri sorumlularınca cihazdaki bilgilerin depolanması konusunda açık rızanın reddi ve bunun yasal olarak bağlayıcı bir göstergesi olarak kabul edilmesini sağlamalarını tavsiye etmektedir. Bu standart, sadece çerezlerin izleme teknolojisi ile sınırlı olmayı parmak izi gibi diğer izleme türlerine de hitap etmesi bakımından önemlidir[165].

Aynı görüşte, E- Gizlilik Tüzük taslağında kullanıcılardan sık sık rıza alınmasına karşı korumak için de bu şekilde veya ayrı bir kara liste üzerinden izlemeyi kabul veya red seçeneklerinin kaydedilerek aynı kuruluş tarafından aynı kullanıcıya en az 6 ay boyunca rıza talebinde bulunmasını engellediğinden emin olmasına ilişkin bir düzenleme yapılması tavsiye edilmiştir[166]. Bu kural kullanıcı tarafından doğrudan internet sitesi ziyaret edildiğinde rıza alınmasının önüne geçmeyecektir ancak uygulamada örneğin video sitesi, kullanıcıların cihazlarına izleme çerezleri yüklüyorsa kullanıcı video izlemek istediğinde ondan rıza isteyebilir ancak kullanıcı rıza vermeyi reddettiğinde ilgili site, 6 ay süre boyunca yeniden rıza talebinde bulunmamalıdır.[167]

Bununla ilgili olarak, kullanıcıya rıza vermesine ilişkin seçeneğini tarayıcı ayarları geri alabileceğinin hatırlatılmasında kullanıcıya daha açık olunması tavsiye edilmiş. E- Gizlilik Tüzük taslağının 9.3.maddesinde son kullanıcıların 6 aylık periyodik zaman aralıklarında rızalarını geri alabilecekleri ihtimallerinin hatırlatılması gerektiği düzenlenmiştir. Mobil uygulamaların ara yüzleri dahil olmak üzere genel ayarları herhangi bir senaryoda belirli bir konuda rıza vermek için uygun değilse bu durumda geçerli bir rıza verildiği kabul edilmeyecektir. Mobil cihaz ve uygulamanın varsayılan ayarları, kullanıcı dostu olmalı. Rıza ayarları kullanıcının onay verdiği tüm veri işlemesi için katmanlı olacak şekilde ve veri işlemesine neden

[165]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.18

[166] Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.18

[167] Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.18

olacak ekipman fonksiyonlarını kapsamalıdır. Son kullanıcıya en azından 6 aylık periyodik zaman aralıklarında ayarlarını değiştirmesi yönünde hatırlatmalar yapılmalı[168].

Bilgilendirmeye dayanma yükümlülüğü, açık rızanın bir unsuru olması dışında, aynı zamanda 6698 Sayılı Kanun'un veri sorumlusunun aydınlatma yükümlülüğü başlıklı 10. maddesi uyarınca veri sorumlusuna getirilmiş bir yükümlülüktür[169].

3.7.3. Özgür İradeyle Açıklanmış Olma

Rızanın özgür iradeyle verilmesi, kullanıcının rıza vermemesi halinde tercih özgürlüğünün kısıtlanmamasını ifade eder. Kullanıcı, uygulamayı kullanmak için mutlaka rıza göstermesi gerekiyor ve aksi halde uygulamayı cihazına indiremiyor veya ilgili uygulamadan elde edeceği menfaatten mahrum bırakılıyorsa bu durumda özgür iradeyle verilmiş bir açıklamadan söz edilemez. Mobil cihazlarda kullanıcının verilerinin işlenmesi konusunda mutlaka kabul veya reddetme tercihi bir arada olmalı. Örneğin uygulamanın indirilmesi için sadece 'evet kabul ediyorum' şeklinde bir butonun olması değil iptal veya red seçeneklerinin de bir arada olması gereklidir[170].

6698 Sayılı Kanun gerekçesinde yer alan rıza beyanının 'tereddüde yer vermeyecek açıklıkta olması', ilgili kişinin rızasını aktif bir davranışla açıklamasını ifade eder. Buna göre ilgili kişinin rıza gösterip göstermediğine dair herhangi bir şüphenin bulunmaması için mutlaka kişinin aktif bir davranışı olmalıdır[171]. Mobil uygulama alanında da aktif davranış önceden işaretlenmemiş kutucuğun işaretlenmesi veya boş bir formun içine onayda bulunulması veya dokunmatik olarak bir işaretleme yapılması gibi örnekler verilebilir. Opt out onay ise açık rıza olarak kabul

[168] Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.34
[169] Taştan, s.154 6698 sayılı Kanun'un 10. Maddesi kapsamında ilgili kişiye doğruda bir aydınlatma metni sunulabilir. Bunun dışında katmanlı bilgilendirme yöntemine de başvurmak mümkündür.
[170] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.14
[171] Taştan, s.156

edilmemektedir. Ayrıca kullanıcılar verdikleri rızayı her zaman kolay ve rahat bir şekilde değiştirme ve geri alabilme hakkına sahip olmalılardır.

Kurul tarafından verilen bir kararda da aynı şekilde açık rızanın üyeliğin ve hizmetin bir şartı olarak alınmasının açık rızayı sakatlayacağını belirtilmiştir[172].

Mobil uygulamalar, kullanıcının cihazına indirilmeden önce kullanıcıya açık bir şekilde bilgilendirme yaparak hangi verilerinin işleneceği belirtmeli kullanıcıların verecekleri rızaları hangi şekilde ve nasıl geri alacağını gösterecek şekilde açık bir rıza almalıdır. Birçok uygulama cihaza indirildiğinde cihazdaki bilgilere erişim sağlamaktadır. Bu sebeple 2002/58 Sayılı Direktif de cihaza indirilmeden veya cihaza indirildiği sırada ve cihazdan bilgi almadan önce açık bir bilgilendirme ile kullanıcıdan rıza alınmasını şart koşmaktadır. Her ne kadar bazı uygulama mağazaları uygulama hakkında ön bilgi vererek indirilmesini sağlasa da bu ön bilginin geçerli rızanın arandığı şartlara uygun olduğundan bahsedilmeyecektir. Ayrıca mobil uygulamada varsayılan ayarların kullanıcının rıza göstermesi ile aktif olacak şekilde teknik altyapısını oluşturulması gerekmektedir.

Aynı şekilde E- Gizlilik Tüzüğü taslağında da GVKT'ünde yer alan rıza tanımının elektronik haberleşme verilerinin korunmasında da uygulanacağını belirtilmiştir. Öncelikle, internet erişimi ve mobil telefon hizmetlerinin temel hizmetler olduğunun ve bu hizmetleri sağlayanların müşterilerini gerekli hizmetin sağlanması dışında veri işlenmesi için rıza vermeye zorlamamaları gerektiğine de dikkat edilmelidir.

3.7.4. Tüzel Kişiler Bakımından Rıza Kavramı

6698 Sayılı Kanun ve GVKT sadece gerçek kişilere ait kişisel verilerin korunmasına yönelik hükümler getirirken EHK ve 2002/58 sayılı Direktif ise hem gerçek hem tüzel kişilere ait kişisel verileri korumaktadır. Örneğin şirket aracına takılan GPS cihazına ilişkin uygulama veya ücretli yollardan hızlı geçiş imkanı

[172] https://kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi

sunan hızlı geçiş sistemlerine ilişkin uygulamalar veya şirket sistemine ait IP adresleri bakımından koruma nasıl olacaktır? Aynı şekilde rıza kavramı, tüzel kişiler bağlamında nasıl uygulanacaktır? Her ne kadar 2202/58 Sayılı Direktif ve bu direktifi ilga edecek E- Gizlilik Tüzük taslağında tüzel kişiler koruma kapsamında yer alsa da bu korumanın pratik uygulaması açık değildir. Tüzel kişinin de rızasını vermesi gereken durumda "bilgilendirilmiş" olduğu ve aktif bir eylemde bulunduğunun düşünülmesi gerekir. İşverenlerin çalışanlarına araba tahsis ettiği bir durumda ve idari maksatlarla, aracın araç kartı birimi aracılığıyla konum verilerini toplamasına izin verir. Bu durumda çalışanla işveren arasındaki ilişki ayrı işveren ile konum verisinin paylaşıldığı 3. şahıs arasında ayrı bir ilişki olduğu kabul edilmelidir. Konum verileri toplanan araç, kiralama hizmeti veren başka bir şirket aracı olduğunda da durum daha da karmaşık hale gelebilir. İlk örnek bakımından EHGT taslağında yer alan düzenlemeye göre, işverenin bir istihdam ilişkisi bağlamında belirli ekipman temin ettiği, işçinin bu ekipmanın kullanıcısı olduğu ve müdahale, ekipmanın işleyişi için kesinlikle gerekli olduğunda verilerin toplanması ile orantılılık ve yerindenlik ilkelerinin uygulanmasını gerektirmektedir. Ancak bu koşullar yerine getirilirse, işverenin son kullanıcı cihazlarına müdahale etmesi mümkün olmalıdır.

3.8. MOBİL UYGULAMALARDA KİŞİSEL VERİLER İŞLENİRKEN RIZANIN ARANMADIĞI DURUMLAR

3.8.1. Kanunda Açıkça Öngörülmesi

6698 Sayılı Kanun'un 5. maddesinde kişisel verilerin ilgilisinin açık rızası olmadan işlenemeyeceği hükme bağlanmış devamı fıkrasında ise açık rızanın aranmadığı haller tek tek sayılarak belirtilen durumların var olması halinde açık rıza olmaksızın kişisel verilerin işlenebileceği düzenlenmiştir. Kanunda açıkça kişisel verilerin işlenmesine izin verilen hallerde rıza aranmayacağı açıktır. Örneğin Vergi Usul Kanunu'nun 232. maddesi yaptıkları işler dolayısıyla fatura vermek ve almakla yükümlü kılınanları saymış 230. maddesinde ise faturada en az bulunması gereken bilgileri tek tek saymıştır. Elektronik ticaret yapan mobil uygulamalarda fatura

düzenlemek için kullanıcıdan bazı bilgilerin talep edilmesi ise Vergi Usul Kanunu'ndan kaynaklandığı için bu durumda kanun kapsamında işlenmesi gereken kişisel veriler bakımından açık rıza alınmasından söz edilmeyecektir.

EHK 51. maddesinin 5 numaralı bendinden aynı kanunun 49. maddesi kapsamında, kamu yararının sağlanması ve BTK tarafından işletmecilere getirilen yükümlülüklerin yerine getirilmesi amacıyla kişisel verilerin işlenebileceği kanun ile hüküm altına alınmıştır. İşletmeciler, bu kanun maddesi ile sınırlı olarak kanundan kaynaklanan bir yükümlülükle kişisel veri işleyebilecektir. Ancak kişisel verilerin amaçla sınırlılık ve ölçülük ilkesi gereği kanunda belirtilen amacı aşacak şekilde ve kanunda talep edilenden fazla kişisel verinin işlendiği takdirde hukuka uygunluk söz konusu olmayacaktır.

3.8.2. Üstün Özel Yarar

6698 sayılı Kanunun 5. Maddesinin 2. Fıkrası b bendi gereğince fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasının geçerli sayılmadığı hallerde kişinin hayat veya beden bütünlüğünün korunması için verilerinin işlenmesi zorunlu olduğu takdirde kişisel verileri işlenebilir. Bu durumda hukuka aykırılık söz konusu olmayacaktır. Kanun gerekçesinde kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda hayat veya beden bütünlüğünün korunması amacıyla tıbbi müdahale yapılması sırasında kişisel verileri işlenebileceği ifade edilmiştir. Buna örnek olarak da kişinin tehdit altında olması veya yerinin tespit edilmesi amacıyla mobil uygulama ile konum verilerinin işlenmesi verilebilir. Nitekim EHK'na göre acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilmektedir.

3.8.3. Üstün Kamusal Yarar

6698 Sayılı Kanun'un 28. maddesinde kişisel veri işleme faaliyetleri bakımından kanun hükümlerinin uygulama alanı bulmayacağı durumlar sayılmış, maddenin ç bendinde kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesini istisna olarak ele alarak 6698 Sayılı Kanun'un uygulama alanı bulmayacağını belirtmiştir. 2002/58 Sayılı Direktifin 15. maddesinde de amaçların daha sınırlı olduğu benzer bir kısıtlamaya izin verilmektedir[173].

3.8.4. Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili İşlenmesi

6698 sayılı Kanunun 5. maddesinin 2. Fıkrasının c bendinde sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde hukuka aykırılık söz konusu olmayacaktır. Örneğin kullanıcının mobil bankacılık uygulamasını indirmesi halinde kullanıcı ödeme veya para transferi yapmak için uygulamayı kullandığında kullanıcıdan işlemi yapması için gerekli olan bilgileri işlemek için ayrıca bir rıza istemeyecektir. Aynı durum iletişim uygulamalarında da geçerlidir. Kullanıcı, başka biri ile iletişime geçmek istediğinde kişinin isim, telefon numarası, e-posta adresi gibi bilgilerini ifşa etmesi sözleşmenin ifası için gerekli olmaktadır[174].

3.8.5. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Veri işleme faaliyeti veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi için zorunlu ise bu yükümlülük, veri işlemeyi hukuka uygun hale getirecektir.

[173] Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.24

[174] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.16

Örneğin Tüketicinin Korunması Hakkındaki Kanun'un mesafeli sözleşmeleri düzenleyen 48. maddesinin 5. fıkrasında da satıcı veya sağlayıcı adına mesafeli sözleşme kurulmasına aracılık edenlerin bu işlemlere ilişkin kayıtları tutmak ve istenilmesi halinde bu bilgileri ilgili kurum, kuruluş ve tüketicilere vermekle yükümlü olduğu düzenlenmiştir. Bu kapsamda faaliyet gösteren mobil uygulamaların ilgili kayıtları tutmaları kanun hükmünde yer alan amaçla sınırlı olarak işlenmesi, hukuka uygun kabul edilecektir. Veri sorumlusunun hukuki yükümlülükleri kaynağı Türk hukuku olacaktır[175]. Veri sorumluları siciline kayıtlı olan veri sorumlusunun başka bir ülkede yer alan hukuki yükümlülükler kapsamında veri işlemesi Kanunun bu bendindeki hukuka uygunluk sebebi olarak kabul edilmeyecektir[176]. Öte yandan Türkiye dışında da faaliyet gösteren kurum ve kuruluşlar bakımından faaliyet gösterdiği ülkenin hukuk kurallarına uyulmasının zorunlu olduğu ve bu kapsamda veri işlemesinin zorunlu olduğu durumlarda, bu işleme faaliyetinin de hukuki yükülümlülüklerin yerine getirilmesi kapsamında kabul edilmesi gerekir aksi takdirde ilgili kuruluşun yurt dışındaki faaliyeti sekteye uğrayabilecektir.

3.8.6. Kişisel verinin kişinin kendisi tarafından alenileştirilmesi

6698 Sayılı Kanun uyarınca, kişisel veriler kişinin kendisi tarafından alenileştirilmiş olduğu takdirde bu veri, kişinin açık rızası alınmadan işlenebilecektir. Örneğin mobil uygulama kullanıcısı, coğrafi konumunu sosyal medya mobil uygulaması ile herkese açık bir şekilde alenileştirdiği takdirde bu durumda ilgili konumun uygulama tarafından işlenmesi için kişinin açık rızası aranmayacaktır. Ancak kişinin verisini aleniştirmiş olması, işleme faaliyetinin kişisel verilerin işlenmesine ilişkin ilkeler doğrultusunda yerine getirilmesine engel değildir[177]. Bu noktada veri alenileştirilmiş olsa dahi söz konusu işleme faaliyeti, amaçla bağlı ve ölçülü olma ilkesine uygun yerine getirilmelidir. Kurul'un 07.11.2019 tarih ve 2019/331 sayılı kararında da veri sahibi tarafından internet

[175] Taştan, s.166
[176] Taştan, s.166
[177] Türkmen, s.199, Küzeci, Kişisel Veriler,s.346

sitesinde alenileştirilen bilgilerin internet sitesinde bulunma amacıyla kullanılmaması sebebiyle veri sorumlusuna idari para cezası yaptırımı uygulamıştır[178]. Örneğin online bir ilan sitesinde kişinin cep telefonu bilgisi, sadece ilgili ilan bakımından kendisine ulaşılması amacıyla sınırlı olarak veri sahibi tarafından alenileştirilmiştir. Bu noktada veri sahibi dışında üçüncü bir kişinin ilgili platformda alenileştirilen cep telefonları bilgilerinin farklı amaçlar doğrultusunda işlenmesi, bu hüküm kapsamında değerlendirilmeyecektir.

3.8.7. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

6698 Sayılı Kanun uyarınca bir hakkın tesisi, kullanılması veya korunması amacıyla veri işlemenin zorunlu olması durumunda veri sahibinin açık rızası olmaksızın veri işleme faaliyeti yapılabilecektir. Örneğin ulaşım faaliyeti yerine getiren bir şirketinin mobil uygulamasında kullanıcıların bagajlarına ilişkin haklarını kullanmaları için kimlik bilgileri ve diğer kişisel bilgilerine ihtiyaç duyması halinde bu durumda da açık rıza alınmasından söz edilmeyecektir. Kişinin bagajının kendisine ait olup olmadığını anlamak, kişiye bagajına ilişkin haklarını sağlamak amacıyla ve veri sorumlusu kuruluş tarafından hak sahibine mükerrer ödeme yapmamak gibi sebeplerle yolcudan gerekli kişisel verilerinin işlenmesi zorunlu olacaktır.

3.8.8. İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemenin Zorunlu Olması

6698 Sayılı Kanun uyarınca ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması durumunda açık rıza aranmayacaktır. Mobil uygulamaların kendi güvenlik ayarlarını güncelleştirmek amacıyla kullanıcının cihazına erişmesi ve bu kapsamda veri işlemesi, veri sorumlusunun cihazların güvenliğinin güncel kalmasını sağlamak adına meşru menfaati için veri işleme faaliyetine örnek

[178] https://www.kvkk.gov.tr/Icerik/6623/2019-331

verilebilir. Bu nedenle güvenlik yama sağlayıcısı, son kullanıcıdan rıza almadan gerekli güvenlik güncellemelerini yükleyebilmelidir[179].

Özel bir şirket tarafından yapılacak veri işleme faaliyetinin meşru menfaat kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin Kurul'a yaptığı başvuru neticesinde Kurul veri sorumlularının kişisel veri işleme faaliyetinin meşru menfaat kapsamında değerlendirilmesine ilişkin kıstasları sıraladığı bir karar vermiştir[180]. Kararda da belirtildiği üzere gereklilik ve ölçülülük ilkesi uyarınca veri sorumlusunun amaçladığı meşru menfaatin gerçekleşmesi için verilerin işlenmesinin gerekli olup olmadığının değerlendirilmesi ve buna yönelik denge testlerinin yapılması gerekmektedir[181]. Bu kararda da yer aldığı üzere veri işleme faaliyetinin meşru menfaat kapsamında değerlendirilmesi için denge testinin yapılması gerekmektedir.

[179]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.20

[180] KVKK'nun 25/03/2019 tarih ve 2019/78 sayılı Kararı, ilgili kararda sayılan kıstaslar şu şekildedir: 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (f) bendine göre "*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*" hali tespit edilirken veri sorumluları tarafından; Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması, Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi, Meşru menfaatin halihazırda mevcut, belirli ve açık olması, İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması, Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması, Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması, Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması, Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması, Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması.

[181] Aşıkoğlu, s.135, Çekin, Kişisel Verilerin Korunması , s.72

3.9. MOBİL UYGULAMALARDA KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN YÜKÜMLÜLÜKLER

3.9.1. Veri Koruma Etki Analizi

Risk temelli yaklaşım, sadece kişisel verilerin işlenmesi sırasında değil kişisel verilerin işlenmesinden önce de veri koruma etki analizi yapılmasını zorunlu kılmaktadır[182]. Veri koruma etki analizi, kişilerin mahremiyet haklarına yönelik gerçek veya olası etkileri olacak olan eylem, öneri, teknoloji, sistem uyarlaması gibi süreçleri incelemek, sorunları tespit etmek ve sorunları giderici veya önleyici yolları belirleme sürecidir[183]. Veri koruma etki analizinin yapılması GVKT 35. maddesi ile özellikle yeni teknolojik veri işleme metodlarının kullanıldığı veri işleme faaliyetinin kişilerin hak ve özgürlükleri bakımından risk içerdiği durumlarda veri sorumlularına getirilmiş bir yükümlülük olmakla birlikte talep edildiği takdirde veri işleyenler tarafından da yapılmasına imkan tanınmıştır[184]. Veri koruma etki analizi sonucunda hangi önlemlerin fayda sağlayacağı belirlenemiyorsa bu durumda denetim makamına da danışılması mümkün olmaktadır[185]. 6698 sayılı Kanun kapsamında da veri güvenliğine ilişkin politika ve prosedür belirlenmesi sürecinde de veri koruma etki değerlendirmesi yapılması gerekir. Bazı ülkelerde kamu kurumlarının kişisel veri işleme faaliyetinde bu analizin yapılması zorunlu tutulmuştur[186].

Mobil yazılım geliştiricilerden uygulamayı hayata geçirmeden önce aşağıdaki şekilde veri koruma etki değerlendirmesi yapmaları beklenmektedir. Devam eden veri işleme faaliyetinde risk potansiyelini değiştiren bir durumun varlığı halinde de yeniden veri koruma etki analizi yapılması söz konusu olabilecektir.

---

[182] Kaya, Mehmet Bedii, Elektronik Ticaret Hukuku Ticari Elektronik İletiler, Onikilevha Yayınları, İstanbul, Şubat 2020, s. 116

[183] Tataroğlu, Muhittin, Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED), Yönetim Ve Ekonomi dergisi Yıl:2013 Cilt:20 Sayı:1, s.279 http://yonetimekonomi.cbu.edu.tr/dergi/pdf/C20S12013/263-289.pdf Erişim Tarihi : 10.03.2020

[184] Akıncı, s.18

[185] Işık, 168

[186] Tataroğlu, s.267

Tablo 3.3. Veri Koruma Etki Değerlendirmesi

Uygulama, hangi kişisel verileri işleyecek?
Kişisel veriler hangi amaçlar doğrultusunda işlenecek?
Veri toplama yöntemi nasıl olacak?
Rıza ne zaman alınacak?
Veri nerede saklanacak?
Veri başka sistemlere transfer edilecek mi?
Saklama süresi ne kadar olacak?
Veriye kimler erişebilecek?
Veri kimlerle paylaşılacak?
Hangi yöntemle paylaşılacak?
Güvenlik risklerini azaltmak için yapılan önlemler?
Veri nasıl güvenli şekilde silinip yok edilebilecek?

3.9.2. Tasarımla Veri Koruma

GVKT 25.maddesinde düzenlenen bir yükümlülük olan tasarımla veri koruma, veri işleme yönteminin belirlenmesi ve işleme faaliyeti esnasında veri koruma ilkelerinin etkili bir şekilde uygulanması ve GVKT gerekliliklerin yerine getirilmesi amacına yönelik olarak tasarlanan tedbirlerin uygulanmasıdır[187]. Sandbox yöntemi ile bir uygulamanın canlı ortamda çalıştırılmadan önce özel test alanında çalıştırılarak zararlı bir yazılım içerip içermediği veya sistemle uyumlu olup olmadığı incelenmektedir[188].

[187] Berber, Bilgili, Leyla Keser Berber, Ali Cem Bilgili, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, Oniki Levha Yay, İstanbul, 2020 s.15
[188] Berber, Bilgili, s.59

3.9.3 Varsayılan Ayarlarla Veri Koruma

Uygulama geliştiricinin varsayılan ayarları gizlilik dostu olmalı kullanıcı tarafından verilmesi zorunlu ve ihtiyari verilerin ayrımı yapılarak kullanıcının verileri üzerinde hakimiyet kuracağı bir sistem oluşturulmalıdır[189].

3.9.4. Mobil Uygulamalarda Gizlilik Politikası

Veri sorumlulukları, mobil uygulama için anlaşılması ve erişilmesi kolay bir kişisel verilerin korunması veya gizlilik politikası oluşturmalılardır. Uygulama satıcıları, mağazalarında kullanılacak uygulamaları seçerken gizlilik politikası olmayan uygulamaları mağazaya kabul etmemektedirler.

Gizlilik politikasında şeffaflık ilkesi kapsamında veri sorumlusunun kim olduğu ve iletişim bilgileri, uygulama kullanıldığında hangi kategorideki kişisel verilerin toplanmasının ve işlenmesinin istendiği, hangi amaçla işlendiği, verilerin üçüncü kişilerle paylaşılıp paylaşılmadığı, paylaşılıyorsa kiminle paylaşılacağına ilişkin bilgi kullanıcıların sahip oldukları haklar, rızanın geri alınması ve verinin silinmesi ile ilgili bilgiler yer almalıdır.

29. Madde Çalışma Grubu, 02/2013 nolu görüşünde uygulama geliştiricilere gizlilik politikalarına GVKT'ya tabi kullanıcılar için uygulamanın GVKT'ne uyumlu olduğu ve kişisel verinin aktarıldığı başka bir ülke mevzuatına da uyumlu olduğu bilgisini eklemelerini tavsiye etmektedir[190].

3.9.5. Mobil Uygulamalarda Aydınlatma Yükümlülüğü

Veri Sorumlusunun 6698 Sayılı Kanun kapsamında düzenlenen yükümlülüklerinden biri de aydınlatma yükümlülüğüdür. Aydınlatma yükümlülüğü, 10.03.2018 tarihli resmi gazetede yayınlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında

[189]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü,s.20

[190]Madde 29 Çalışma Grubu 'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.10

Tebliğ ile ayrıntılı olarak düzenlenmiştir. Aynı şekilde GVKT'nün 14. maddesinde de aydınlatma yükümlüğünün kullanıcının talebine bağlı olmadığı ve veri sorumlusunun kişisel veri toplama esnasında verisi toplanan kişiye karşı gerekli bilgilendirmeyi yapma zorunluluğu yer almaktadır. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı da veri sorumlusuna yükletilmiştir. Kullanıcı tarafından fark edilmeyen erişimlerde örneğin bazı mobil uygulamaların cihazın sensörlerine ve veri yapılarına erişimi olduğu düşünüldüğünde bu bildirimin varlığı daha da önemli hale gelmektedir.

Gerekli aydınlatma yükümlülüğünün yerine getirimesi, özellikle kişisel verisi işlenen kişinin veri işleme sırasında hukuka uygunluk nedeni olan açık rızasını vermesi aşamasında önem arz etmektedir. Rızanın geçerliliği de kişinin verilerinin işlenmesi konusunda önceden bilgilendirilmiş olmasına bağlı olmaktadır. Bu bilgilendirme, mobil uygulama tarafında da veri işleme faaliyetine başlamadan önce yapılmalıdır. GVKT'de kişisel veri işleme faaliyetinin açık rıza alınması şartına bağlı olarak gerçekleştirildiği durumlarda aydınlatma yükümlüğü ile açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği düzenlenmiştir. Veri işleme faaliyeti, rıza dışında başka bir hukuka uygunluk sebebine dayanırsa bu sebebin ne olduğuna aydınlatma metninde yer verilmesi gerekir. Örneğin, bir e-ticaret mobil uygulamasında kullanıcı ile mesafeli satış sözleşmesi kurulmuşsa burada yer alan veri işleme faaliyetinin sözleşme ilişkisine dayandığı aydınlatma metninde yer almalıdır.

Aydınlatma bildiriminde; kullanıcılara kişisel verilerinin kim tarafından hangi amaçla işlendiği, işlenen verilerin kimlere hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi, veri sorumlusunun kim olduğu, veri sorumlusu ile nasıl iletişime geçileceği ve ilgili kişinin haklarına ilişkin bilgiler yer almalıdır. Mobil uygulama sektöründe yer alan birden fazla aktör düşünüldüğünde mobil cihazda veri sorumlusu, işletim sisteminde veri sorumlusu ve mobil uygulamada veri sorumlusu kimlikleri açıkça belirtilmeli uygulama geliştiriciler ile veri işleyen diğer kişiler arasındaki ilişkiyi araştırma işi son kullanıcıya bırakılmamalıdır.

Veri işleme amacı değiştiğinde her yeni amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir. Veri Sorumlusu, veri sorumlululuları siciline kayıtla yükümlüyse aydınlatma metninin sicile de uyumlu olması gerekmektedir[191]. Uygulama mağazaları veya şirketin teknik departmanı tarafından şirket adına oluşturulan mobil uygulamalarda veri sorumlusu olan şirket, mobil uygulamada bu bilginin ulaşılabilir ve kolayca erişilebilir olduğundan emin olmalıdır.

Yukarıda belirtilenlere ek olarak veri sorumlusunun kullanıcılara mutlaka, cihazda hangi tür verinin toplandığı veya hangi verilere erişildiği, verinin muhafaza süresi, veri sorumlusu tarafından uygulanan güvenlik tedbirleri bilgilerini vermesi gerekmektedir.

Bir müzik çalar uygulamasının geliştiricisi, cihaz bir telefon araması aldığında veya telefon görüşmesi yaptığında uygulamanın müzik çalmayı duraklatmasını istediği takdirde bunu sağlamak için, uygulamanın gelen veya giden çağrıların durumunu izlemesi gerekir. Bu izleme faaliyet için erişim izni istediğinde "bir telefon araması aldığınızda veya bir telefon görüşmesi yaptığınızda müzik çalmayı duraklatmak için uygulamanın telefon işlevlerine erişmesi gerekir" şeklinde bir aydınlatma yapması gerekir. Aksi takdirde uygulama geliştiricisinin, uygulamanın orijinal amacı için kesinlikle gerekli olmayan örneğin çağrıları dinleme veya kaydetme izni gibi işlevlere veya cihazdaki verilere potansiyel olarak erişebileceği anlamına gelir[192].

3.9.5.1. Aydınlatmanın şekli

6698 sayılı Kanun ve ilgili yönetmelik ile GVKT'de aydınlatmanın ne şekilde olacağı belirtilmemekle birlikte söz konusu aydınlatma, mobil cihaz ekranından direkt olarak görünebilmeli ve kullanıcı tarafından kolayca erişilebilir olmalıdır. Mobil cihazların küçük ekranlarına sığamayacak ayrıntıları mutlaka kullanıcının daha ayrıntılı açıklamaya ulaşmasına imkân verecek şekilde ulaşılabilirlik

[191] Baysal, s.50
[192] ICO, Privacy in mobile apps Guidance for App Developers, s.15 https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf Erişim Tarihi : 15.03.2020

sağlanmalıdır. Örneğin gizlilik politikasında mutlaka uygulamanın kişisel veriyi nasıl kullandığı, veri sorumlusunun kim olduğu ve kullanıcının haklarını nerde kullanacağının bilgisi verilmelidir. Bu yaklaşım, ikon kullanımı, resim, video ve ses kullanımı ile desteklenmeli uygulama adres defterine veya fotoğraflara eriştiğinde içeriksel gerçek zamanlı bildirim kullanılmalıdır. Bu ikonlar anlamlı, açık, tereddüte mahal vermeyecek şekilde olmalı.

Uygulama geliştiriciler, küçük ekranlar için programlama ve karışık arayüzler tasarlamada uzman olduklarından Madde 29 Çalışma grubu bu endüstrideki kişilere kullanıcılara etkili bildirimde bulunmak konusunda daha yaratıcı çözümler sunmaya davet etmektedir. Bu bilginin teknik ve hukuki altyapısı olmayan insanlar için gerçekten anlaşılabilir olup olmadığından emin olmak için çalışma grubu seçili strateji için test yapmayı tavsiye etmektedir.

3.9.6. Veri Güvenliğinin Sağlanması

Kişisel verilerin korunması mevzuatında veri güvenliği, en geniş anlamıyla kişisel verilerin korunması amacıyla gerekli tüm idari ve teknik tedbirlerin alınmasını ifade eder[193]. 6698 Sayılı Kanun ve GVKT kapsamında veri sorumlusu ve veri işleyen kişisel verilerin saklanması ve işlenmesi ile ilgili tüm teknik ve idari güvenlik önlemlerini almak suretiyle hukuka aykırı olarak verilere erişim veya işlenmesinin önüne geçmek ve kişisel verilerin muhafazasını sağlamakla yükümlüdürler.Veri korunmasına yönelik tedbirler standart olmadığından her bir veri sorumlusu, yapısı, büyüklüğü, faaliyetleri, işlediği kişisel verilerin niteliği ve miktarı ile barındırdığı risklere göre veri güvenliğine yönelik tedbirleri kendisi belirleyecektir[194].

İdari Tedbirler, risk ve tehditlerin belirlenmesi, personelin eğitilmesi ve farkındalığının arttırılması, kişisel veri güvenliği politika ve prosedürlerin belirlenerek, bunların yayınlanması ve kontrollerinin sağlanması, veri minimizasyonunun sağlanması, veri işleyenlerle ilişkinin belirlenmesi, iç ve dış

[193] Taştan, s.71
[194] Taştan, s.71

denetimlerin yaptırılması örnek olarak verilebilir[195]. Teknik tedbirlere ise siber güvenliğin sağlanması, kişisel veri güvenliğinin izlenmesi ya da takip edilmesi, kişisel veri bulunan ortamlarda güvenliği sağlanması, kişisel verinin bulut ortamında saklandığı durumlarda bulut güvenliğinin sağlanmasının temin edilmesi, bilgi teknoloji sistemlerinin tedariği, geliştirilmesi ve bakımının yapılması, kişisel verilerin yedeklenmesi işlemleri olarak örnek verilebilir[196]. Genel anlamda veri sorumlusunun , kimlik doğrulama, erişim yönetimi, veri kayıtlarına ya da loglara erişim, vaka yönetimi, bilişimin güvenliği, veri işleme güvenliği, iç ağın korunması, sunucuların güvenliği, web sayfaların güvenliği, sürekliliğin sağlanması, güvenli arşivleme, bakımın denetlenmesi, verilerin imhasının gözlenmesi, veri işleyenlerin yönetilmesi, fiziksel ortam güvenliği, yazılım geliştirmenin denetlenmesi ve şifreleme mekanizmalarının kullanımı gibi noktaların denetlenmesi veya kontrol edilmesi gerekmektedir[197].

Uluslararası Standardizasyon Kurumu ("ISO") ve Uluslararası Elektroteknik Komisyonu ("IEC") işbirliği ile, yürürlükte bulunan yasal düzenlemelere tamamlayıcı nitelikte bilgi ve iletişim teknolojilerinde gizlilik ve kişisel verilerin işlenmesinde güvenlik standartlarının iyileşmesi amacıyla standartlar hazırlanmaktadır[198].

Türk Standartları Enstitüsü'nün veri güvenliğini sağlamak amacıyla yayınladığı ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ile kurumların veriyi uygun şekilde kullanması, buna ilişkin politikaları oluşturması, organizasyonel yapılar oluşturması, ayrıca uygun yazılım ve donanımlardan faydalanması amaçlanmıştır[199]. Bu standarda ek olarak güvenlik teknikleri gizlilik bilgi yönetimi için ek gereklilik ve rehber standart olarak ISO 27701 standardı çıkarılmıştır[200]. ISO/IEC 29100 Standardı ile de kişisel verilerin korunmasında ortak bir anlayış

[195] Turan, s.89
[196] Turan, s.91
[197] Turan, s.93
[198] Berber, Bilgili, s.2
[199] Taştan, s.72
[200] Berber, Bilgili, s.2

geliştirilmesi ve kişisel verilerin işlenmesi sürecinde mevcut güvenlik standartlarının iyileştirilmesi hedeflenmiştir. ISO 29100 standardında bilgi iletişim sistemlerinde gizlilik arttırıcı teknolojiler tanımlanmıştır[201].

Veri Sorumluları ayrıca veri güvenliğine ilişkin olarak Kurul tarafından 6698 Sayılı Kanunun 22. maddesinin ç ve f bendi uyarınca belirlenen özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemler ile kurul tarafından düzenlenen veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla yapılan düzenleyici işlemlere de uymak zorundadır.

Mobil uygulamalarda veri güvenliği yükümlülüğüne uygunluk amacı çift yönlü işlemekte, bir tarafta cihaz sahibi kullanıcı, kendi verileri üstünde kontrol hakkına sahip olurken kendi sorumlu olduğu ölçüde verilerini korumak için tedbirlerini almalı, diğer yanda kişisel veriyi yöneten diğer veri sorumlusu cihaz ve işletim sistemi üreticisi, uygulama geliştirici, uygulama mağazaları da sorumlu oldukları ölçüde veri güvenliğini sağlamalıdır[202].

Mobil uygulama geliştiricilerin, yazılım hazırlamak için kullanılan bileşenlerdeki zafiyetleri tespit etmesi ve izlemesi kendilerinden beklenmektedir. İşletim sistemi ve cihaz üreticileri de aynı şekilde güvenlik açığı yönetim süreci belirleyerek uygulamanın kullanıldığı akıllı mobil cihazların kişisel verileri işlemeleri açısından zafiyetlerini düzenli olarak test ederek, güncellenmiş mobil uygulamaların olabildiğince erken sunulmasını ve kullanıcıların güncellemeleri yüklemeleri konusunda uyarılmasını sağlayacak metodları belirlemelidir.

Uygulama satıcıları, mağazalarına uygulamaları kabul etmeden önce belirli güvenlik kriterleri belirleyerek bunların ilgili uygulamada mevcut olmasına göre uygulamaları kabul etmektedir. Ayrıca mağazalar tarafından belirlenen kriterlerin uygulamada süreklilik arz etmesi için uygulamalar düzenli denetim ve testlere tabi

[201] Berber, Bilgili, s.10
[202] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.18

tutulmaktadır[203]. Google Play, uygulama geliştiricilere yönelik hazırladığı politikasında da uygulamanın, Google Play'in güncelleme mekanizması dışında bir yöntem kullanarak kendisini değiştiremeyeceği veya güncellemeyeceğini belirtmiştir[204]. Mobil uygulama kullanıcılarının da dikkatsizlik, tecrübesizlik veya bilgisizlik gibi zayıf yönlerinin kullanılması suretiyle kişisel verilerin başkasının eline geçme ve korunma konusunda farkındalığının arttırılması yönünde çalışmalara uygulamalar içerisinde yer verilmesi sağlanmalıdır. Aynı şekilde cihaz üretici ve işletim sisteminin mobil cihaz kaybolduğunda veya başkasına eline geçtiğinde cihaz içindeki ve uygulamalarda yer alan verilerin başka kişiler tarafından erişilmesine önleyici tedbirlerin olması örneğin mobil cihazlara kullanıcı dışında erişimi kolay olmayacak şekilde şifre üretilmesine izin verecek yapı ve kullanıcılara bunu teşvik edici şekilde tasarlanmış olması gerekir. Mobil cihaz kullanılmadığında otomatik olarak şifre ile korunması, uzun süre kullanılmayan uygulamaların sistemden kaldırılması için kullanıcıya uyarı verilmesi gibi güvenlik tedbirlerine imkan tanınmalıdır.

Kişisel verilerin saklanmasında şifreleme metodlarına uygun şekilde saklanması, işleme sistem ve servislerinin gizlilik, bütünlük, kullanılabilirlik ve esnekliğin sağlanması gerekir[205].

3.9.7.Veri Sorumluluları Siciline Kayıt Yükümlülüğü

6698 Sayılı Kanun'da veri sorumlusuna getirilen yükümlülüklere ilişkin olarak veri sorumluları siciline kayıt yükümlülüğü bulunan veri sorumlularının kişisel veri işleme envanteri ve kişisel veri saklama ve imha politikası hazırlaması gerektiği ve veri sorumlulularının kişisel veri işlemeye başlamadan önce Veri Sorumluluları Sicili'ne kayıt olmalarının zorunlu tutulduğu düzenlenmiştir. Konu ile ilgili çıkarılan yönetmelikte yer alan kriterler doğrultusunda kayıt yükümlülüğüne istisna

[203] https://play.google.com/intl/en-US/about/developer-content-policy-print/ Erişim Tarihi : 10.02.2020

[204] https://play.google.com/intl/en-US/about/privacy-security-deception/malicious-behavior/ Erişim Tarihi : 10.02.2020

[205] Işık,s.171

getirilebileceği de düzenlenmiş ve bu doğrultuda alınan kararla istisnalar belirlenerek resmi gazetede yayımlanmıştır[206].

3.9.8. Veri Koruma Otoritelerine Bildirime İlişkin Yükümlülükler

6698 Sayılı Kanun'un 12. maddesinin 5. fıkrası veri sorumlusuna, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirme yükümlülüğü getirmiştir. Maddenin devamında Kurul'un, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edeeği de düzenlenmiştir. Kurul buna ilişkin yayınladığı rehberinde, veri güvenliği ihlalini, işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi olarak tanımlamış örnek olarak da hizmet sağlayıcısının bilgisayar sisteminde bulunan müşterilere ait kişisel verilere, güvenlik ihlalleri nedeniyle internet aracılığıyla üçüncü kişiler tarafından erişilmesi, veri sorumlusunun veya veri işleyenin müşterilerine ait kişisel verilerin bulunduğu USB anahtarı veya CD-ROM'unun çalınması, özel nitelikli kişisel verilerin yer aldığı sabit diskin silinmeden internet üzerinden satılması gibi. durumları vermiştir[207]. Kurul'un 2019/10 sayılı kararı ile kurula yapılacak bildirimler için bu süre 72 saat olarak belirlenmiş, aynı kararda ilgili kişilere bildirimlerin ise "makul olan en kısa süre içerisinde" yapılması gerektiği ifade edilerek bildirim sırasında uyulması gereken usul ve esaslar belirtilmiştir[208].

3.9.9. Mobil Uygulamalarda Kişisel Verilerin Saklama Süresi

Veri sorumlulukları, uygulama geliştiriciler, mobil uygulamada toplanan verilerin depolanma süresini ve depolama riskini dikkate alarak yazılımı tasarlamalılardır. Saklama süresi, uygulamanın amacı ve verinin kullanımına göre değişmektedir. Örneğin takvim, günlük veya fotoğraf paylaşma uygulaması, verinin depolama süresini son kullanıcının kontrolüne bırakıcağı gibi navigasyon uygulamasında ise

[206] Kişisel Verileri Koruma Kurulu'un 02.4.2018 Tarih ve 2018/32 Sayılı Kararı
[207] https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/
[208] Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararı

uygulama tarafından sadece son gidilen belli sayıdaki konum verisinin saklanması yeterli olacaktır.

Uygulama geliştiriciler, kullanıcıların uygulamayı kullanmadıkları takdirde verilerinin belli bir süre sonra kendiliğinden silineceği bir altyapı oluşturmalılardır. Kullanıcıların, mobil cihazlarını kaybettikleri, çaldırdıkları veya cihaz değiştirdikleri ve kullanıcının eski cihazlarındaki uygulamaları silmedikleri durumlarda uygulama geliştiriciler kullanıcıların aktif olmadıkları dönem için bir zaman dilimi belirlemeli sonrasında da hesapla ilgili olarak kullanıcının son kullanma tarihi geçtiği bilgisini kullanıcıya iletecek bir alt yapı oluşturmalılardır. Bu zaman aralığının son geçerlilik tarihinde veri sorumlusu kullanıcıyı uyarmalı ve kullanıcıya kişisel verisini yeniden düzenlemesi için şans vermelidir. Kullanıcı bu uyarıya cevap vermezse kullanıcıyla ilgili kişisel veri ve uygulamanın kullanımı geri dönülmez şekilde anonimleştirilmeli veya silinmelidir. Hatırlatma periyodu ise uygulamanın amacına ve verinin saklandığı yere göre değişmektedir. Bir oyun uygulamasında en yüksek skor uygulama yüklü olduğu müddetçe saklanırken sadece yılda bir kere kullanılacak bir veri olduğunda örneğin kayak sezonunda otel ile ilgili bir bilgiye ilişkin hatırlatma en fazla 15 ay olabilecektir.

Uygulama, mobil cihazdan kaldırıldığında veri sorumlusunun sunucularından da tüm kişisel verinin kaldırılması mümkün olmalıdır. İşletim sistemi üreticisi, uygulama cihazdan kaldırıldığında kullanıcının verisini silmek için uygulama geliştiriciye haber vericek bir mekanizma kurmalıdır. Kullanıcı uygulamayı sildikten sonra uygulama geliştiricinin kullanıcı ile ilgili verileri işleyememesi bu yüzden de tüm veriyi silmesi gerekir. Eğer bir uygulama geliştirici belirli bir veriyi geliştirmeyi isterse örneğin kullanıcıya uygulamanın yeniden yüklenmesi halinde bilgilerin geri gelmesi gibi bir tercih hakkı verilecekse de uygulamanın kaldırma sürecinde bu konuda ve fazladan saklama süresi için kullanıcın rızasını ayrıca alması gerekir.

3.9.10. İlgilinin Haklarının Yerine Getirilmesi

6698 Sayılı Kanun'un 13. maddesinde veri sahiplerinin veri sorumlulularına başvurularına ilişkin hükümler düzenlenmiştir.

Tablo 3.4. Veri sahiplerinin veri sorumlulularına başvurularına ilişkin hükümler

13/a	Kişisel veri işlenip işlenmediğini öğrenme hakkı
13/b	Kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkı
13/c	Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme hakkı
13/ç	Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkı
13/d	Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkı
13/e	Kanun'un 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkı
13/f	13(d) ve 13(e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme hakkı
13/g	İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı
13/ğ	Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme hakkı

Veri sorumlusuna başvuruya ilişkin usul ve yöntemler KVKK tarafından 10.03.2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de ("Tebliğ") düzenlenmiştir. Kanunda ilgili kişi taleplerini yazılı veya Tebliğ'de belirlenen diğer yöntemlerle veri sorumlusuna ileteceği düzenlenmiir. Veri sorumlusuna yapılacak başvurunun zorlaştırılmaması gerektiği ise bir operatör şirketinin, ilgili kişinin internet sitesi üzerinden yapmış olduğu başvurusunu kimlik teyidi yapamadığı gerekçesiyle reddetmesine ilişkin olarak veri sahibi tarafından Kurul'a yapılan başvuru neticesinde verilen kararda yer almaktadır[209]. Kararda; veri sorumlusu şirketin veri sahibine kimlik teyidi sağlamak amacıyla yalnızca noter kanalı veya e-imza ile başvuruda bulunabileceğinin bildirilmesi sonucu 6698 Sayılı Kanun'da ya da Tebliğ'de öngörülmeyen maddi bir külfet getirmesi ve ilgili kişinin bu şekilde

[209] Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/296 Sayılı Kararı

yanlış yönlendirilmesi suretiyle söz konusu Kurul talep formunu doldurarak usule uygun bir başvuru yapma hakkının engellenmesinin Tebliğ'in 6'ncı maddesinde sayılan hukuka uygunluk ve dürüstlük kuralı ile bağdaşmayacağına ilişkin karar ile veri sorumlusu şirketin talimatlandırılmasına karar verilmiştir[210].

Veri Sorumlusu bu talepleri en kısa sürede ve en geç 30 gün içerisinde ücretsiz olarak sonuçlandırmakla yükümlüdür. İşlemin maliyet gerektirmesi halinde ücret alınabileceği de belirtilmiştir. Veri sorumlusu gelen talebi yazılı olarak veya elektronik ortamda cevaplandıracaktır. Talebi kabul ettiği takdirde gereğini yapacak, talebi reddettiğinde ise bunun gerekçesini açıklamak durmundadır. Başvuru sahibi cevabı yeterli bulmaz veya başvurusu reddedilir veya süresi içinde kendisine cevap verilmediği takdirde Kurul'a şikayet yoluna başvurabilecektir.

3.9.10.1. İlgilinin Bilgi Alma Hakkı

Mobil uygulama sistemindeki veri sorumluları, mobil uygulamaları, kullanıcıların bilgi edinme, düzeltme, sildirme, engelleme ve itiraz haklarını kullanmalarına olanak sağlayacak iletişim bilgisi vermelidir. Kişisel verileri işlenen bireyin bilgi alma hakkının asgari olarak şu hususları içermesi gerekmektedir: Veri sorumlusunda kendisine ait kişisel veri bulunup bulunmadığını bilme hakkı, verilerin işlenme amacını bilme hakkı, kendisine veri aktarılacak alıcı veya alıcı kategorileri ile verilerin kökenine yönelik bilgi alma hakkı[211]. Veri sahibinin bu haklarını kullanmak için kendisinden ilave kişisel veri alınmayacak şekilde kimlik doğrulaması yapılması da gereklidir.

Kişisel verilere ilişkin bilgi edinme hakkı, 6698 sayılı Kanun'un 11. maddesinde belirtilmiştir. Bu maddeye göre; aynı şekilde GVKT'nün 15. Maddesinde bilgilere erişim hakkına yönelik düzenlemeler mevcuttur. Bilgi edinme hakkının ücretsiz kullanılması zorunluluğu ise bulunmamaktadır[212].

---

[210] https://kvkk.gov.tr/Icerik/6557/2019-296

[211] Aydın Akgül, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yay, İstanbul, 2016, s.150

[212] Akgül, s.151

3.9.10.2. Silinme, Yok Edilme Veya Anonimleştirme Talep Hakkı

Unutulma hakkı olarak da tanımlanan bu hak, GVKT 17. maddesi kapsamında düzenlenmiştir. Buna göre kişisel verisi işlenen veri sahipleri, verilerinin toplanma amacı ile ilgili olarak tutulmasının gerekli olmadığı, rızalarının bulunmadığı yahut veri sahibinin verisinin işlenmesini istemediği veya kişisel verinin hukuka aykırı işlendiği durumlarda verilerinin silinmesini veya bundan sonra işlenmemesini talep edebilme hakkına sahiptir. Buna karşılık bazı istisna hallerin varlığı durumunda bu verilen tutulması hukuka uygun olarak değerlendirilmektedir. Bu istisnalar, bilgi ve ifade hürriyetinin kullanılması için gerekli olması, istatistik amaçlar, genel sağlık ve bilimsel araştırmalar, yasadan kaynaklanan durumlar ile kamu yararının varlığı halleri sayılmıştır.

Kişisel verilerin işlenmesi için uyulması gereken ilkelerden olan kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme ilkesi kapsamında her mobil uygulama, kişisel veriyi mevzuatta belirtilmiş bir süre varsa o süre sonunda her halükârda işlendikleri amaç için gerekli olan süre sona erdiğinde silmek zorundadır. Veri sorumlusu, Verbis'e kayıt olduğu sırada kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmek zorundadır. Türk Ceza Kanunun 138. maddesinde kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verileceği, suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek cezanın bir kat artırılacağı da hüküm altına alınmıştır.

6698 Sayılı Kanun'un 17. maddesinde kişisel verileri silmeyen veya anonim hâle getirmeyenler hakkında uygulanacak ceza ile ilgili olarak Türk Ceza Kanu'nun 138. maddesi hükmüne atıf yapılarak ayrıca bir düzenleme yapılmamıştır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve Kurul tarafından yayınlan rehberde; veri sorumlularınca, yönetmelikte yer alan asgari unsurları içerecek şekilde kişisel veri saklama ve imha

politikası hazırlaması, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi ile ilgili yapılan tüm işlemleri kayıt altına almaları gerektiği ve bu kayıtların diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süre ile saklamaları gerektiği belirtilmiştir.

EHK 10. maddesinde de kanun kapsamında sunulan hizmetler çerçevesinde eğer kişisel veriler soruşturma, inceleme de denetime konu olmuşlarsa bu ilgili soruşturma sona erene kadar, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarının iki yıl, kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtların ise asgari olarak abonelik süresince, saklanacağı veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma sürelerinin yönetmelikle belirleneceği düzenlenmiştir.

6698 Sayılı Kanun ve ilgili mevzuata uygun olarak işlenmiş olmasına rağmen işlemeyi gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, resen ya da ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

3.9.10.3. Kişisel verilerin Silinmesi

Bu kavram kişisel verilerin hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu bunun için gerekli her türlü teknik ve idari tedbiri almakla yükümlüdür[213]. Mobil uygulamalarda kişisel verilerin silinmesi yöntemlerinden birkaç tane örnek vermek gerekirse bunlar, bulut üzerinden silme, merkezi sunucudan silme, veri tabanından silmedir. İnternet üzerinden satın alınan Android işletim sistemi ile çalışan ikinci el telefonlarda yapılan çalışmada kullanıcılar verilerini cihazdan silseler dahi cihazda depolanan 40,000 kayıtlı fotoğraf, 1.500'den fazla çocukların bulunduğu aile fotoğrafı, 750'den fazla çıplak kadın fotoğrafı, 1.000'den fazla Google araması, 750'den fazla e-posta ve kısa

[213]https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb993bba31258508.pdf Erişim tarihi : 05.04.2018

mesaj, 250'den fazla iletişim bilgisi, eski telefon sahibi kimlik bilgisi ve bir tane tamamlanmış kredi başvurusuna tekrar ulaşılabildiği tespit edilmiştir[214].Ortalama teknik bilgiye sahip bir kullanıcının ilgili verilerini cihazda tekrar ulaşılamayacak şekilde yok edecek yöntemi bilmesi olası olmadığından cihaz ve işletim sistemi üreticilerinin silinen verilere tekrar ulaşılmasını önleyici bir yapı kurması önemlidir.

3.9.10.3.1. Kişisel Verilerin Yok Edilmesi

Verilerin bulunduğu tüm yedeklerin tespit edilerek fiziksel olarak imha edilmesi, hiçbir şekilde geri getirilememesi anlamına gelir.

3.9.10.3.2. Kişisel Verilerin Anonim Hale Getirilmesi

Anonim hale getirme, kişisel verilerin kimliği belli ve veya belirlenebilir gerçek kişi ile ilişkilendirilmeyecek şekilde değiştirilmesi ve ilgili kısımların çıkarılması anlamına gelmektedir. Verilerin anonimleştirilmesi veri minimizasyonu ilkesine uygun olarak gerçekleştirilmelidir. Anonimleştirmeden önce gerekli minimum kişisel veriler toplanmalıdır.

2002/58 Sayılı Direktif'in 6. maddesinin 1. fıkrasında, işlenen ve saklanan trafik verilerinin haberleşmenin temini için gerek duyulmadığı zaman, silinmesi veya anonimleştirilmesi gerektiği belirtilmiştir. e-gizlilik tüzüğü taslağında da meta verilerin ve elektronik haberleşme içeriğinin açık rıza dışında işlenmesi yasağı istisnası olarak anonim hale getirilememe yer almaktadır. Bununla birlikte, Madde 29 Çalışma Grubu, anonimleştirme tedbirleri uygulansa bile, hizmet sağlayıcıların daima veri koruma etki değerlendirmesi yapması ve hizmet sağlayıcıların verileri nasıl anonimleştirildiklerini ve topladıklarını halka açıklamak için ilave bir yükümlülük düzenlenmesini önermektedir[215].

[214]https://blog.avast.com/2014/07/08/tens-of-thousands-of-americans-sell-themselves-online-every-day/

[215]Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü, s.9

3.9.10.4. İtiraz Hakkı

Kişisel verilerin işlenmesi sonucunda bu verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmek suretiyle kişinin aleyhine bir sonuç çıktığı takdirde veri sahibi kişinin bu duruma itiraz etme hakkı, hem 6698 Sayılı Kanun'da hem de GVKT'de düzenlenmiştir. GVKT'de ilgili kişilerin, kişisel verilerinin doğrudan satışların gerçekleşmesi amacıyla pazarlama amacı ile kullanılması durumlarında, itiraz hakları ayrıca düzenlenmiş buna göre veri sahibi doğrudan pazarlama ile alakalı olduğu ölçüde profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin işlenmesine itiraz edebilecektir[216].

3.9.10.5. Kişisel Verisi İşlenen Kişinin Zararının Giderilmesini Talep Etme Hakkı

Kişisel verisi işlenen ve bu sebeple zarara uğrayan kişiler, 6698 Sayılı Kanun'un 11. maddesinin ğ bendi kapsamında veri sorumlusuna başvurarak zararının giderilmesini talep edebileceklerdir ancak tazminat talebinde bulunan kişinin ne kadar bir zarara uğradığının tespiti uygulamada sorun oluşturabilir. Kişinin ne kadar bir zarara uğradığının tespitinin, ticari menfaati ön plana tutan veri sorumlusuna bırakılması hukuka uygun bir çözüm getirmeyecektir. Bu sebeple bu hakkın mahkeme aracılığı ile talep edilmesi daha uygun olacaktır[217].

Bu durumda örneğin bankacılık faaliyetleri için mobil uygulama kullanan bir bireyin kişisel verilerinin hukuka aykırı olarak işlenmesi neticesinde kişinin mal varlığında bir azalma olması veya manevi itibarında bir zarar meydana gelmesi durumunda Türk Medeni Kanun'u 24. ve 25. maddeleri ile Borçlar Kanunu'nda yer alan ilgili maddeler dayanak olacak şekilde dava açılabilecektir. Aynı şekilde GVKT'nün 82. Maddesinde kişi aleyhine meydana gelen zararların tazmini öngören hükümler yer almaktadır[218]. Burada kusura dayanan bir sorumluluğun

[216] Kaya, s. 38
[217] Taştan, s.193
[218] Taştan, s.176

varlığından söz edilebilir[219]. Madde metninde manevi tazminat talebi düzenlenmediğinden manevi tazminatın talep edilip edilemeyeceği konusunda açıklık bulunmamaktadır[220]. Ancak, genel hükümler dâhilinde manevi tazminatın da istenebileceği kabul edilmektedir[221].

3.9.11. Verilerin Yurt dışına Aktarımı

Mobil uygulamalarda kişisel verilerin yurtdışına aktarılması mobil uygulama geliştiriciler ile işletim sistemi ve cihaz üreticilerinin bilgi yedeklerini bulut bilişimde saklamaları ve bu serverların genelde yurtdışında kurulu olması sebebiyle önem arz etmektedir. Özellikle bazı mobil cihazlarda kişinin cihazındaki tüm uygulamaları ile cihaz kimlik bilgisi, fotoğraflar ve rehber bilgisi bir hesapta kaydolmakta ve bu hesap cihazın bulut hesabında yedeklenmektedir. Kullanıcı cihazını kaybettiğinde veya başka bir cihaz kullanmaya başladığında kendi hesabındaki bilgileri otomatik olarak diğer cihazından indirebilme imkanı sağladığından bu yöntem tercih edilmektedir.

6698 Sayılı Kanun'da kişinin açık rızası olmadan bilgilerinin yurtdışına aktarılamayacağı düzenlenmiştir. Ancak kanunda açık rıza aranmayan hallerin varlığı halinde ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması veya yeterli koruma olmadığı takdirde de Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlusunun yeterli korumayı taahhüt etmesi ve kurulun izni olması durumunda kişisel verilerin yurtdışına aktarılabileceği düzenlenmiştir. Yeterli korumanın bulunduğu ülkeler listesinin Kurul tarafından belirleneceği de aynı maddede düzenlenmiş olup hali hazırda Kurul tarafından bu liste hazırlanmamıştır.

Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verilerinin ancak ilgili kişilerin açık rızaları

[219]Hayrünnisa Özdemir, Erzincan Binali Yıldırım Üniversitesi, Hukuk Fakültesi Dergisi, Haberleşmenin Gizliliği ve Kişisel Veriler, s.300 Bknz. Ehmann/Helfrich, 280, pn.15; 141. http://hukukdergi.erzincan.edu.tr/wp-content/uploads/2015/10/2009-XIII_1-11.pdf, Erişim Tarihi : 10.10.2018

[220] Özdemir, s.300 Bergmann/Möhrle/Herb, §7 pn. 9; Wedde, pn. 91.

[221] Özdemir, s.300 Brühann/Zerdick, 429(435).

alınmak koşuluyla yurt dışına aktarılabileceği de EHK 51. maddesinin 6. fıkrasında düzenlenmiştir.

3.10. VERİ KORUMA OTORİTELERİ TARAFINDAN MOBİL UYGULAMALAR ÖZELİNDE VERİLEN ÖRNEK KARAR ÖZETLERİ

3.10.1. Mobil Uygulama Bağlantılı Oyuncak – Fransız Veri Koruma Otoritesi Soruşturması

Genesis Industries Limited tarafından çocuklar için üretilen bebek 'My Friend Cayla' ve 'I-Que' adlı robot, internet bağlantılı oyuncaklar olarak adlandırılmakta, üzerindeki mikrofonla ve hoparlör yardımıyla çocuklar tarafından matematik problemi veya hava durumu ile ilgili sorulan sorulara mobil cihazlara indirilen mobil uygulamayla bağlantı kurarak cevap vermektedirler. Sorulan sorulara verilecek cevaplar mobil uygulama aracılığı ile internetten alınarak oyuncak aracılığı ile çocuklara iletilmektedir. Bu oyuncaklara ait mobil uygulamanın 2002/58 Sayılı Direktif'in 5. maddesinin 3. fıkrasına aykırı olduğu ve güvenlik zafiyeti gerekçesi ile Fransız Veri Koruma Otoritesi CNIL tarafından oyuncağı üreten şirkete karşı soruşturma başlatılmıştır.

Yapılan kontrollerde oyuncakları üreten şirketlerin çocukların kendileri, arkadaşları ve aileleri hakkında sayısız kişisel veri topladığı bunların içinde ses verileri, oyuncaklarla yapılan içeriğinde kişiyi belirlenebilir kılan isim ve adres bilgilerinin olduğu konuşma içerikleri, ayrıca oyuncağın kendisine ait mobil uygulamasında da oyuncak sahiplerine form doldurtularak çeşitli bilgilerin işlendiği anlaşılmıştır.

Fransız Veri Koruma Otoritesi yetkilileri oyuncaktan 9 metre uzaklıkta olan herhangi birinin de herhangi bir kullanıcı adı veya şifre girme zorunluluğu olmadan veya oyuncaktaki herhangi bir düğmeye basmadan kablosuz ağ veya bluetooth yardımı ile telefon ile oyuncağa bağlanabildiğini tespit etmişlerdir. Bu uzaklıktaki herhangi biri, çocuk ve oyuncak arasındaki veya yakınlardaki bir konuşmayı dinlemekte ve kaydedebilmektedir. Yetkililer ayrıca iki metotla da oyuncakla oynayan çocukla iletişime geçilebildiğini gözlemlemişlerdir. Bunlardan ilki

hoparlör aracılığı ile önceden kaydedilen seslerin veya kelimelerin çıkarılmasıyla veya oyuncakta yer alan eller serbest uygulamasıyla oyuncağın yakınındaki çocuklar konuşmak için oyuncağın bağlantılı olduğu telefonu araması şeklindedir.

Fransız Veri Koruma Otoritesi Başkanı bu oyuncaklarla ilgili güvenlik zafiyetinin, çocukların ve oyuncak sahiplerinin haberleri olmadan arkadaşlar ve aile arasındaki konuşmalara erişimin Bluetooth fonksiyonu ile bağlantı kurularak sağlanmasının Fransız Veri Koruma Kanununun 1. maddesinde yer alan bilgi teknolojisinin kişinin kimliği, insan haklarını, mahremiyetini veya bireysel veya kamusal özgürlüklerini ihlal etmemeli hükmüne aykırılık taşıdığına karar vermiştir.

Oyuncak kullanıcılarına eksik bilgi verilmesi, şirketin kişisel verileri işlemesine rağmen, kurum üyeleri tarafından oyuncak sahiplerinin kişisel verilerin işlenmesi bakımından yeterince bilgilendirilmediklerini ayrıca konuşma içeriklerinin AB üye olmayan ülkelere transfer edildiği konusunda da yeterince bilgilendirilmediği anlaşılmıştır.

Fransız Veri Koruma Otoritesi resmi bir bildirim ile oyuncak üreten şirkete iki ay içerisinde kanunla uyumlu hareket etmek üzere ihtarda bulunmuştur. Mahremiyetin ihlal edilmesi ve konunun kamuyu ilgilendirmesi ve güvenlik zafiyetini bildirme yükümlülüğü kapsamında kurul yönetimi bu ihtarı kamuya duyurmuştur.

Şirkete belirtilen zaman diliminde gerekli uyumlulukları yapması için 2 aylık süre verilmiş, bu uyumlulukları yerine getirmediği takdirde yaptırım uygulayacağı bildirilmiştir[222]. Şirket kendisine verilen süre zarfında Fransız Veri Koruma Otoritesinin ihtarında yer alan gereklilikleri yerine getirmiş ve soruşturma kapatılmıştır.

[222] https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security Erişim Tarihi : 02.04.2018

3.10.2. Mobil Mesajlaşma Uygulaması - Norveç Veri Koruma Otoritesi Tarafından Verilen Ceza

Oslo'da faaliyet gösteren bir eğitim kuruluşunda kullanılmak üzere veli ve öğrencilerin, okul personeline mesaj gönderebilmesini sağlamak amacıyla bir mobil mesajlaşma uygulaması geliştirilmiştir. Norveç Veri Koruma Otoritesi, mobil uygulamada bilgi güvenliğini korumak için teknik ve organizasyonal önlemlerin yetersiz olması ve bu sebeple yetkisiz kişilerin uygulamaya yetkili kullanıcı olarak giriş yapabilmeleri ve bu kişilerin öğrenciler, veliler ve çalışanlar hakkındaki kişisel verilere erişebilmelerine olanak sağladığı gerekçesiyle 29.04.2019 tarihinde Oslo Şehir Eğitim Departmanına 203.000 Euro para cezası kesilmesine karar vermiştir[223] [224].

3.10.3. Futbol Mobil Uygulaması – İspanya Veri Koruma Otoritesi Tarafından Verilen Ceza

İspanya'nın profesyonel futbol ligi olan Laliga tarafından taraftarların maç ve istatistikleri takip etmeleri amacıyla hazırlanan Laliga mobil uygulamasının kullanıcıların cihazlarındaki mikrofon ve GPS verilerine erişerek yasadışı maç yayını yapan barları tespit ettiği anlaşılmıştır. Bunun üzere İspanya Veri Koruma Otoritesi, mobil uygulamanın kullanıcılarını yeteri kadar bilgilendirmediği, mobil uygulamanın rızanın geri alınmasına ilişkin gereklilikleri karşılamadığı, ve bilgilendirme yükümlülüğünü yerine getirmediği gerekçeleri ile GVKT 7.maddesi 3. fıkrasına aykırılık nedeni ile Laliga'nın 250.000 Euro para cezası ödemesine karar vermiştir[225].

[223] http://www.enforcementtracker.com/ Erişim Tarihi : 06.10.2019
[224]https://www.datatilsynet.no/contentassets/f7246f38ff394d32bef6895bc65a4b4f/varsel-om gebyr---oslo-kommune.pdf Erişim Tarihi : 06.10.2019
[225] http://www.enforcementtracker.com/ Erişim Tarihi : 06.10.2019

3.10.4. Facebook Yüz Tanıma Yoluyla Arkadaş Bulma Sistemi – Hamburg Veri Koruma Otoritesi Soruşturması

Facebook, yüz tanıma yoluyla arkadaş bulma sistemini geliştirdiğinde yeni kullanıcılar tarafından uygulama ilk indirildiğinde kullanım şartları ve koşullarında, arkadaş bulmak için yüzün tanınmasına rıza gösterilmesine yer vermiştir. 21 Eylül 2012 tarihinde Hamburg Veri Koruma Komisyonu, standart şartlar ve koşullarda atıfta bulunulmasının kullanıcının açıkça bilgilendirildiği rıza olarak kabul edilemeyeceği gerekçesiyle Facebook aleyhine soruşturma başlatılmasına karar vererek Facebook'a ilgili aykırılığı düzeltmesi için süre vermiştir. Komisyon, söz konusu idari kararı verilen sürede yerine getirilmemesi halinde Facebook'un biometrik veri tabanının silinmesi kararını vermiştir. Facebook 7 Şubat 2012 tarihinde Komisyon kararını süresinde yerine getirmiştir [226].

3.10.5. Rehberlik Hizmeti Veren İnternet Sitesi ve Uygulamalar – Türkiye Kişisel Verileri Koruma Kurumu İlke Kararı

Get Contact adı verilen bir uygulama, indirildiği cihazdaki telefon rehberine erişmek suretiyle kişilerin kendi telefon numaralarını başkalarının rehberinde nasıl kaydedildiğini görebilme imkanı sağlaması bakımından popüler olmuştu. Uygulamanın, kişinin cihazındaki bilgileri kopyalayarak bu uygulamayı kullanan başka kişilerle paylaştığı anlaşılmıştır.

Bu mobil uygulama ile ilgili olarak kişilerin açık rızaları alınmaksızın isimden telefon numarası veya telefon numarası bilgisinden isim sorgulaması yapılmasına izin veren ve başkasının telefon rehberinde nasıl kayıtlı olunduğunu öğrenme gibi konularda rehberlik hizmeti vermesi neticesinde Kurul'a ihbar ve şikayetler iletilmiş, Kurul'un 21.12.2017 tarih 2017/61 sayılı ilke kararı ile kanunda ve ilgili mevzuatta dayanağı bulunmaksızın ilgili kişilerin iletişim bilgilerinin paylaşımını yapan internet siteleri ve mobil uygulamalar tarafından gerçekleştirilen veri işleme faaliyetinin 6698 Sayılı Kanun'un 15. maddesinin 7. fıkrası uyarınca derhal

[226]Ayözger, s.126

durdurulması gerektiği, söz konusu site ve mobil uygulamanın bu işleme son vermediği takdirde TCK'nın Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" başlıklı 136. maddesi çerçevesinde ilgili internet siteleri/uygulamaları hakkında gerekli hukuki işlemlerin tesisi için konunun Ceza Muhakemesi Kanununun 158. maddesi uyarınca ihbaren Cumhuriyet Başsavcılığına bildirileceğine ve bu karara uymayanlar hakkında 6698 Sayılı Kanunun 18. maddesi kapsamında işlem yapılmasına karar verilmiştir.[227]

[227] https://kvkk.gov.tr/Icerik/4113/2017-61 Erişim Tarihi : 05.10.2019

DÖRDÜNCÜ BÖLÜM

ÖRNEK OLAY İNCELEMESİ

4.1. CAMBRİDGE ANALYTİCA – FACEBOOK VERİ İHLALİ

2018 yılında İngiliz yayın kuruluşu Channel 4 haber kanalı tarafından yürütülen gizli bir araştırma sonucunda, Donald Trump'ın 2016 yılındaki seçim kampanyasında veri analiz firması olarak faaliyet gösteren İngiltere merkezli Cambridge Analytica şirketi tarafından veri ihlali[228] gerçekleştirildiği ve söz konusu ihlal neticesinde 87 milyona yakın ABD vatandaşının etkilendiği ortaya çıkarılmıştır.

Facebook platformunda yer alan anket temelli kişilik testi uygulamasıyla ABD'de yaşayan yetişkinlerden elde edilen veriler ile bu kişilerin karakter özellikleri, siyasi düşüncesi ve yaşam tarzları analiz edilerek[229] seçmen profili oluşturulmuştur. Karşıt görüşlü seçmenlere oy tercihini değiştirecek, taraftarlara ise tercihlerini pekiştirecek içerikte seçmen profiline özel dijital video içerikleri üretildiği ve netice itibariyle seçim kampanyasının bu şekilde kazanıldığı iddia edilmiştir.

4.1.1. Veriler Nasıl Toplandı ?

2014 yılında Cambridge Üniversitesi'nde Profesör olarak görev yapan Alexsandr Kogan, ABD seçmeni hakkında ayrıntılı psikolojik profil çıkarmak amacıyla "thisisyourdigitallife" adıyla bir anket uygulaması geliştirmiştir. Bu uygulamayı

---

[228] Kişisel veri ihlali kavramı, GVKT tanımlar başlıklı 4. maddesinde; paylaşılan, saklanan veya başka şekilde işlenen kişisel verilerin kazara veya hukuka aykırı şekilde imha edilmesi, kaybedilmesi, değiştirilmesi, yetkisiz şekilde ifşa edilmesi ve bunlara erişilmesine imkan veren bir güvenlik ihlali olarak tanımlanmıştır. 6698 Sayılı Kanun'da açık bir tanım bulunmamakla birlikte, bu kavramın sadece işlenen kişisel verilerin kanuni olmayan yollarla ele geçirilmesi olarak tanımlandığı anlaşılmaktadır.

[229] Stanford Üniversitesi'nde öğretim üyesi ve veri madencisi Michal Kosinski isimli araştırmacı, bireylerin Facebook beğenilerinden yola çıkarak kişilik özelliklerini, politik eğilimlerini, yaşam tarzlarını ve diğer pek çok özelliği tespit edebilen bir yöntem geliştirmiştir. https://www.researchgate.net/profile/Ahmet_Oezker/publication/330703883_Financial_Performance_Objective_of_Public_Expenditures_in_Last_Period_and_Its_in_Connected_with_Economic_Budget_in_Turkey/links/5c503e9192851c22a3989c81/Financial-Performance-Objective-of-Public-Expenditures-in-Last-Period-and-Its-in-Connected-with-Economic-Budget-in-Turkey.pdf#page=16, Erişim Tarihi : 10.10.2019

indiren kişilerden Facebook hesap bilgilerine erişim izni istenmiş ancak uygulama sadece indiren kişinin değil bu kişinin Facebook profilinde yer alan arkadaş listesinde ekli kişilerden de veri toplamıştır. Kogan, Amazon'un Mechanical Turk ("Mturk")[230] projesini kullanarak uygulamayı hayata geçirmiş ve ankete katılan MTurk kullanıcılarına 1'er dolar ödeme yapmıştır. Bu uygulama, 300 bin kişi tarafından indirilerek kullanıcılarla birlikte kullanıcıların arkadaşlarının da bilgilerinin toplanmış ve yaklaşık 87 milyon kişilik devasa bir kullanıcı bilgisine ulaşılmıştır[231]. 2015 yılında İngiliz gazetesi "The Guardian", bu verilerin, Alexsandr Kogan tarafından kurulan şirketin Cambridge Analytica ile iş yapan bir başka şirketle anlaşması neticesinde Cambridge Analytica'ya satıldığını haber yapmıştır[232]. Bu durum veriye verilen önemi ve verinin maddi bir mal olarak satıldığını göstermesi açısından da önemlidir.

4.1.2. Hangi Veriler Toplandı ?

ICO tarafından Facebook şirketi aleyhine verilen 24 Ekim 2018 tarihli kararda; Kogan tarafından geliştirilen uygulama ile kullanıcının Facebook profilindeki ismi, cinsiyet bilgisi, kullanıcı profilde paylaşmışsa yaşadığı şehir bilgisi, kullanıcının etiketlendiği fotoğraflar, kullanıcının beğendiği sayfalar, gönderiler, haber kaynağı, arkadaş listesi, adresler, e-posta adresleri ve facebook mesaj içeriklerine erişildiği yer almaktadır. Uygulamanın kullanıcının arkadaş listesindeki kişilerin verilerinden ise Facebook profili isim, cinsiyet, kullanıcı bilgisini ve kişi profilinde paylaşmışsa yaşadığı şehir bilgisi, kullanıcının etiketlendiği fotoğraflar, kullanıcının beğendiği sayfalara erişildiği tespit edilmiştir[233].

---

[230] İsmini Avusturya-Macaristan asıllı Wolfgang Von Kempelen tarafından 1770 yılında icat edilen adını yarı otomatik satranç makinasından alan Amazon tarafından dijital işlerin yapılması ve yaptırılması amacıyla hareket eden kişileri buluşturmak için tasarlanmış bir nevi online işgücü pazar yeri uygulaması.

[231] ICO tarafından Facebook şirketi aleyhine verilen 24 Ekim 2018 tarihli karar, https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf , s.12, Erişim Tarihi : 10.10.2019

[232] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data. Erişim Tarihi : 10.10.2019

[233] https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf, Erişim Tarihi : 10.10.2019

4.1.3. Facebook Şirketinin Rolü ve Alınan Aksiyonlar

Facebook şirketinin kurucusu ve CEO'su Mark Zuckerberg, 21 Mart 2018 tarihinde kişisel Facebook sayfasında[234]; Cambridge Analytica Skandalı ile ilgili olarak açıklama yaparak, Aleksandr Kogan tarafından geliştirilen uygulama ile milyonlarca kişinin verisine erişildiğini kabul etmiş ve özür dilemiştir. Zuckerberg; bu durum neticesinde Facebook platformlarında değişikliklere gidildiği, uygulama sahiplerinin platformda yer alan veriye erişiminin sınırlandırıldığı, 3.kişiye ait verilerin ancak veri sahipleri tarafından rıza verildiği takdirde toplanabileceği ve uygulamanın Facebook şirketinden izin almadan hassas verilere erişemeyeceğini açıklamıştır. Bu açıklama ile Zuckerberg, Facebook şirketinin kişisel verilerin işlenmesi ile ilgili ilkelere uygun hareket etmediğini bu skandal ortaya çıkmadan öncesine kadar teknik ve idari tedbirleri almadığını da kabul etmiş olmaktadır.

Açıklamanın devamında Zuckerberg, 2015 yılında Kogan'ın verileri Cambridge Analytica'ya sattığını öğrenmesi üzerine veri sahiplerinin rızası olmadan verilerin transfer edilmesinin Facebook gizlilik politikasına aykırı olması sebebiyle uygulamanın kaldırıldığını, iki şirketten de verilerin silindiğine dair belge talep edildiğini ve uygulama geliştiricilerin veri erişimini sınırlayıcı, örneğin uygulamanın 3 aylık sürede kullanılmaması halinde uygulama geliştiricinin kişi verisine erişiminin kalıdırlması, uygulamaya kaydolmak için minumum veri alınması gibi önlemlerin alındığı, kullanıcılara ana sayfalarında uygulamalara verdikleri izinleri yönetecekleri yöntemlere yer vereceklerini belirterek Facebook platformunun daha güvenli olması için gereken aksiyonları aldıklarını belirtmiştir.

4.1.4. Verilen Kararlar

ICO, FTC tarafından Facebook şirketi ve Cambridge Analytica CEO'su ve uygulama geliştirici aleyhine yürütülen soruşturmalar neticesinde taraflar ile anlaşmaya varılmış ve aşağıda ayrıntıları yer alan kararlar alınmıştır.

[234] https://www.facebook.com/zuck/posts/10104712037900071, Erişim Tarihi : 10.10.2019

Ayrıca bu olay ile ilgili olarak Facebook şirketi aleyhine açılan ve ABD San Francisco mahkemelerinde görülen yargılama hala devam etmektedir.

4.1.4.1. ICO Tarafından Verilen Karar

İngiltere Bilgi Komisyonu Ofisi ("ICO") 24 Ekim 2018 tarihinde Facebook'a Cambridge Analytica olayındaki rolü için başlattığı soruşturmada, Facebook'un kişisel verilerin güvenliğini sağlamada yetersiz olduğu, Cambridge Analytica tarafından bu verilerin izinsiz bir şekilde işlenmesine izin verdiği ve 87 milyon kişinin verisinin ihlal edildiği gerekçesiyle 400.000 Sterlin para cezası ödemesine karar vermiştir. Aradan geçen 1 yıllık dava ve temyiz süreci sonrasında Facebook, ICO ile anlaşmaya vararak Ekim 2019 tarihinde cezayı ödemeyi kabul etmiş ve ihtilafı anlaşma yoluyla çözmeyi tercih etmiştir.

Karar, ihlalin işlendiği tarihte yürürlükte bulununan İngiliz Veri Koruma Yasası hükümleri çerçevesinde alınmıştır.

Kararın gerekçesinde; uygulamayı kullanan kişilere, kişilerin arkadaşlarına ait veriler ile bu kişilerle mesajlaşan kişilere ait verilerin haksız bir şekilde işlendiği, uygulamayı indiren kişilerin arkadaşlarından rıza alınmadan verilerinin toplandığı, verilerinin işlenmesi ile ilgili bilgi verilmediği, bu tarz bir veri işlemenin şirket politikasında yasaklanmadığı, her ne kadar bu işlemenin kullanıcıların rızası ile olduğu düşünüldüyse de hukuki anlamda açık ve anlaşılır bir bilgilendirmeye dayanmaması sebebiyle geçersiz olduğu ve bu sebeple veri işlemenin hukuki bir temele dayanmadığı, Facebook şirketinin veri sorumlusu olarak yetkisiz ve hukuka aykırı veri işlenmesini önleyici teknik ve idari tedbirleri almadığı, Facebook şirketinin söz konusu uygulamanın gizlilik politikasına uygun davranıp davranmadığını ve uygulamanın yaptığı faaliyeti kontrol etmediği, hatta bu haber, Guardian gazetesinde ifşa edilene kadar Facebook'un durumdan haberdar olmadığı hususları yer almıştır[235].

[235]https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf, Erişim Tarihi : 10.10.2019

4.1.4.2. Federal Ticaret Komisyonu (“FTC”) Tarafından Verilen Karar

ABD kişisel verilerin korunmasına yönelik federal bir kanuna sahip olmamasına rağmen ülkede veri koruması, gizlilik ile ilgili düzenlemeler çerçevesinde sağlanmaktadır. Federal düzeyde veri koruma düzenlemelerinin uygulanması ve kişisel verinin korunması hususu, Federal Ticaret Komisyonu (“FTC”) tarafından yerine getirilmektedir. Bu sebeple mezkur olayla ilgili FTC tarafından Facebook şirketi aleyhine soruşturma başlatılmış ve soruşturma[236] neticesinde Facebook’un 5 milyar dolar ceza ödemesine hükmedilmiştir. Söz konusu para cezası, şimdiye kadar gizlilik ve veri ihlali sebebiyle verilmiş en yüksek para cezası olmuştur. FTC tarafından para cezasının yanı sıra hesap verilebilirlik ilkesini şirket yönetimi içerisine yerleştirecek kararlar ile şeffaflık ilkesi gereğince şirket tarafından FTC’ye belirli periyodlarda rapor verilmesi, en az 500 kullanıcıyı etkileyen veri ihlallerinde Facebook şirketinin FTC´yi bilgilendirmesi ve mevcut sorunların çözümlerine ilişkin belgeleri 30 gün içinde FTC´ye sunması gibi şirketin iç yapısını değiştirecek kararlar da alınmıştır[237].

Facebook şirketinin kurucusu ve CEO'su Mark Zuckerberg'in kullanıcı gizliliğini etkileyen kararlar üzerindeki kontrolsüz denetiminin kaldırılması ve bu konudaki yetkinin üyelerinin bağımsız bir aday gösterme komitesi tarafından atandığı ve yalnızca Facebook yönetim kurulunun nitelikli çoğunluğu ile işten çıkarılabildiği bağımsız bir gizlilik komitesine verilmesi ile hesap verilebilirlik ilkesi yönetim kurulu seviyesine çıkarılmıştır. Ayrıca söz konusu hesap verilebilirlik ilkesi bireysel seviyede de arttırılmış ve Facebook şirketinin gizlilik programından sorumlu olacak olan uyumluluk görevlilerini tayin etmesi gerektiği, bu uyumluluk görevlilerinin, yeni yönetim kurulu gizlilik komitesinin onayına tabi olduğu ve Facebook şirketinin CEO’su veya Facebook şirketinin yöneticileri tarafından değil, yalnızca bu komite tarafından görevlerine son verilecekleri bir yapı kurması beklendiği hususlarında Facebook şirketine ilave sorumluluklar yükletilmiştir.

[236]https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf

[237]https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Kararın devamında; Facebook şirketi CEO'su Mark Zuckerberg ve tayin edilen uyumluluk görevlileri tarafından şirketin kararın gerektirdiği gizlilik programına uygun olduğuna dair sertifikaları 3 aylık periyotlarda ve her yıl şirketin genel olarak karara uygun olduğuna ilişkin sertifikaları FTC'ye sunacağı, herhangi bir şekilde gerçeğe aykırı sertifikasyonlarında ise hukuki ve cezai yaptırımlara maruz bırakılacağına ilişkin düzenlemeler de yer almıştır. Ayrıca Facebook, kararın gerekli kıldığı gizlilik programını, WhatsApp ve Instagramı da kapsayacak şekilde kurgulayacak ve her yeni ürün, hizmet ve yönetimin Facebook platformunda sunulmadan önce gizlilik incelemesi yapmak suretiyle ve kullanıcı gizliliği hakkındaki kararlarını belgelendirerek hareket edeceği bir yapı oluşturacaktır.

Bunun dışında, Facebook şirketinin platform politikalarına uygun olmayan veya belirli kullanıcı verilerine olan gereksinimlerini gerekçelendiremeyen uygulama geliştiricileri sonlandırmak; yüz tanıma teknolojisinin kullanımı hakkında net ve dikkat çekici bir bilgilendirme yapmak ve kullanıcılardan buna ilişkin açık rıza almak, kapsamlı sürdürülebilir bir veri güvenliği programı oluşturmak, kullanıcı şifrelerini şifreleyerek bu şifrelerin düz metinde saklanıp saklanmadığını tespit etmek için düzenli olarak tarama yapmak için gerekli aksiyonları alması beklenmektedir.

4.1.4.3. ABD Menkul Kıymetler ve Borsalar Komisyonu Tarafından Verilen Karar

Facebook şirketi, ICO ve FTC dışında ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC) ile de anlaşma yapmıştır. SEC tarafından başlatılan soruşturma sonunda verilen karar gerekçesinde; Facebook şirketinin 2015 yılında kullanıcılarının bilgilerinin kötüye kullanıldığını keşfetmesine rağmen söz konusu açıklığı, iki yıldan fazla bir süredir düzeltmediği, bunun yerine, yatırımcılara "kullanıcılarımızın verilerine uygunsuz bir şekilde erişilebildiğini, kullanılabildiğini veya ifşa edilebildiğini" söylemeye devam ettiği, Cambridge Analytica'nın Facebook kullanıcılarına ait verilerin kullanımına ilişkin yaptığı araştırmada herhangi bir uygunsuzluğun olduğunun kanıtlanmadığını söylemesi

ancak olayın Mart 2018'de söz konusu ifşanın şirket tarafından kabul edildiğinde ise hisse senedi fiyatları düşmesi gibi halka açık bir şirketin işletmeye yönelik bu kadar önemli riskleri kamuoyu ile paylaşmaması buna ilişkin politika ve prosedürlerinin olmamasını da şikayet konusu yapmıştır. Soruşturma sonunda Facebook şirketi SEC ile anlaşmaya vararak 100 milyon dolarlık ceza ödeyemeyi kabul etmiştir[238].

4.1.4.4. Cambridge Analytica ve Yöneticileri Hakkında Verilen Kararlar

FTC tarafından Cambridge Analytica ve yöneticileri aleyhine başlatılan[239] idari soruşturma ve dava sürecinde[240], şirket ve iştirakleri iflas ettiğini ilan etmiştir. FTC ile Cambridge Analytica eski CEO'su Alexander Nix ve uygulamayı geliştiren Aleksandr Kogan gelecekte yürütecekleri faaliyetler bakımından bir takım kısıtlayıcı idari yaptırımlara uygun şekilde iş yapacakları ve mevcut toplanan tüm kişisel bilgiyi yok etmek ve silmek konusunda anlaşmaya varmıştır.

[238] https://www.sec.gov/news/press-release/2019-140, Erişim Tarihi : 10.10.2019

[239] https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf, Erişim Tarihi : 10.10.2019

[240] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer, Erişim Tarihi : 10.10.2019

Büyük veri içerisindeki kişisel verilerin veri eşleştirme ve veri madenciliği gibi teknikler ile üretilmesi sonucu ortaya çıkan yeni veriler[241], topluma faydalı amaçlarla kullanılabileceği gibi manipülasyon ve algı yönetimi gibi olumsuz amaçlarla da kullanılabilmektedir.

Örneğin üniversiteler, büyük veriyi insan genetiği ve genetiğe dayalı hastalıkların araştırılması için kullanmakta, veri madenciliği yöntemiyle her yıl dünya grip haritası çıkarılarak salgın hastalıkların tespit edilmesi mümkün hale gelmektedir. Aynı şekilde biometrik verilerin kişiye özgü olması, kopyalanma ve çalınma ihtimalinin olmaması gibi sebeplerle şifre, doğrulama vb. yöntemlerde kullanılması, konuya özel buluşları yaygınlaştırmıştır. Bu buluşlar, şifre vb. yöntemlere aşina olmayan kişilerin, alzeimer hastalarının veya belli konularla engelli olan insanların biometrik verileri ile işlem yapmalarını kolaylaştırmış, yapılan işlemlerde sahtecilik ve dolandırıcılığı minumum seviyeye indirgeyerek, ulusal ve uluslararası güvenliğin sağlanmasına katkı sağlamıştır.

Diğer tarafta Cambridge Analytica örneğinde olduğu gibi basit bir kişilik testi ile elde edilen kişisel verilerin politik tercihlere nasıl yön verebileceği açıkça gözler önüne serilmiştir. Bu olay, kişisel verilerin bireylerin seçim ve tercihlerini manipüle etmeye yönelik gizli amaçlarla da işlenebileceğini göstermesi bakımından modern çağda özgür irade kavramının sorgulanmasına neden olmuştur.

Gizlilik ve mahremiyet kavramının kökeni antik çağlardaki hipokrat yeminine kadar uzanmaktaysa da[242] 1903 yılına kadar bu konuda herhangi bir kanuni bir düzenleme yapılmamıştır. İlerleyen süreçte bilgi teknolojilerinin ortaya çıkışı ve bilginin otomatik yollarla işlenmesi faaliyetinin artması ile birlikte özel hayatın gizliliği hakkına ilişkin koruma yetersiz kalmıştır.

---

[241] Artuç, Murat, Mahremiyet Açısından Birey Devlet İlişkisi, 2015, Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, Anayasa Mahkemesi'nin 09/04/2014 tarihli 2013/122 esas ve 2014/74 sayılı kararı, s.111, http://adudspace.adu.edu.tr:8080/xmlui/bitstream/handle/11607/1502/10075513.pdf?sequence=3&isAllowed=y, Erişim Tarihi : 10.10.2019

[242] Aydın, Sedat Erdem, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, Aralık, 2015, s.9, Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.6

Kişisel verilerin korunması konusundaki ilk uluslararası düzenleme, 1981 yılında Avrupa Konseyi tarafından ihdas edilen sözleşme[243] ile olmuştur. 1981 yılından GVKT'nin yürürlük tarihi olan 2018 yılına kadar geçen süreçteki hukuki gelişmelerle kişisel verilere ilişkin eksik ve açıkta kalan noktaları tamamlayıcı ve düzenleyici yenilikler getirilmişse de Cambridge Analytica olayı, mevcut yasal düzenlemelerin, kişisel verilerin korunması bakımından yeterince caydırıcı olmadığı ve kendisinden beklenen korumayı sağlamakta yetersiz kaldığını göstermiştir. Bu olayın ifşa olması, Facebook şirketinin kurucusu ve yöneticisinin milyonlarca kişinin verisinin rızası dışında farklı amaçlarla işlendiğini kabul etmesi, kişisel verilerin korunması kapsamında yeni düzenlemeler yapılmasını gerekli kılmıştır. Nitekim GVKT'da düzenlenen Unutulma Hakkı, ilk kez İspanyol bir avukatın Avrupa Adalet Divanı'na yaptığı başvuru neticesinde verilen karar[244] ile ortaya çıkmıştır. İspanyol avukat, Google arama motorunda kendisi hakkındaki bilgilere ulaşılabilir olmasının o dönem yürürlükte olan 95/46 Sayılı Direktif'e aykırı olduğu gerekçesi ile Avrupa Adalet Divanına başvurmuş ve yapılan yargılama neticesinde; veri sahiplerinin tutulmasında kamu yararı bulunmayan ve artık güncel olmayan bir verilerin silinmesini talep etme hakkı olduğuna hükmedilmiştir[245].

ABD'de federal düzeyde koruma sağlayan bir veri koruma yasası bulunmamasına rağmen FTC tarafından Facebook'a uygulanan para cezası dışında dikkat çeken nokta, şirketin iç işleyişine de yönelik bir dizi düzenleme getirilmiş olmasıdır. Öyle ki; en büyük sosyal medya ağlarını elinde bulunduran ve tüm dünyadaki kullanıcılara ait kişisel verileri işleyen bu şirketin veri gizliliğine ilişkin karar alma yetkisi ve verinin yönetimi ve korunması, yönetim kurulu ve/veya CEO'dan alınmış, bağımsız bir komiteye verilerek şirketin insiyatifinden çıkarılmıştır. Söz konusu komitenin yalnızca gizlilik ile ilgili konularda karar alması, komitenin bağımsızlığının sağlanması ve gizliliğe ilişkin raporların belirli periyotlarda

[243] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına İlişkin 108 Sayılı Sözleşme ve 181 Sayılı Ek Protokol
[244] Google Spain SL, Google Inc. v. Agencia Española deProtección de Datos, Mario Costeja González (C-131/12), 2014
[245] Aydın, s.114

FTC'ye sunulmasına ilişkin verilen bu karar, şeffaflığın sağlanması bakımından son derece önemlidir.

Özel bir şirket bakımından içtihatlarla böyle bir yapının sağlanması mümkün iken devlet tarafından işlenen kişisel veriler bakımından da benzer hassasiyette bir korumanın sağlanması da mümkün olmalıdır. E-devlet, mobil devlet gibi hizmetler kapsamında birçok kişisel veri, devletin veri bankalarına akmaktadır. Geçmiş yıllarda, farklı birimlere ait kayıt ve defterlerde kilit altında korunan arşivler, şu anda birbirine ağlarla bağlı dijital ortamlarda saklanmakta ve bu veriler tek bir yerde bir araya getirilerek yeni veriler üretilebilmektedir[246]. Bu durumun varlığı, siyasi iktidarın bu bilgiyi kendi lehine, baskıcı ve otoriter amaçlarla kullanması ihtimalini doğurduğu gibi yeterli siber güvenlik önlemleri alınmazsa bu verilerin 3. taraf saldırılara da açık olmasına da zemin hazırlamaktadır.

Nitekim devlet politikalarında da bilgi güvenliği alanında önemli çalışmaların yapılması gerekliliği ülkemizde de hassasiyetle vurgulanmaktadır. Cumhurbaşkanı'nın "Ülkemizin sahip olduğu verileri ve ürettiği bilgileri, tıpkı topraklarımız gibi, hassasiyetle korumazsak geleceğimize güvenle bakamayız. Geleceğin savaşlarının, konvansiyonel silahlarla değil siber silahlarla gerçekleştirileceğini unutmamalıyız"[247] sözleri konuya devlet açısından verilen önemi vurgulamaktadır.

Kamusal alanlarda ve kritik veri işleyen özel kuruluşlarda kişisel veriye erişim yetkisi olan personelin yaptığı işlemlerde bıraktığı dijital izlerin takip edilmesi, amaçla sınırlılık ilkesi dışında hareket edildiğinin tespitinde buna ilişkin önleyici tedbirler alınması ile birlikte idari ve cezai işlemlerin başlatılması, özellikle belirli erişim yetkileri olan personelin bu konuda zorunlu sertifikasyon ve eğitimlere tabi

[246]Tataroğlu, Muhittin, E-devlet'te Kullanılan Gözetim ve Kayıt Teknolojilerinin Mahremiyet üzerinde etkileri, 2009, Abant İzzet Baysal Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi – Journal of Social Sciences, Cilt / Volume: 2009-1 Sayı / Issue: 18, s.97 https://dergipark.org.tr/en/download/article-file/154664, Erişim Tarihi : 10.10.2019

[247]https://cbddo.gov.tr/haberler/4259/cumhurbaskani-erdogan-hgm-atlas-ve-hgm-kure-uygulamalarinin-tanitilmasi-toreni-nde-dijital-gelisimi-vurguladi, Erişim Tarihi : 10.12.2019

tutulması personelin hatalı veya kasti olarak hukuka aykırı hareket etmesini önleyici nitelikte tedbirlere örnek olarak verilebilir.

Ayrıca kişisel verinin depolandığı sunucu hizmetlerine ilişkin büyük verinin veri madenciliği vb. yöntemlerle işlenmesi konusunda ilave sorumluluklar ve denetim yükümlülüklerin yerine getirilmesi, bu işlemlerin izinlere tabi tutularak yapılması, Facebook örneğinde olduğu gibi veri işleme faaliyetinin riskli olduğu ve verinin amacı dışında kullanılabileceği alanlarda faaliyet gösteren firmalar özelinde farklı sorumluluk ve yükümlülükler getirilmesi, bağımsız iç denetim mekanizmalarının oluşturulması, toplumsal farkındalığın arttırılması için çalışmalar yapılması da son derece önemlidir.

İşletmelerin kişisel veriler bakımından kanun ve mevzuatın gerekliliklerini yerine getirmek için teknik alt yapı sağlamak, denetim yapmak, iş gücü istihdam etmek için büyük bütçeler harcamak zorunda kaldığı ve çoğu zaman bu bütçeleri harcamaktan kaçınmayı tercih edebildiği durumlar olmaktadır. Bu noktada devlet tarafından şirketlerin uyumluluklarını sağlamak adına çeşitli teşviklerin yapılması veya vergisel açıdan indirimler sağlanması da motive edici olabilecektir.

Kişisel veri, doğası gereği paylaşıldığı andan itibaren veri sahibinin kontrolü dışında sonsuz kere paylaşılabilir[248]. Bu noktada Kurul'un kendi internet sitesinde Kasım 2019 tarihinde Kişisel Verilerin Korunması Kanunu Uyum Sürecine İlişkin Duyuru başlığı altında yer alan bilgilendirme çerçevesinde[249], sektörün ihtiyaçları ve verinin kullanıldığı alanlara göre ayrımlar yapılması, özellikle yurt dışında da şubeleri olan ve dünya genelinde farklı ülkelerde faaliyet gösteren firmalarla veri alışverişine giren bu kuruşların uyumluluk konusunda yaşadıkları sıkıntılara çözüm getirecek sertifikasyonların yapılması sektörel uyumluluk bakımından önemli katkı sağlayacaktır.

[248]TEPAV, s.23

[249]https://kvkk.gov.tr/Icerik/6554/Kisisel-Verilerin-Korunmasi-Kanunu-Uyum-Surecine-Iliskin-Duyuru, Erişim Tarihi : 10.12.2019

4.2. COVID - 19 KAPSAMINDA TEMAS TAKİP UYGULAMALARI

2019 yılının sonlarına doğru ortaya çıkan ve Dünya Sağlık Örgütü tarafından pandemi ilan edilen COVID - 19 bulaşıcı solunum yolu enfeksiyonu hastalığı, salgının yayılımını önlemek ve kontrol altına almak amacıyla birçok ülke ve bölgede karantina ve kısmi sokağa çıkma yasakları uygulanmasına neden olmuştur.

Dünya Sağlık Örgütü, "contact trace" "temas takibi" kavramını, ilgili bakım ve tedaviyi almasına yardımcı olunması amacıyla bulaşıcı hastalığa yakalanmış bir kişiyle temas etmiş olabilecek kişilerin belirlenmesi ve izlenmesi olarak tanımlamaktadır. Sınırlı sayıda vakalarda temas takibi manuel şekilde yapılabilirken binlerce veya daha fazla teşhis edilmiş hasta olduğunda aynı şekilde manuel takip yapılması mümkün olmayacaktır. Diğer yanda COVID - 19 teşhis edilen birisi ile yakın temasta bulunan herkesin kendisini iki hafta boyunca karantinaya almasının gerekli olduğu düşünüldüğünde hareket halinde olan insanlar tarafından hastalığın yayılmasını önlemek, hastalık bulaşma riskini tespit etmek ve bulaşma riskinden korunmak adına dünyanın bir çok ülkesinde temas takip mobil uygulamalarının geliştirilmesine ihtiyaç duyulmuştur. Bu uygulamalar aynı zamanda virüs riskini belirlemek, virüs yayılım haritası çıkararak, tedavi ve karantina uygulanması, karantinaya alınanların kontrolü, sokağa çıkma yasağının uygulanması, kalabalık yerlerin tespiti gibi fonksiyonlara da sahip olabilmektedir.

Bu sürece uygun olarak geliştirilen temas takip uygulamaları, en basit şekilde mobil telefonlar aracılığı ile bluetooth, kablosuz ağ veya GPS verileri ile kişiler arasındaki yakınlığı kaydederek kullanıcılara enfekte teşhisi konmuş biriyle temas halinde olduklarını ve kendilerini izole etmeleri gerektiğini etkili bir şekilde bildirmeleri amacıyla tasarlanmış uygulamalardır.

Top10 VPN isimli internet sitesinin yaptığı haberde; Nisan 2020 tarihi itibariyle 23 ülkede temas takip mobil uygulaması kullanıldığı, bazı ülkelerde birden fazla mobil uygulamanın kullanılması sebebiyle dünya genelinde 43 tane temas izleme

mobil uygulamasının bulunduğu, mevcut mobil uygulamalarının %28'inin gizlilik politikası bulunmadığı bilgisi yer almaktadır[250].

Temas takip uygulamalarının kısa zamanda bir çok ülkede uygulamaya konulması, kişisel verilerin korunması ve mahremiyet sorunlarını da gündeme getirmektedir. Avrupa Komisyonu, kamu sağlığı otoritelerinin COVID - 19 teşhis edilmiş hasta ile temas halinde olan kişileri tanımlayarak, kişilere süreçle ilgili destek ve tavsiye vermek suretiyle bu kişilerin kendilerini karantinaya almalarını sağlamak amacıyla tüm Avrupa Birliği üye ülkelerde kullanılacak temas takip mobil uygulama geliştirilmesini teklif etmiş ve mobil uygulamanın gizlilik kurallarına uygun şekilde geliştirilmesi için AVKK'dan rehber bir görüş yayımlanması talebinde bulunmuştur[251].

Buna karşılık bir çok ülkede temas takip sistemi ile, gizlilik ve mahremiyet kuralları dikkate alınmaksızın veri işleme faaliyetinin yerine getirildiği anlaşılmaktadır. Örneğin İsrail hükümeti, enfeksiyondan şüphelenilen kişilerin mobil telefon verilerinin izlenmesine izin veren yasa çıkarılmış,[252] Güney Kore hükümeti ise enfekte olduğu bilinen hastaların yaş, cinsiyet, meslek ve seyahat rota bilgilerini işlediği bir veri tabanı oluşturmuştur[253]. Ayrıca devlet tarafından vatandaşların mobil telefonlarına "60 yaşlarında bir kadın COVID - 19 testi pozitif çıktı. Bu kişinin hastahaneye gelmeden önce ziyaret ettiği yerleri öğrenmek için tıklayın" şeklinde SMS gönderdiği dünya basınında da yer almıştır[254]. Bu şekilde gönderilen mesajlar, vatandaşların kimliğini deşifre edebileceği gibi konum verisi ile kişinin cinsel hayatından, din bilgisine kadar çeşitli özel nitelikli kişisel verisinin de ifşa edilmesine neden olabilecektir. Tayvan'da, sağlık kurumlarına hastaların seyahat

[250] https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/ Erişim Tarihi: 24.04.2020

[251] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf Erişim Tarihi: 24.04.2020

[252] https://www.bbc.com/news/technology-51930681 Erişim Tarihi: 24.04.2020

[253] https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking_apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html Erişim Tarihi: 24.04.2020

[254] https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives Erişim Tarihi: 24.04.2020

geçmişlerine erişim izni verilmiştir. Yetkililer karantina altındaki kişilerin telefon konum verilerini izleyerek kişinin evden çıkması veya telefonun kapalı olması durumunda güvenlik ve polis birimlerini alarma geçirerek 15 dakika içinde kişiye erişim sağlamaktadırlar[255]. İran hükümeti tüm vatandaşlarına, hastaneye veye sağlık merkezine gitmeden önce "AC19" adlı uygulamayı indirmeleri gerektiği duyurmuştur. Bu uygulama ile ad, soyad, adres, doğum tarihi ve gerçek zamanlı konum bilgisi toplanmaktadır. Uygulamanın kişilere evet-hayır testi ile hastalık teşhisi yaptığı iddia edildiğinde uygulama, Google tarafından uygulama mağazasından çıkarılmıştır[256].

Avrupa Birliği'ne üye ülkelerden Polonya'da teşhis konulmuş kullanıcıların iki tane tercih hakkı bulunmaktadır. Kullanıcılar ya kolluk kuvvetleri tarafından beklenmeyen ziyaretleri kabul edecek ya da devlet tarafından geliştirilen "Home Quarantine" adlı mobil uygulamayı indirerek belirli aralıklarla konum tabanlı selfie göndereceklerdir. Kullanıcılar belirlenen süreyi 20 dakika geciktikleri takdirde güvenlik güçleri devreye girmektedir. Bu uygulamada sadece konum verisi değil aynı zamanda görüntü verisi de işlendiği dikkate alındığında veri minimizasyonuna aykırı bir veri işleme faaliyetinden söz edilebilecektir.

Singapur, iki uygulama kullanıcısının yakınlık bilgisini bluetooth üzerinden takip eden bir mobil uygulama geliştirmiştir. Bu şekilde bir kişi kendisinin enfekte olduğunu bildirdiğinde, Sağlık Bakanlığı, kullanıcının açık rızasına istinaden son 21 günlük mobil uygulama datasına erişerek, uygulamayı kullanan ve COVID - 19 teşhisi konmuş kişi ile yakın temasta olan kullanıcılar ile iletişime geçecektir.

Avusturya'da geliştirilen uygulama, telefonlar arasındaki temas takip verisini "digital handshake" aracılığı anonim loglar ile saklamaktadır. Enfekte olan kişi, bu bilgiyi, uygulamaya işlediğinde, uygulama, bu telefonla temas eden şifreli anonim

[255] Hyunghoon Cho, Daphne Ippolito, Yun William Yu, Contact Tracing Mobile Apps for COVID-19:Privacy Considerations and Related Trade-offs, 2020, https://arxiv.org/pdf/2003.11511.pdf Erişim Tarihi: 24.04.2020

[256] http://static-ssl.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3/#iran-asked-citizens-to-download-an-invasive-app-3, Erişim Tarihi: 24.04.2020

temas verilerini tarayarak merkez bir sunucuya iletmekte, şifreli mesaj, bu telefona temas eden diğer kullanıcıların telefonlarına gönderilmektedir. Şifreli mesajlar ancak "digital handshake" ile saklanan şifreler eşleştiğinde açılabilmektedir. Böylece uygulamada işlenen tek kişisel veri, COVID – 19 teşhis edilmiş kişinin telefon iletişim bilgisi olmaktadır. Bu veri, olası bir suistimali önlemek adına maksimum 30 gün boyunca saklanmaktadır.

Almanya ve İngiltere gibi bazı ülkelerde bu tarz mobil uygulama geliştirilmesinden önce yapılacak geliştirmenin güvenlik, gizlilik, hukuk, etik ve halk sağlığı uzmanları tarafından dikkatle incelenmesi gerektiğinden bu ülkelerde temas takip uygulamaları hala geliştirilme aşamasındadır.

Ülkemizde Sağlık Bakanlığı tarafından çıkarılan karantina altına alınan kişiler tarafından kullanılması zorunlu tutulan "Hayat Eve Sığar" mobil uygulamasının App Store uygulama mağazasında yer alan aydınlatma metninde; uygulamanın COVID - 19 riskini belirleme amacıyla, COVID - 19 test sonucu pozitif çıkan kişilerin ve risk yoğunluğunun harita üzerinden gösterilmesi, izolasyon altında bulunulan lokasyonun belirlenmesi, bu lokasyonun terk edilmesi durumunda veri sahibine bildirim gönderilmesi ve ilgili makamlara bilgi verilmesi gibi fonksiyonlara sahip olduğu bilgisi yer almaktadır. Uygulama içerisinde ayrıca kullanıcılara yöneltilen bir takım sorulara verilen yanıtlara göre kullanıcının en yakın sağlık tesisini ziyaret etmesinin istenebileceği veya periyodik aralıklarla hastalık belirtileri hakkında sorular yöneltileceği de belirtilmiştir.

4.2.1 Veri Koruma Etki Analizi Yapılması ve Veri Koruma İlkelerine Uygun Veri İşleme Yapısının Tasarlanması

Temas takip mobil uygulaması, geliştirilmeden önce veri koruma etki analizi yapılarak veri işleme amaçlarının belirlenmesi ve amaçla sınırlılık ve ölçülülük ilkesi, veri minimizasyonu ve hesap verilebilirlik ilkeleri kapsamında kişisel veri işleyecek bir yapının kurulması önemlidir. AVKK, bu uygulamaların hesap verilebilirlik ilkesi doğrultusunda tasarımla ve varsayılan ayarlarla veri koruma

mekanizmaları dahil olacak şekilde geliştirilmesi, veri koruma etki analizlerinin belgelendirilmesi, kaynak kodun bilim topluluğu tarafından mümkün olan en geniş inceleme için uygun hale getirilerek geliştirilmesi gerektiğinden bahsetmektedir[257].

Bu uygulamalarda 3 farklı protokol söz konusu olmaktadır[258]. 1. tarz protokolde her uygulama sadece kendi konumunu kaydeder. Kullanıcı enfekte olduğunda konum ve zaman bilgisi otoriteye gönderilir. Otorite, enfekte olmuş her kullanıcının konum ve zaman verisini maskelenmiş şekilde paylaşarak diğer kullanıcıların enfekte olmuş bireylerle yakın temasa geçip geçmediklerini kontrol eder. Bu tarz protokol kullanımı konum verisinin kişisel veri olması sebebiyle veri minimizasyonuna aykırı olacaktır. 2. tarz protokolde, her uygulama, otorite tarafından belirlenen özel belirleyicileri[259] bluetooth aracılığı ile yayar ve iki telefon yanyana geldiğinde telefonlar bu özel belirleyicileri takas ederler. Kullanıcı enfekte olduğunu bildirdiğinde etkileşime geçtiği tüm özel belirleyiciler otoriteye gönderilir. Otorite enfekte olan kullanıcı ile etkileşime geçen tüm kullanıcılarla iletişime geçer. Bu protokolde kullanıcıyı işaret eden konum verisi işlenmese de özel belirleyicilerin telefona adreslenmesinden dolayı burada da kişisel verilerin işlenmesi söz konusu olacaktır. En güvenli yöntem olan 3. tarz protokol, 2. tarz protokol gibi çalışmakta ancak özel belirleyiciler her saat başı değiştirilmekte ve oluşturulan farklı özel belirleyiciler otoriteye gönderilmektedir. Burda özel belirleyiciler sürekli değiştiği ve direkt olarak kişiye adreslenemeyeceği için kullanıcının verileri farklı zaman aralıklarında izlenemeyecektir.

4.2.2. Gizlilik Politikalarının Şeffaflık İlkesi Kapsamında Açık ve Anlaşılır olması

Mobil uygulama gizlilik politikalarında geliştiricilerin güvenlik tedbirleri ve önlemlerini alması uygulamanın faaliyeti sırasında yönetişim ve hesap verilebilirlik

[257] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf Erişim Tarihi: 24.04.2020

[258] https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/ Erişim Tarihi: 24.04.2020

[259] Bknz. 15 nolu dipnot.

süreçlerin ve bu işlemenin gerekli ve etkili olduğunun belirlenmesi, takip faaliyetinin nasıl yürütüldüğü bu konuda hangi kontrol vasıtalarına sahip olunduğu ve gizliliği korumak adına ne gibi önlemler alındığı açıkça belirtilmelidir.

Singapur Sağlık Bakanlığı tarafından çıkarılan "Trace Together" uygulaması hakkında ayrıntılı bilgi verilen internet sitesinde uygulamanın hangi verileri, hangi yöntemle toplandığı ve ne kadar süre sakladığı, uygulamanın çalışma yöntemi, verilen rızanın nasıl geri alınabileceği, verilerin nasıl korunduğu vb. bilgiler açık bir şekilde yer alırken ayrıca uygulamanın çalışma yönteminin kullanıcıların daha kolay ve anlaşılır olmasını sağlamak adına animasyon video hazırlanmıştır[260]. Buna karşılık ülkemizde kullanılan Hayat Eve Sığar mobil uygulaması ile ilgili hazırlanan aydınlatma metni, en basit ifade ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ çerçevesinde aydınlatma metninde olması gereken başlıklara yer vererek veri sahibinin sahip olduğu haklar, kişisel verilerin toplama yöntemleri ve hukuki sebepleri ve başvuru yöntemine ilişkin mevzuat maddelerine atıf yapmaktadır. Aydınlatma metninde, mobil uygulamanın hangi veri işleme faaliyetinde hangi kanuni sebebe dayanarak veri işlediği tam olarak açık şekilde belirtilmemiştir. Metinde kişsiel verilerin kimlerle paylaşıldığı bilgisi yer almasına rağmen hangi kullanıcıların verilerinin kimlerle paylaşıldığının belirtilmemesi, kullanıcı açısından karışıklığa sebep olabilecektir. Örneğin uygulama içerisinde COVID - 19 teşhis edilmiş birinin konum verisi ve diğer verilerinin paylaşılması ile teşhis edilmemiş bir kullanıcının verilerinin paylaşılması arasında bir ayrım olup olmadığı bilinmemektedir.

4.2.3. Konum Verilerinin Anonim Şekilde Kullanılması Ve Veri Minimizasyonu Kapsamında Veri İşlenmesi

Bazı ülkeler kullanıcıların hareketlerini anonim veri kullanarak izlerken bazı ülkelerde bu konuda daha detaylı veri işlenmesi söz konusu olabilmektedir. Temas

[260] https://tracetogether.zendesk.com/hc/en-sg Erişim Tarihi: 24.04.2020

takip uygulamalarında kişinin hareketlerine ilişkin veri toplamak, veri minimizasyonu ilkesini ihlal edeceği gibi bu durum büyük ölçekte güvenlik ve mahremiyet risklerini de beraberinde getirecektir. Konum verisinin bireyi belirlenebilir kılması riskini indirebilmek amacıyla uygulamada maskeli veya anonim konum verisi kullanılması daha doğru olacaktır. AVKK, temas takip uygulamalarının bireylerin konum verilerine ihtiyaç duymadığını belirterek bu kapsamda uygulamanın amacının vakaları tespit etmek, test sonucu pozitif çıkan kişilere temas edenler olduğunu, kişilerin hareketlerini takip etmek ve talimatların uygulanmasını sağlamak olmadığını, belirtmiştir.

Kurul'un internet sitesinde 9 Nisan 2020 tarihinde yayımlanan kamuoyu duyurusunda, salgın hastalık durumunda toplum sağlığı ve kamu düzeni ile kamu güvenliğinin sağlanmasını teminen konum verisinin kişisel veri olarak kullanılmasının gerekli olduğu durumda 6698 Sayılı Kanun'un 28. maddesinin 1. fıkrasının ç bendinde[261] düzenlenen istisna maddesinin uygulama alanı bulacağı açıklanmış, her halükarda ilgili kurum ve kuruluşların kişisel verilerin güvenliğini sağlamaya yönelik her türlü teknik ve idari tedbirlerin almaları ve verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde söz konusu kişisel verilerin silinmesi veya yok edilmesi gerektiği yer almıştır[262].

Ülkemizde kullanınan mobil uygulamada işlenen veri kategorilerinin, kimlik verileri, iletişim verileri, konum verileri, meslek ve sağlık verileri olduğu düşünüldüğünde bu uygulamanın veri minimizasyonu ilkesine aykırı şekilde veri işlediği söylenebilecektir. Özellikle kişilerin ailelelerinin iletişim bilgilerini de uygulamaya eklemesine ilişkin bir yapı ile üçüncü taraf kişisel verilerin uygulama aracılığı ile paylaşılması amaçla sınırlılık ve ölçülülük ilkesine uygun olmayacaktır.

[261] Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde Kanun hükümlerinin uygulanmayacaktır.

[262] https://kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2- Erişim Tarihi: 24.04.2020

Singapur'da kullanılan "TraceTogether" uygulamasının gizlilik politikası incelendiğinde, uygulamanın GPS, kablosuz ağ izi, hücresel ID gibi fiziksel konum verisini toplamadığı, sadece bluetooth aracılığı ile yakınlık bilgisi topladığı bu şekilde kullanıcının konumunu izleyerek kullanıcının kimliğine ulaşmanın imkansız olduğu belirtilmiştir. Kullanıcıların enfekte olmuş bir hastaya yaklaştığının tespit edilmesi halinde durumun Sağlık Bakanlığı tarafından kendisine haber verilmesi amacıyla aranmak için sadece mobil telefon numarasının işlendiği, verilerin kullanıcıların cihazında saklandığı hususları dikkate alındığında kullanıcıya COVID - 19 teşhisi konulması halinde bu kişi ile yakın temas kurmuş kişilere ulaşmak amacıyla Bakanlık kişinin açık rızasına istinaden son 21 günlük mobil uygulama datasına erişmektedir[263].

Android ve IOS işletim sistemi üreticileri Google ve Apple şirketleri sağlık otoriteleri tarafından geliştirilen temas takip uygulamaları ile etkileşime geçecek ortak bir arayüz çalışmasını 2020 yılının Mayıs ayında tamamlayacaklarını açıklamıştır. İki işletim sistemi üreticisi, bu arayüz ile birlikte, temas takip uygulama kullanıcılarının Bluetooth Low Energy (BLE) transfer yöntemi ile veri paylaşımı yapılabilecekleri ve tüm sağlık otoritelerinin tek bir sistem üzerinde çalışacağı bir yapı tasarlamaktadırlar[264]. Bu şekilde enfekte kişiler ile bu kişilerle temas eden kullanıcılara ait verilere başka uygulamalar aracılığı ile tek bir sistem üzerinden erişilmesi gizlilik ve güvenlik riskini de beraberinde getirmektedir.

4.2.4. Uygulama Aracılığıyla Yanlış Vaka Tespit Edilmesi Riskinin En Aza İndirgenmesi.

Uygulamaların esas amacı, COVID-19 teşhis edilmiş bir kişiyle temas halinde olan kişileri tanımlamak ve bu kişilere tavsiye vermek olduğu için bu kişilerin tanımlanmasında basit veya doğrudan yöntemlerin kullanılmaması, uygulama içi bildirim yoluyla bilgilendirme kurgusu, uygulamanın sadece rastgele takma adlar ile veriyi işleyeceği bir yapı ile tasarlanmasını gerekli kılmaktadır. AVKK,

[263] https://tracetogether.zendesk.com/hc/en-sg Erişim Tarihi: 24.04.2020
[264] https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app Erişim Tarihi: 24.04.2020

uygulamalarda kullanıcılara yöneltilen sorulara karşılık verilen cevaplara göre risk değerlendirilmesi yapılmasının vaka sayısının yanlış bir şekilde artışına yol açmaması gerektiğini vurgulamıştır. Aksi takdirde bu durum karantina tedbirlerinin kaldırılmasını engelleyici bir duruma neden olabilecektir. AVKK, bu şekilde uygulamaya girilen bilgilerin doğru olduğundan emin olunan bir mekanizma oluşturulmasını örneğin, kişi tarafından tek kullanımlık bir kod ile giriş yapılması tavsiye etmektedir. AVKK, temas izleme uygulamalarında kullanılan algoritmaların, pozitif ve negatif sonuçların yanlış değerlendirilmesi ihtimalini sınırlamak için bu tespitlerin yetkin personelin sıkı gözetimi altında yapılması ve hiçbir şekilde "sonraki adımlarla ilgili tavsiyeler" şeklindeki yönlendirmenin otomatik karar alma mekanizması ile yapılmaması gerektiğini vurgulamaktadır.

4.2.5 Verinin Saklanması Ve Silinmesi

AVKK, mobil uygulamanın işlevi için ne kadar verinin toplanması ve işlenmesi gerektiğinin belirlenerek temas takip bilgisinin merkezi olmayan sistemlerde kişilerin cihazlarına kaydırılacak şekilde yapılmasını önermektedir. Diğer yanda kullanıcı cihazında saklama ile merkezi sunucuda saklama faaliyetinin yeterli güvenlik önlemlerinin mevcut olması koşuluyla geçerli alternatifler olabileceği ve uygulamanın nihai amacına bağlı olarak farklı kuruluşların veri sorumlusu olarak kabul edilebileceği görüşündedir. Her halükarda, AVKK verilerin kullanıcı cihazında saklanmasının veri minimizasyon ilkesi ile daha uyumlu olduğunu vurgulamaktadır. Singapur ve Avusturya mobil uygulamalarında verilerin kişilerin mobil cihazlarında saklandığı bir yapı kurulduğu, Singapur mobil uygulamasında, verilerin en fazla 21 gün saklanladığı, Avusturya mobil uygulamasında verilerin 30 gün sonra silindiği gizlilik politikalarında yer almaktadır. Ülkemizde uygulanan mobil uygulamanın aydınlatma metninde verinin ne kadar süre saklanacağı bilgisinin yer almaması şeffaflık ilkesine aykırı değerlendirilebilecektir.

4.2.6 Değerlendirme

Salgın hastalıklar, kamu sağlığını korumak adına, olağan sağlık önlemlerinin yeterli olmadığı ve ilave önlem alınmasının gerektiği hastalıklardır. Anayasa'nın 20.

maddesinde tanımlanan ve korunan herkesin kişisel verilerinin korunmasını isteme hakkı ile devletin COVID-19 bulaşıcı hastalığından korunmak ve kamu sağlığını ve kamu yararını korumak adına alması gereken tedbir ve önlemler karşısında denge kurulması hukuk devletinin gereğidir. Temas takip uygulamalarında telefon numarasının kaydedilmemesi, şifre ve takma adların kullanılması ve veri sahibinin açık rızasına dayanarak kişisel veri işleme faaliyetlerinin mevzuatın gerektirdiği korumayı ne ölçüde sağladığı konusunda da soru işaretleri uyandırmaktadır. Geliştirilen uygulamalarda yapılan veri işleme yöntemlerinin gerçek kişi ile bağdaştırılabilecek herhangi bir riski öngörüp bunu bertaraf edecek teknik alt yapıyı oluşturması beklenir. Mobil uygulamaların uygulama yöntemi, kişisel verilerin işleme amaçları, hukuki sebepleri, ne kadar süre ile saklanacağı gibi bilgilerin varlığının yeterince açık ve anlaşılır bir şekilde kullanıcıya sağlanmaması ve buna gerekçe olarak salgın hastalığın kontrol edilmesi amacıyla kamu sağlığının korunmasının gösterilmesi Anayasa 13. madde ile düzenlenen ölçülülük ilkesine aykırı olabilecektir.

Özellikle Avusturya mobil uygulamasında uygulamanın neredeyse hiçbir kişisel veri işlemeye ihtiyaç duymadan fonksiyon göstermesi, kullanıcıların kişisel verilerinin kendi kontrolüne bırakılması, teknolojik şifreleme ve maskemele yöntemleri ile cihazlar arasında oluşturulan anonim verilerle kontrollerin sağlanması salgın kontrolünün yapılması ile kamu sağlığını koruyucu tedbirleri alırken aynı zamanda bireylerin mahremiyetlerini ve kişisel verilerin hukuka uygun şekilde korunmasını da sağlamaktadır.

Bir çok ülkede olduğu gibi ülkemizde de salgını kontrol altına almak, enfekte olan kişilere temas edenleri tespit ederek uyarmak, riskli alanları belirlemek gibi amaçlarla teknolojinin sunduğu imkanlarla önlemler alınmaktadır. Ancak bu önlemler alınırken hastanın takibinden ziyade hastalığın takibinin yapılması, dolayısıyla kişinin sağlık verisi başta olmak üzere konum verileri yerine anonim veri kullanılacak veya uygulamanın fonksiyonu için mümkün olacak en az kişisel veri işlenmesi için gereken teknik ve idari alt yapının tercih edilmesi kamuya duyulan güveni de arttıracaktır.

Kişisel verileri başta 6698 Sayılı Kanun'un 4. maddesinde düzenlenen ilkelerden veri minimizasyonu, işlendiği amaçla bağlılık ve ölçülülük ilkeleri olmak üzere mevzuata uygun şekilde en son çare açık rıza hukuki sebebine dayanarak işlenmesi, bu işleme faaliyetinin hukuka uygun gerçekleştirilmesi için her türlü önlemin alındığından emin olunması halinde hukuk devletinden söz edilebilecektir.

SONUÇ

Mobil uygulamalar, seyahatten, ulaşıma, bankacılıktan, eğitime, alışverişten, spor alışkanlıklarına kadar hayatın her alanında sınırsız seçenekleri ile hayatımızı kolaylaştıran teknolojilerdir.

COVID – 19 pandemisi ile tüm dünya genelinde kamu sağlığını korumak adına mobil uygulamalar geliştirilmesi, mobil uygulamaların önemini bir kez daha ortaya çıkarmıştır. Öte yandan kişisel verilerin mobil büyük veri alanına dahil olması, mobil pazarlama alanında kullanılması ve mobil verinin direkt sahibini adreslemesi karşısında verinin izlenme riski ile Cambridge Analytica örneğinde olduğu gibi kişisel verilerin bireylerin seçim ve tercihlerini manipüle etmeye yönelik gizli amaçlarla işlenme riskleri dikkate alındığında bu alanda gizlilik ve mahremiyete ilişkin hukuki korumanın öneminin arttığı da söylenebilir.

Gerek AB gerekse ülkemizde yürürlükte bulunan kişisel verilerin korunması mevzuatına uyumlu bir mobil uygulamadan söz edebilmek için bu sektörde yer alan aktörlerin yükümlülüklerini ayrı ayrı yerine getirmesi gerekmektedir. Mobil uygulamanın geliştirilmesi aşamasından son kullanıcıya sunulduğu süre içerisinde bile birden fazla aktörün dahili olduğu düşünüldüğünde veri sorumlusu ve veri işleyen sıfatlarının her bir mobil uygulama özelinde ayrı bir şekilde değerlendirilerek, hukuka uygun veri işleme yapısının kurgulanması ile verinin paylaşım, erişim sınırları ve kurallarının kullanıcıyı da aydınlatacak şekilde net bir şekilde belirlenmesi esastır.

İşletim sistemi ve cihaz üreticilerinin, hangi durumda ve ne ölçüde kişisel veriye erişime izin verileceğini belirlediği, uygulama geliştiricinin sadece uygulamanın çalışması için gereken en az bilgiye erişimini veya mümkünse anonim veri ile sağlayacak şekilde bir yöntem belirlediği durumda ancak hukuka uygun bir işleme faaliyetinden söz edilebilecektir[265]. Uygulama geliştiricinin mobil uygulamanın

[265] Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü, s.11

kullanım amacı gereği cihazda yer alan sensörlere erişim izni istemesi, bu izni isterken kullanıcıları bilgilendirmesi, kullanıcıların erişim iznini yönetebilecekleri bir mekanizma kurması, kullanım amacını aşacak şekilde erişim talep etmemesi gerekir. COVID - 19 salgın sürecinde salgını kontrol altına almak amacıyla geliştirilen bazı temas takip uygulamalarında açık rıza hukuki sebebine dayanarak konum verisi ile sağlık verisi işlenirken Singapur ve Avusturya ülkelerinde geliştirilen mobil uygulama örneklerinde aynı amaç doğrultusunda anonim veri ile fonksiyon gösterebilecek teknik bir yapı kurgulanmıştır. Bu iki örnek aynı amaç için dahi olsa kamu sağlığının korunması karşısında kişisel verilerin amaçla sınırlılık ve ölçülülük ilkesi ile veri minimizasyonu ilkelerine uygun şekilde de işlenebileceğini farklı ülkeler tarafından geliştirilen mobil uygulamalar özelinde göstermiştir.

Mobil uygulama dünyasında kullanıcıların da veri güvenliğini sağlamak konusunda kendilerine düşen sorumlulukları yerine getirmeleri beklenmektedir. Kullanıcı zafiyetinin önüne geçmek için toplumsal farkındalığı arttıcı faaliyetlerin yapılması ve kişilerin gizlilik konusunda bilgilendirilmeleri önemlidir. Kullanıcılar, cihazlarında ve mobil uygulamalarda yer alan gizlilik ile ilgili politikaları inceleyerek, gizlilik tercihlerini ve ayarların gereğini yapmalı, indirdikleri uygulamaların ayarlarını kontrol etmelidir. Çocuklara hizmet sunan mobil uygulamalar ise çocuklara özel hukuki düzenlemeler ve uygulama mağazalarının çocuklara yönelik uygulamalara ilişkin kural ve kriterleri doğrultusunda bir yapı tasarlanmalı, bu uygulamalrda üçüncü taraf reklam ve hizmet sağlayıcılara daha sınırlı ve kısıtlı bir yapı kurgulamalıdır.

Gerek cihaz ve işletim sistemi üreticisi gerekse uygulama geliştirici tarafından mobil uygulamalarda bilgi ve veri güvenliğinin sağlanması buna ilişkin teknik ve idari tedbirlerin alınması, mevcut veya muhtemel veri koruma riskleri ile ilgili denetimler yapması şarttır. Aynı şekilde mobil hizmeti sunan tüm kamu, özel kurum ve kuruluşların verilerinin saklandığı alanlarda doğrulanabilir güvenlik sertifikaları ve ödeme sistemlerini güncel şekilde koruyucu tedbirleri alıp almadığının kullanıcılar tarafından sorgulanması güvenliği arttıracaktır.

Yazının icadından beri görülmüştür ki; her yeni fikir, buluş ve akım insanoğluna hizmet ve kolaylık sağladığı gibi farklı amaçlarla kullanılarak olumsuz sonuçlar da doğurmuştur. Bu noktada yeniliğe karşı çıkarak, gelişmeleri kabul etmemek veya kullanmayı reddetmek çözüm olmayacağı gibi içinde bulunduğumuz yüzyılda neredeyse imkansızdır. Ortaya çıkan her yeni olay, içinde yaşadığımız çağda kişisel veriyi elinde bulundurmanın ne kadar önemli olduğunu tekrar tekrar gözler önüne sermektedir. Gerek siyasi iktidarlar gerekse sermaye şirketleri kişisel veriyi elde etmek için teknolojinin her türlü imkanını kullanmaktan çekinmemekte bazı durumlarda fahiş para cezaları bile caydırıcı olmamaktadır.

Bu gelişmeler ile ortaya çıkabilecek olumsuz durumları hukukun yardımı ile en az seviyeye indirmek; kamu kurumları ve ticari işletmeler karşısında bireylerin haklarını koruyacak bir yapıyı sağlayacak güç ve nitelikte düzenlemeler yapmak ancak bu düzenlemelerin teknolojik gelişmelerin önünü tıkayacak veya ticari işletmeleri iş yapamayacak şekilde katı şekilde de uygulanmayacağı bir yapı kurmak ana hedef olmalıdır. Ancak doğası gereği hukuki düzenlemeler mevcutta olan, yaşayan durumları düzenlemekte, teknolojinin hızına ayak uyduramamaktadır. Google'un Unutulma Kararı ile Cambridge Analytica olayı, düzenleyici işlemler ve kuralların ancak korunmaya muhtaç bir durum ortaya çıktıktan sonra gündeme geldiğini göstermektedir. Dolayısıyla teknolojik hızla paralel bir hukuki koruma sağlamak için ortaya çıkarılacak çözümlerin akademik olarak geliştirilmesine ihtiyaç vardır.

KAYNAKÇA

Akgül : Aydın Akgül, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul, 2016

Akıncı : Ayşe Nur Akıncı , Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Çalışma Raporu 6, 2017

Arthur : Charles, Arthur, Dijital Savaşlar Apple, Google, Microsoft ve İnternet Savaşı, İstanbul, 2017

Artuç : Murat Artuç, Mahremiyet Açısından Birey Devlet İlişkisi, Yüksek Lisans Tezi, Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Ana Bilim Dalı, Aydın, 2015

Aşıkoğlu : Şehriban İpek Aşıkoğlu, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul, 2018

Aydın : Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul, 2015

Ayözger : A. Çiğdem Ayözger Öngün, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, 2019

Ayözger : A. Çiğdem Ayözger, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, 2016

Baysal : Mustafa Baysal, KVKK Kişisel Verilerin Korunması Kanunu El Kitabı, Ankara, 2020

Berber,Bilgili : Leyla Keser Berber, Ali Cem Bilgili, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, İstanbul, 2020

Brug : Anıl Altaş Brug, e-ticaret Satışta Tsunami Etkisi, İstanbul, 2019

Castells : Castells Manuel, İletişim Gücü, İstanbul, 2016

Cho, Ippolito, Yu : Hyunghoon Cho, Daphne Ippolito, Yun William Yu, Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs, 2020, https://arxiv.org/pdf/2003.11511.pdf

Çekin : Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul, 2018

Determann : Lothar Determann, Kişisel Verilerin Korunması Uygulama Kılavuzu, İstanbul, 2020

Dülger : Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, İstanbul, 2019

EC : European Commission, Proposal Regulation of The European Parliament and Of The Council Concerning the Respect For Private Life and the Protection of Personal Data In Electronic Communications and Repealing Directive 2002/58 EC, Brussels, 2017

EDPS : EDPS Guidelines On The Protection Of Personal Data Processed By Mobile Applications Provided By European Union Institutions, 2016

EDPS : Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)

ENISA : Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR

Henkoğlu : Türkay Henkoğlu, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara, 2015

ICO : Big Data, artificial intelligence, machine learning and data protection, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

ICO : Privacy in mobile apps Guidance for App Developers, https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

Işık : Sezen Kama Işık, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, 2020

Kaya : Mehmet Bedii Kaya, Elektronik Ticaret Hukuku Ticari Elektronik İletiler, İstanbul, 2020

Karabey : Işık Karabey, Wi-Fi Tabanlı Parmak İzi Yöntemi Kullanarak İç Ortam Konumlandırma, Atatürk Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 2015

Keser : Leyla Keser, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları özelinde Kişisel Verilerin Korunması, 2014

Kopmaz, Arslanoğlu : Büşra Kopmaz, Ali Arslanoğlu, Mobil Sağlık ve Akıllı Sağlık Uygulamaları, Sağlık Akademisyenleri Dergisi, 2018 https://dergipark.org.tr/en/download/articlefile/63366

Kröger : Jacob Kröger, Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things, IFIP International Internet of Things Conference, 2018 https://link.springer.com/chapter/10.1007/978-3-030-15651-0_13

Kumar : Pradeep Kumar, Analyzing Data Leakage Using Third Party Connections in Mobile Appliacations, Thapar University Master of Engineering in Information Security, Patiala, 2015

Kurtagıc : Haris Kurtagic, Tüketicilerin Mobil Pazarlama Uygulamalarını Kabullenmelerinde Etkili Olan Faktörler: Balkan Ülkelerindeki Üniversite Öğrencileri Üzerine bir araştırma, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İşletmecilik Anabilim Dalı Yüksek Lisans Tezi, İstanbul 2019

Madde 29 Çalışma Grubu : Madde 29 Çalışma Grubu'nun 27 Şubat 2013 tarih ve 02/2013 sayılı "Akıllı Cihaz Uygulamaları" hakkındaki görüşü

Madde 29 Çalışma Grubu : Madde 29 Çalışma Grubu 'nun 04 Nisan 2017 tarih ve 01/2017 sayılı "Elektronik Haberleşme Tüzük Taslağı" hakkındaki görüşü

Madde 29 Çalışma Grubu : Madde 29 Çalışma Grubu 'nun 22 Haziran 2010 tarih ve 02/2010 sayılı "Çevrimiçi Davranışsal Reklamcılık" hakkındaki görüşü,

Madde 29 Çalışma Grubu : Madde 29 Çalışma Grubu'nun 16 Mayıs 2011 tarih ve 13/2011 sayılı "Akıllı mobil cihazlarda coğrafi konum hizmetleri" hakkındaki görüşü

Mangset : Peder Lind Mangset, Analysis of Mobile Application's Compliance with the General Data Protection Regulation (GDPR), 2018

Mangset : Privacy in the Smartphone Age A study on the privacy and data protection risks and violations of mobile applications, http://arno.uvt.nl/show.cgi?fid=142089

Özdemir : Hayrünnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, 2009

Özdemir : Hayrünnisa Özdemir, Erzincan Binali Yıldırım Üniversitesi, Hukuk Fakültesi Dergisi, Haberleşmenin Gizliliği ve Kişisel Veriler, 2009

Pedro : Pedro, Filipa Carmo, Privacy in the Smartphone Age A study on the privacy and data protection risks and violations of mobile applications, Master thesis in Law and Technology, http://arno.uvt.nl/show.cgi?fid=142089

Sert : Aybike Sert, Cep Telefonu Kullanıcılarının Mobil Reklamlara Karşı Tutumlarını Etkileyen Faktörler Üzerine Bir Araştırma, İstanbul Arel Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı/İşletme Yönetimi Programı,Yüksek Lisans Tezi, İstanbul,2012

Şahin : Osman Şahin, BTK, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Bilişim Uzmanlığı Tezi, Haziran 2011, Ankara

Tataroğlu : Muhittin Tataroğlu, Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED), Yönetim ve Ekonomi Dergisi, 2013

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı : T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı, 2016, http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf

Taştan, : Furkan Güven Taştan, Türk Sözleşme Hukuku'nda Kişisel Verilerin Korunması, İstanbul, 2017

Tataroğlu : Tataroğlu, Muhittin, E-devlet'te Kullanılan Gözetim ve Kayıt Teknolojilerinin Mahremiyet üzerinde etkileri, 2009, Abant İzzet Baysal Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi – Journal of Social Sciences, Cilt / Volume: 2009-1 Sayı / Issue: 18, https://dergipark.org.tr/en/download/article-file/154664

TBMM : TBMM Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyon Raporu, Haziran 2012, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf ,

TEPAV : TEPAV Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, İstanbul Bilgi Üniversitesi, 21.05.2014

Turan : Metin Turan, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Ankara, 2020

Türkmen : Sevgi Eraslan Türkmen, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, İstanbul, 2019

URL-1 : https://www.cnnturk.com/fotogaleri/ekonomi/sirketler/whatsapp-turkiyenin-20-devini-gecti

URL-2 : https://www.kisiselverilerinkorunmasi.org

URL-3 : https://cbddo.gov.tr/

URL-4 : http://www.kbd.org.tr/s/2389/i/KBD_EH-KisiselVeriler-20170807-239-Karar.pdf

URL-5 : https://kvkk.gov.tr/

URL-6 : https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf

URL-7 : https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

URL-8 : https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

URL-9 : https://www.optimisthub.com/facebook-cambridge-analytica-skandali.html

URL-10 : http://davelevy.info/Downloads/cabridgeananalyticafiles%20theguardian_20180318.pdf

URL-11 : https://ieeexplore.ieee.org/abstract/document/843640

URL-12 : https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security

URL-13 : https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

URL-14 : http://www.enforcementtracker.com/

URL-15 : https://sensortower.com/blog/

URL-16 : https: //www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

URL-17 : https://pando.com/2014/02/24/whatsapp-bought-for-19-billion-what-do-its-employees-get/

URL-17 : https://www.statista.com/statistics/309448/global-smartphone-shipments-forecast-operating-system/

URL-18 : https://sensortower.com/blog/top-apps-worldwide-q1-2019-downloads/

URL-19 : https://webrazzi.com/2019/10/24/turkiye-mobil-uygulama-kullanici-sayisi-gemius/

URL-20 : https://play.google.com/intl/en-US/about/privacy-security-deception/malicious-behavior/

URL-21 : https://www.newscientist.com/article/2152366-phone-sensors-can-save-lives-by-revealing-what-floor-you-are-on/#ixzz6Cd03Cm00

URL-22 : https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare

URL-23 : https://www.apple.com/tr/privacy/features/

URL-24 : https://developer.apple.com/app-store/review/guidelines/#before-you-submit/

URL-25 : https://developer.apple.com/app-store/review/guidelines/#data-collection-and-storage/

URL-26 : https://www.termsfeed.com/blog/privacy-policy-analytics-sdk/

URL-27 : https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/

URL-28 : https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

URL-29 : https://www.bbc.com/news/technology-51930681

URL-30 : https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking_apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html

URL-31 : https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives

URL-32 : http://static-ssl.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3/#iran-asked-citizens-to-download-an-invasive-app-3

URL-33 : https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/

URL-34 : https://tracetogether.zendesk.com/hc/en-sg

URL-35 : https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app

Uyar : Ahmet Uyar, Tüketicilerin Mobil Uygulamalara İlişkin Algılarının Teknoloji Kabul Modeli İle Değerlendirilmesi, İşletme Araştırmaları Dergisi Journal Of Busıness Research-Turk 2019, 11(1), 687-705, s.1, webrazzi.com, https://www.isarder.org/2019/vol.11_issue.1_article53_full_text.pdf

Yamamoto : Gonca Telli Yamamoto, Mobil Yaşam ve Uygulamaları, İstanbul, 2011

Yenilmez : Gülhan Yenilmez, Algılanan Deneyimsel Değer Ve Akış Deneyiminin Mağaza Memnuniyeti Ve Satın Alma Niyeti Üzerindeki Etkileri: Çevrimiçi, Fiziksel Ve Mobil Mağaza Kanallarının Karşılaştırılması, Osmaniye Korkut Ata Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı, Yüksek Lisans Tezi, 2019

Yıldırır, S. C. & Burçin, K. : Yıldırır, S. C. & Burçin, K. (2019). Mobil uygulama kullanımının benimsenmesi: teknoloji kabul modeli ile bir çalışma. KAÜİİBFD, 10(19), 22-51