Kastamonu İletişim Araştırmaları Dergisi - Sayı 14 / Bahar 2025
Kastamonu Üniversitesi İletişim Fakültesi
Süreli Elektronik Dergi

E-ISSN: 2667-727X

Mobil Sağlık Uygulamaları Mahremiyetimizi Nasıl Tehdit Ediyor?

How Mobile Health Apps Threaten Our Privacy?

Murat Uluk, Dr. Öğr. Üyesi, İstanbul Beykent Üniversitesi İletişim Fakültesi,
E-posta: uluk.murat@gmail.com,
ORCID ID: 0000-0001-5923-8468
Araştırma Makalesi/Research Article

Anahtar Kelimeler:

sağlık verileri, mahremiyet, mobil uygulamalar, üçüncü taraf izleyiciler

Öz

Sağlık verileri, bireylerin zihinsel ve fiziksel durumlarına ilişkin son derece hassas verilerden oluşur. Hastalıklar, tahlil sonuçları ve sağlık raporları gibi verilerin yanı sıra tansiyon, nabız, uyku düzeni ve gündelik aktiviteler de sağlık verileri arasında yer almaktadır. Mobil uygulama mağazalarında bireylerin sağlık durumunu takip etme, kontrol etme ve yönetmeleri için birçok uygulama bulunmaktadır. Hassas veriler toplayan ve işleyen bu uygulamaların kullanıcı mahremiyetine ne denli saygı duyarak süreci yürüttükleri hakkında bilgi eksikliği söz konusudur. Çalışma, Türkiye'deki Google Play mağazasında en popüler 20 mobil sağlık uygulamasının hangi üçüncü taraf izleyiciler barındırdıklarını, kullanıcı cihazlarından hangi izinleri talep ettiklerini ve gizlilik sözleşmelerinde bunları nasıl ele aldıklarını incelemiştir. Araştırma, 22 Mart – 29 Mart 2024 tarihleri arasında gerçekleşmiştir. Elde edilen veriler, uygulamaların %75'inin yabancı şirketlere ait olduğunu ve tüm uygulamalarda toplam 153 izleyicinin olduğunu göstermektedir. Tüm uygulamalarda en az iki farklı üçüncü taraf izleyici yer alırken, Google ve Meta'ya ait izleyicilerin yoğunluğu dikkat çekmektedir. İzleyicilerin büyük çoğunluğu reklam ve analitik amaçlar için kullanılmaktadır. Yüklendikleri cihazlardan belirli özellik veya verilere erişmek için en çok 83, en az 9 izin istenmiştir. 19 uygulama en az bir özel/tehlikeli olarak etiketlenen izin istenmiştir. Uygulamaların hepsi Türkçe olmasına rağmen yarısının gizlilik sözleşmesi İngilizcedir. 3 uygulamanın sözleşmesi hiç yoktur, 7 uygulamanın sözleşmesi Türkçedir. Türkçe sözleşmelerde uygulamaların sahip olduğu izleyiciler ve talep ettikleri izinler nadiren yer almaktadır. İngilizce sözleşmelerin okunabilirlik seviyesi en az lise mezunu ve/veya üniversite öğrencisi seviyesindedir. Çalışma, sağlık alanındaki uygulamaları mahremiyet odaklı çözümleyerek alandaki eksikleri ortaya çıkarmaktadır. Bu alanda mahremiyetin sağlanmasının özel yaşama ve bireysel özgürlüklere katkı sağlaması beklenmektedir.

Keywords:

health data, privacy, mobile apps, third-party trackers

Abstract

Health data consists of highly sensitive data about individuals' mental and physical states. In addition to disease diagnoses, test results, and medical reports, health data include blood pressure, heart rate, sleep pattern, and daily activities. Many apps are available in mobile app stores for individuals to track, control, and manage their health. However, there is a lack of information about how these apps collect and process sensitive data and respect user privacy. Based on this, the study analyzed the 20 most popular mobile health apps on Google Play in Türkiye. The study examined which third-party trackers are included in the apps, what permissions they request from user devices, and how these are addressed in their privacy policies. The research was conducted between March 22 and March 29, 2024. The data demonstrate that foreign companies owned 75% of the apps, and all apps had 153 trackers. Each app had at least two different third-party trackers, with a high concentration of trackers belonging to Google and Meta. Most trackers were used for advertising and analytical purposes. The apps requested between a minimum of 9 and a maximum of 83 permissions to access specific features or data from the devices on which they were installed. 19 apps requested at least one permission labeled as special/dangerous. Although all the apps are available in Turkish, half have privacy policies only in English. Three apps had no policy, and seven apps had a Turkish policy. Turkish policies rarely mention the third-party trackers in the apps and the permissions they request. The readability of English policies is at least at the level of high school graduates and/or university students. This study analyses practices in the monitoring of one's own health with a focus on privacy and reveals shortcomings in the field. Ensuring privacy is expected to contribute to private life and individual freedom.

Başvuru Tarihi: 13.09.2024

Yayına Kabul Tarihi: 09.04.2025

Uluk, M. (2025). Mobil sağlık uygulamaları mahremiyetimizi nasıl tehdit ediyor?. *Kastamonu İletişim Araştırmaları Dergisi (KİAD),* (14), 160-190. DOI: 10.56676/kiad.1549707

Giriş

Teknolojinin hızla gelişmesiyle birlikte günümüzde kullanıcıların dijital izlerinin ve kişisel verilerinin toplanması daha önce hiç olmadığı kadar yaygın hâle gelmiştir. Bununla birlikte modern ekonomilerde bilgi üretiminin yeri ve önemi ile bilgi teknolojilerindeki ilerlemeler söz konusu verilerin toplanması, saklanması, analiz edilmesi ve yeni anlamlar üretilerek yeniden kullanılmasını kayda değer ölçüde artırmıştır (Acquisti vd., 2016). İlerlemeler doğrudan fiziksel dünyayı da kapsayarak büyük veriyi daha da büyütmeye olanak sağlamıştır. Çevrim içi ve çevrim dışı dünya arasındaki sınırlar özellikle mobil teknolojiler ve akıllı nesnelerin (sensörler) gündelik hayattaki yoğun kullanımı ile belirsizleşmeye başlamıştır. Bu süreç, kişisel verilerin toplanması ve kullanım alanları ile ilgili mahremiyet endişelerini de beraberinde getirmiştir.

Mahremiyet kavramı, tarih boyunca çeşitli şekillerde var olmuş olsa da çağın getirdiği yeniliklerle birlikte çok boyutlu ve karmaşık bir hâl almaya başlamıştır. Çünkü bugün mahremiyetin korunması yalnızca bireysel özgürlüğün ve bilgiye erişimin kontrolünün sağlanmasını değil, aynı zamanda demokratik toplumun teminatı için gereklidir. Dolgun (2015, s. 209), mahremiyeti insan haklarının temeli ve modern devletlerde bireysel özgürlüklerin güvencesi olarak tanımlar. Dolayısıyla günümüzde mahremiyet insan hakları, özgürlük, hukukun üstünlüğü ve demokrasi gibi değerlerle bir arada yer almaktadır.

Zuboff (2019, s. 52), dijital dünyada mahremiyetin "çevrim içi hizmetlere erişim karşılığında feda edilmesi için beklenen bir meta" olarak görüldüğünü söylemektedir. Diğer ifadeyle, gözetlenme, kişisel verilerin paylaşımı ve kontrolünün kaybolması ücretsiz dijital hizmetlerin karşılığını ödemenin bir yolu olarak kabul edilmektedir. Bu yaklaşım, çevrim içi dünyada tehlikeli bir normalleşmeyi de beraberinde getirmiştir. Özellikle bugün insanın en önemli teknolojik uzantısı olan akıllı cihazlar, kişisel asistanlar olduğu kadar farklı uygulamaların kişisel veri üretim, paylaşım ve dağıtım aracı olma görevini de üstlenmektedir.

Akıllı cihazlar ve mobil uygulamalar aracılığıyla gündelik hayatın her alanından toplanan veriler, kullanıcılar farkında olmadan çeşitli amaçlar doğrultusunda kullanılabilmektedir. Toplanan verilerin arasında hassas verilerin de olması ve bu hassas verilerin çeşitli işlemlerden geçirilerek kişi hakkında özel çıkarımlarda bulunması dijital çağda mahremiyete ilişkin endişeleri de beraberinde getirmektedir.

Sağlık ve Fitness kategorisi altındaki mobil uygulamalar, kullanıcıların sağlık durumlarını izleme ve yönetmelerine olanak tanımaktadır. Bununla birlikte söz konusu uygulamaların gerek yer aldıkları mobil cihaz gerekse entegre çalıştıkları akıllı cihazlar aracılığıyla işledikleri veriler çoğunlukla sağlık verisi olarak kabul edilebilmektedir. Sağlık uygulamalarının türüne göre değişmekle beraber ilgili uygulamaların birçoğu kalp atış hızı, vücut sıcaklığı, adım sayısı, uyku düzeni, egzersiz süresi, yakılan kalori, su tüketimi, ilaç takibi, beslenme alışkanlıkları, ruh sağlığı, doğurganlık bilgisi ve regl takibi gibi birçok hassas veriyi görüntülemekte ve saklamaktadır. Veriler, kullanıcıların sağlık durumlarını daha iyi anlamalarına ve iyileştirmelerine yardımcı olurken öte yandan verilerin depolanması, üçüncü taraflarla paylaşımı ve farklı amaçlar için kullanımı olasılıkları da endişe yaratmaktadır.

Çalışma, mobil sağlık uygulamalarını kullanıcı mahremiyetini merkeze alarak incelemek üzere tasarlanmıştır. Bu doğrultuda uygulamaların cihazdan hangi izinleri talep ettiği, hangi üçüncü taraf şirketlere iş birliği yaptığı ve gizlilik sözleşmelerinde bunlara nasıl yer verdiğini ortaya çıkartmayı amaçlamaktadır.

Temel Bir İnsan Hakkı Olarak Mahremiyet

Mahremiyetin geçmişi, insanlık tarihinin geçmişine kadar dayanmaktadır. Adem ve Havva'nın vücudunu yapraklarla örtmesi veya İncil'de, birinin özel alanına girilmesine utanç ve öfke duyulması gibi durumlar mahremiyetin eski zamanlara dayandığını göstermektedir (Adrienn, 2016, s. 257). Daha sonraları, Hammurabi Kanunları ve antik Roma hukukunda eve izinsiz girişlerle ilgili sıkı yaptırımlar yer almıştır. İngiliz örf ve âdet hukukunda gözetime karşı koruma sağlayan kanunlar, dönem insanlarının özel hayatlarının ihlal edilmesini engellemeye yönelik tedbirler içermiştir (Solove, 2011, s. 4).

Görece yakın tarihte, 19.yy sonlarına doğru, kamera, telefon ve fonograf gibi icatlar bir yanıyla çığır açarken diğer yanıyla mahremiyet endişelerini gündelik hayatta daha çok hissettirmeye başlamıştır (Lauer, 2012, s. 571 - 577). Neticesinde, 1890 yılında, Samuel Warren ve Louis Brandies (1890), "the Right to Privacy" adlı bir eser yayımlamışlardır. Halen başucu eseri olarak görülen makalenin yazılmasına konu olan olay ise icat edilen teknolojilerin mahremiyete olumsuz etkilerine dikkat çekmek olmuştur. Kodak kamerasının icadı ile dönemin ünlülerinin özel anları hızlıca ifşa edilmeye başlanmıştır. Yazarlar, yeni teknolojileri sınırsız kullanmanın bireyin kendisine ait bilgiyi kontrol etme hakkını zedelediği gerekçesiyle endişelerini bu eserle dile getirmiştir. Eserde mahremiyet, "rahat bırakılma hakkı" olarak tanımlanmıştır. Dolayısıyla modern anlamdaki mahremiyet anlayışına ait ilk tohumun bu eserle atıldığı söylenebilmektedir.

Mahremiyet bireysel bir hak olmasıyla beraber, özgürlük ve demokrasi için de temel bir gerekliliktir (Hartmann, 2022, s. 50). Özel hayat, gizlilik ve mahremiyet gibi kavramlar İnsan Hakları Evrensel Beyannamesi (1948) ve Avrupa İnsan Hakları Sözleşmesi (1950) gibi uluslararası metinlerde temel insan hakkı şeklinde yer bulmuştur. Dönemin öncü metinlerinden birisi de Türkiye'nin 1961 Anayasası olmuştur. Anayasanın 15. maddesinde *"adlî kovuşturmanın gerektirdiği istisnalar dışında"* özel hayatın gizliliğine dokunulamayacağı yer almaktadır. Önceki anayasalarda yer almayan kavram, küresel çapta mahremiyeti korumaya yönelik ilk yasal düzenlemelerden birisi olarak kabul edilmektedir (Strömholm, 1967).

Mahremiyete yönelik üzerinde uzlaşılmış, tek ve net bir tanım yoktur. İletişimciler, hukukçular, sosyologlar ve çeşitli alandaki uzman kişiler mahremiyeti farklı açılardan ele alarak farklı tanımlarda bulunmuştur. ABD'li hukukçu Daniel J. Solove (2002, s. 1094), mahremiyet kavramına atfedilen farklı bakış açılarını altı ana başlık altında toplamıştır; (1) rahat bırakılma hakkı, (2) kişisel bilgiye sınırlı erişim, (3) gizlilik, (4) kişisel bilgi kontrolü, (5) kişilik hakları ve (6) özel olma durumu. Bu başlıklar, mahremiyetin ne kadar zengin anlamlar içerdiği ve birey için ne kadar önemli olduğunu vurgulamaktadır.

Mahremiyet, bireyin neyi kendinde saklayacağını, neyi başkasıyla paylaşacağını kontrol edebilme ve denetleyebilmesidir. Bireyin kendisine ait bir dokunulmazlık alanıdır. Hartmann (2022, s. 50), Sir Edward Coke'un 17. yy'de yayımladığı *The Institutes of the Laws of England* adlı eserinde yer alan "bir adamın evi kalesidir ve her adamın evi onun en güvenli sığınağıdır." ifadesine atıfta bulunarak bu sığınağı, fiziksel

bir alandan ziyade düşüncelerin, duyguların ve özel bilgilerin barındığı bir mahremiyet alanı olarak kabul eder. Benzer olarak Strömholm da (1967, s. 16-17) 19. ve 20. yy'de özel ve kamu alanı arasındaki uçurumun derinleştiğini, özel alanın dokunulmazlığı ideolojisinin güçlendiğini ve orta sınıfın "evim benim kalemdir" felsefesini benimsediğini dile getirir.

Mahremiyet ihlali bireyin özerkliğini ve "kendi kaderinin efendisi" olmasını engeller (Lynch, 2016). Bu bağlamda Edward J. Bloustein (1964), mahremiyet hakkının zedelenmesinin yalnızca zihinsel bir probleme yol açmadığını, bunun "insan onuruna bir darbe" ve "kişilik saldırısı" olduğunu savunmuştur. Gizli telefon dinlemeleri ve evine izinsizce girilip eşyalarının karıştırılması gibi eylemlerle karşılaşan bireyler duygusal travmalar yaşasa da bu davranışların asıl yarattığı problem kişinin bireyselliğini küçük düşürmesidir. Çünkü Bloustein mahremiyeti bireyselliğin içsel değeri üzerine inşa eder. "Kişisel özgürlük" olarak isimlendirdiği kavram bireyselliğin belirli müdahalelerden azade olma hakkını içerir. Kavram, doğrudan özerklikle bağlantılıdır. Özerkliğe, bir kararın doğrudan zorlanarak veya kişinin değerlerini dolaylı olarak kontrol ederek zarar verilebilir (Lynch, 2016, s. 86 - 87). Mahremiyet ihlali özerkliği zayıflatarak kişinin kendisine ait bilgileri kontrol etme hakkından yoksun bırakılmasına neden olur.

Mahremiyet, doğrudan özel alana işaret eder. Kamusal ve özel alan arasındaki ayrım Antik Yunan'a kadar dayanmaktadır. Aristoteles, kamusal alan olan "polis" ile özel alan olan "oikos"u birbirinden ayırmıştır. Buna göre *polis*, yurttaşların katılımıyla yönetilen bir kamusal alanken; *oikos*, aile ve bireysel yaşamın idame edildiği özel alan olarak tanımlanmıştır. Yakın tarihte bilginin kamusal mı yoksa özel mi olduğu veya bu ayrımın nasıl gerçekleştirildiği üzerine yeniden tanımlanma ihtiyacı doğmuştur. Neyin "kamu" neyin "özel" olduğu ve bu kavramların ayrıştırılmasında önemli kilometre taşlarından birisi bilginin herkese açık olup olmamasıdır. Herkese açık veriler "kamu" niteliği taşırken; bireysel mektuplar, kişisel günlükler veya tutulan ajandalar "özel" nitelikli olarak kabul edilir (Strömholm, 1967, s. 66). Kamusal verilere örnek olarak devlet harcamaları, hava durumu, coğrafi bilgiler veya kamu istatistikleri gibi halka açık bulunabilen veriler verilebilmektedir. Özel nitelikli veriler, kamusalın tam aksine, oldukça hassas, çoğunlukla bireysel ve ifşası mahremiyeti zedeleyebilecek verilerden oluşur.

DeBrabander, mahremiyetin anlaşılmazlığını ve önemsiz görülmesini Platon'un Meno diyalogu üzerinden ele alır (2020, s. 21-22): Meno diyalogunda, Sokrates'in ısrarlı sorgulamasıyla karşılaşan Meno, kendini savunma becerisini kaybeder ve kendini ifade etmekte zorlanmaya başlar. Platon, bu diyalog aracılığıyla insanların sıkça kullandığı kavramların gerçek anlamı ve önemini bilmekten ne kadar uzak olduklarını vurgular. DeBrabander de bu diyalog örneği ile dijital çağda mahremiyet ve gizlilik gibi kavramların sıkça kullanılmasına rağmen yanlış anlaşıldığını ve yeterince önemsenmediğini iddia eder. Yazar, mahremiyetin korunmasını "bireysel özerkliği ve kişisel özgürlüğü savunmakla" doğrudan bağlantılı olduğunu belirtir. Mahremiyetin korunmaya çalışıldığı ise gözetleme faaliyetleridir. Bu bağlamda gözetleme, bireyin kendini özgürce ifade etme ve hayatını kendi dilediği gibi idame ettirme becerilerini tehdit eden bir unsur olarak tanımlanır.

Mahremiyete ilişkin sorunlar büyük ölçüde gözetleme ile başlar fakat toplanan verilerin işlenme süreçleri farklı sorunlar ortaya çıkartır. Solove (2011, s. 22), bu durumu Franz Kafka'nın Dava romanından esinlenerek açıklamaktadır. Roman, bir adamın tutuklandığını ancak suçunun ne olduğunu öğrenemediğini anlatır. Gizemli bir mahkeme adam hakkında bilgi toplayıp onun hayatını etkileyen kararlar alır ama adam bu bilginin nasıl kullanıldığı hakkında hiçbir şey öğrenemez. Toplanan bilgilerin nasıl işlendiğinin bilinmemesi, bireyin güçsüz kalmasıyla ve çaresizliğe uğramasıyla sonuçlanır. Bu metafor ile Solove, gözetleme ile toplanan verilerin yanında bu verilerin nasıl işlendiğinin de mahremiyetin ihlali açısından önemli bir sorun oluşturduğunu ve sürecin bireyi savunmasız bıraktığını vurgular.

Günümüz bilgi çağında bilgiye erişim iki yönlü işlemektedir. Kullandığımız ağa bağlı cihazlarla dünyadaki herhangi bir bilgiye hızlıca erişebiliriz. Diğer taraftan, ağa bağlı olma durumu bizi de başkalarının erişimine açabilir. Lynch'in (2016, s. 66) ifadesiyle biz ağın penceresinden dışarı bakarken, aynı zamanda ağ da pencerenin içerisine merakla bakmayı sürdürmektedir. Bu merak, izinsiz bir gözetlemeyle mahremiyeti zedeleyecek boyuta geldiğinde durum karmaşık bir hâl almaya başlamaktadır.

Sosyal bir varlık olarak insan genellikle kişisel bilgilerini farklı seviyelerde paylaşma ihtiyacı duyar. Fakat özel bilgilerini kimlerle paylaşacağına kendisinin karar vermesi beklenir (Lokke, 2018, s. 22). Bu özel bilgilerin izinsiz toplanması ve farklı gruplarla paylaşımı, mahremiyet ihlaline sebep olur. Privacy International'ın Eylül 2019'da yayımladığı *Your Mental Health For Sale* başlıklı rapor, ruh sağlığı kategorisindeki web sitelerinin ilgili kullanıcı verilerini farklı taraflarla nasıl paylaştığını gözler önüne sermektedir (Privacy International, 2019). Rapora göre bu kategorideki siteler Meta, Amazon ve Google'ın yanı sıra diğer reklam teknoloji şirketleri ve veri ticareti yapan şirketler ile iş birliği yapmaktadır. İş birliğinin bir sonucu olarak ise bu kurumların izleyicileri kullanıcı davranışlarını site üzerinde takip edebilmekte, çözdüğü ruh sağlığı testlerini kayıt altına alabilmekte ve hatta üst verilerini toplayabilmektedir. İzleyici yerleştiren tüm üçüncü tarafların ortak noktası ise yer aldıkları sitelere her kullanıcıya atadıkları "benzersiz tanımlayıcı" çerezler ile onları her yerde takip etmek istemeleridir. Sosyalliğin getirdiği bir davranış ile başlayan süreç, ileri aşamalarda izinsiz biçimde toplanan en hassas verilerin farklı gruplara ulaşmasına yol açabilmektedir.

Hızla gelişen teknolojik dünyada herkes için mahremiyeti ön planda tutmak gitgide zorlaşmaktadır. Acquisti ve arkadaşları (2015), mahremiyetin nasıl sağlanacağını veya sağlanması gerektiğiyle ilgili tartışmaları iki farklı yaklaşımla ele alır. İlk yaklaşım, kullanıcıların kendi mahremiyetlerini kendilerinin koruyabileceği becerisine sahip olduklarını varsayar. Diğer ifadeyle, kullanıcılar aktif birer karar alıcıdır ve kendi kaderlerini tayin edebilirler. Bu yaklaşıma sahip olanlar yasal düzenlemeleri ve politikaları eleştirerek bilgi teknolojilerinin faydalı ilerleyişine ve ortaya çıkan yeni ürünlerin potansiyel faydalarına müdahale edildiği görüşündedir. Diğer yaklaşım ise teknolojinin giderek karmaşık hâle gelmesinden dolayı kullanıcıların mahremiyetlerini yönetebilme kabiliyetlerinin zayıfladığına dikkat çekmektedir. Buna göre açık rıza verme, izin tercihlerinde aktif rol oynama gibi karar alma davranışları kullanıcıyı yeterli derecede koruyamamaktadır. Bunun yerine veriyi talep edenler ve veri sahiplerinin aktivitelerini düzenleyici yasaların sıkı şekilde takip edilmesi gerekmektedir. Mahremiyeti temel bir

insan hakkı olarak kabul ettiğimizde her iki yaklaşımın dengeli birlikteliği, mahremiyetin güvenliği ve korunması için oldukça değerlidir.

Diğer bir konu, kullanıcıların kendi mahremiyetleri hakkında ne düşündüğüdür. Kullanıcılar, konu kendi mahremiyetleri olduğunda nasıl bir yaklaşıma sahiptir? Burada karşımıza genellikle mahremiyet ikilemi denilen kavram çıkmaktadır. Buna göre birçok kullanıcı dijital mahremiyetine ilişkin endişeler taşırken davranışlarına bunu yansıtmamaktadır. Bu tutarsızlık durumu, dijital platformların veri toplama faaliyetlerini sınırlamadan devam etmelerine destek olmaktadır. Özellikle e-ticaret alanında küçük ödüller ve indirimler aracılığıyla tetiklenen kullanıcılar, mahremiyet endişelerini bir anda azaltabilmektedir. Kokolakis (2017), mahremiyet ikilemini alan yazını tarayarak araştırmıştır. Kokolakis, ikilemin oluşmasında anlık tatmin ve psikolojik yanlılık gibi etmenlerin söz sahibi olduğunu vurgularken bu ikilemin "karmaşık ve çok yönlü bir olgu" olduğunu belirtmiştir. Dolayısıyla bu ikilemin nasıl oluştuğu üzerine yapılacak yeni araştırmalar, yeni görüşlerin ortaya çıkmasına yardımcı olabilir.

Platformların, mahremiyeti temel bir insan hakkı görerek topladıkları verileri, aldıkları izinleri ve yaptıkları iş birliklerinin şeffaflıkla paylaşmaları beklenmektedir. Bu paylaşımların yeri de çoğunlukla yasal metinlerdir. Oysaki durum, yasal ve etik açıdan sorunlar içerebilmektedir. Örneğin, Hidaka ve arkadaşları (2023), Japonya'daki popüler mobil uygulamaları analiz ettikleri araştırmada, bazı uygulamaların yerel dilde (Japonca) mağazada yer aldığına, yerel dilde kullanılabildiğine fakat gizlilik sözleşmesi gibi önemli metinlerin orijinal dilinde (Örn: İngilizce) olduğuna dikkat çekmektedir. Araştırmacılar, dil bariyeri oluşturan bu durumu, Harry Brignull'un "aldatıcı örüntüler" kavramına yeni bir örüntü ekleyerek açıklar. Buna göre ortaya koydukları "Dilsel Çıkmaz" (Linguistic Dead-End) örüntüsü *"dili temel düzeyde manipüle ederek kullanıcıların bir uygulamanın arayüzünü ve/veya içeriğini anlamasını engelleyen veya cesaretini kıran bir tasarıma atıfta bulunan"* yeni bir aldatıcı örüntü olarak tanımlanmaktadır. Bu ve buna benzer durumların mahremiyet ikilemi gibi olguların oluşmasına neden olduğu görülürken; Acquisti ve arkadaşlarının ilk yaklaşımındaki gibi kullanıcıların kendi kaderlerini kendilerinin çizebildiği varsayımının sahada her zaman yer bulmadığı da açığa çıkmaktadır.

Sağlık Verileri, Mobil Sağlık Uygulamaları ve Metalaşan Sağlık

Sağlık verisi, bireyin ruhsal ve fiziksel sağlığına ait her türlü veridir. Sağlık verileri hassas ve kişiye özel veri olarak kabul edilmektedir. Bu veriler, bir yandan kişinin tıbbi geçmişine, teşhis edilen hastalıklarına ve laboratuvar sonuçlarına dair bilgiler içerirken, diğer yandan bireyin günlük aktivite seviyesi, nabız, tansiyon, kan oksijen seviyesi, kan şekeri, uyku düzeni ve beslenme alışkanlıkları gibi yaşam tarzına dair verileri de kapsamaktadır. Modern öncesi dönemde sağlık verilerinin ilk defa izlenmesi, 1300'lü yılların başındaki hıyarcıklı veba salgınına kadar uzanmaktadır. O dönemde, Venedik Cumhuriyeti'ne yakın bir limana yanaşan gemilerdeki yolcular, sağlık yetkilileri tarafından veba benzeri hastalık belirtileri için taramaya tabi tutulmuş ve buna ilişkin veriler kaydedilmiştir. Bu önlemler sayesinde, potansiyel hastaların karaya çıkması engellenmiştir (Thacker, 2010).

Dijitalleşmeyle beraber sağlık verileri, veri pazarında önemli bir yer edinmiştir. Google, Kasım 2019'da giyilebilir akıllı cihaz olan Fitbit'i 2,1 milyar dolara satın aldığını

duyurmuştur. O tarihte, sağlık verisi takibi yapan giyilebilir cihaz firmaları arasında zirvelerde dolaşan Fitbit'in ekonomik değerini, teknolojisi ve yenilikçi hizmetleri ile birlikte sahip olduğu milyonlarca Fitbit kullanıcısının kişisel sağlık verileri belirlemiştir (Knight, 2021). Veri pazarının aktörlerinden veri şirketleri bu alanda pazarlama firmalarına birçok veri sağlamaktadır. Örneğin, MEDbase200 adlı sağlık ve tıp verileri satan şirket, kişisel bilgileri içeren listeleri ticari amaçlarla satışa sunmuştur. Bu listeler, "ereksiyon problemi yaşayanlar", "alkol sorunu olanlar", "AIDS'li hastalar" gibi sınıflandırmaları içermekte olup, 1000 kişi başına 79 dolar fiyatla satışa çıkarmıştır (Hill, 2013).

Joanne Kim'in, ABD vatandaşlarının ruh sağlığı verilerinin ticaretinin nasıl gerçekleştiğini ortaya çıkarttığı rapor bize sağlık verisi endüstrisi hakkında detaylı bilgi vermektedir (2023). Kim'in görüşme yaptığı veri şirketlerinin bazısı 5000 kayıt için 275 ABD doları ücret talep ederken; bazıları ise yıllık 75 ila 100 bin dolar arasında değişen ücretlerle abonelerine bireylerin ruh sağlığı bilgilerini erişime açtığı görülmektedir. Raporda bir veri şirketinin araştırmacıya depresyon, bipolar bozukluk, anksiyete sorunları, panik atak, kanser, kişilik bozukluğu gibi hastalıklara sahip bireyleri ırk ve etnik kökene göre gruplanmış şekilde pazarladığı belirtilmiştir. Rapordaki önemli bir husus da veri şirketlerinin gizlilik politikalarına ilişkindir. Veri şirketlerinin, ruh sağlığı verilerinin toplanması, düzenlenmesi ve birleştirilmesi gibi konularda müşterilerine ve veri sahibi kullanıcılara bilgi verme konusunda oldukça az istekli olduğu gözlemlenmiştir.

Sağlık verileri kullanıcının sağlıkla ilişkili eylemleri aracılığıyla doğrudan toplanabildiği gibi farklı verilerin bir araya getirilerek tahmin yürütülmesiyle de oluşturulmaktadır. Amerikalı indirim mağazası Target'ın yaptığı pazarlama stratejisi bunun popüler örneklerinden birisidir. Target, 2002 yılında hazırladığı bir algoritma aracılığıyla alışveriş alışkanlıklarını baz alarak hamile olması muhtemel kadınlara gönderilmek üzere promosyon ürünlerle ilgili kuponlar hazırlamıştır. Kızının hamile olduğunu bilmeyen bir baba ise Target mağazasına gelerek evine gelen indirim kuponlarının dolayı şikâyette bulunmuştur. Bu örnekte görüldüğü gibi baba, kızının hamileliğini algoritmalar aracılığıyla öğrenmiştir. Target ise bu yaklaşım ve hedefleme grubundan dolayı eleştirilerin odağında olsa da örnekteki gibi hedefleme yapmaya devam etmiştir. Target'ta çalışan bir yönetici, hamile kadınların gözetlendiğini hissetmediği sürece indirimlere ilgi gösterdiğini keşfettiklerini; çevresine ve komşularına da aynı broşürlerin gittiğini düşündüklerini ve onları ürkütmedikleri sürece mevcut pazarlama stratejilerine devam edeceklerini ifade etmiştir (Fry, 2019, s. 39-40).

Günümüzde algoritmik kararların makine öğrenimi ve yapay zekâ teknolojileriyle birlikte verildiği düşünüldüğünde, çevrim içi hareketlerin yarattığı yeni tahminlerin Target örneğinden hayli geniş çaplı ve başarılı olabileceğini söylemek mümkündür. Wall Street Journal'in 2019'da yürüttüğü bir araştırma, regl takip ve anlık kalp ritmi ölçme gibi çeşitli sağlık uygulamalarının kullanıcıların hassas verilerini "üyesi olmasalar bile" Facebook'a aktardığını ortaya koymuştur (Schechner ve Secada, 2019). Bu veriler uygulama içinde gerçekleştirilen tüm etkinlikleri içerirken verilerin bir kısmını hassas yapan durum, hamile kalmaya çalışan bireylerin takvimi veya tansiyon kayıtları gibi verilerin de yer almasıdır. Facebook'a aktarılan bu verilerin Meta reklamlarında pazarlama amaçları doğrultusunda kullanılabileceğini söylemek mümkündür.

Bugün çevrim içi ortamda kullanıcılar çok fazla imkâna sahiptir. Bir kullanıcı, ruh sağlığını test etmek istediğinde bunu yalnızca arama motoruna yazması yeterlidir. Örneğin, "depresyonda mıyım testi" gibi rastgele bir ifade Google'da arandığında onlarca sonuç bizi karşılar. Kullanıcılar en yalın ve masum halleriyle kendileriyle ilgili bir durumu ortaya çıkarmak için bu testlerin birini veya birkaçını çözmek istediklerinde sonuçlarda çıkan siteleri ziyaret etmeleri yeterlidir. Bu siteler bilinen sağlık kuruluşlarının siteleri olabildiği gibi daha önce hiç duymadığımız bir psikiyatri merkezi, Onedio gibi eğlence platformları veya yabancı kaynaklı fakat Türkçe desteği olan web siteleri olabilmektedir. Kullanıcılar, depresyon testinde verdikleri cevaplar ile sonucun ne olacağını merakla beklerken, gayet anlaşılır bir şekilde bu cevapların nerede depolandığıyla veya kimlerin bu sonuçları göreceğiyle ilgilenmezler. Hayatın olağan akışında bir insanın bu kadar enformasyon yükü altında kalması veya farkındalıkla hayatına devam etmesi pek de mümkün değildir. Privacy International'ın (2019) kullanıcılara depresyon testi sunan web sitelerini incelediği araştırmada, testteki her bir cevabın ve depresyon olup olmadığı sonucunun kimlerle paylaşıldığı veya bunları kimlerin kayıt altına alabildiği ortaya konulmuştur. Çözümlemede bulundukları depresyon testi sunan sitelerde izleyicisi bulunan şirketler çektikleri verileri "gerçek zamanlı açık arttırma" adı verilen reklam yöntemiyle reklam borsalarına göndermektedir. Bunun anlamı, bir kişinin nefreti, üzüntüsü, psikolojik sorunları, ailevi ilişkileri, uyku durumu, hayalleri veya iştahı anlık olarak reklam borsasına reklamcılar için hedeflenebilir veriler olarak iletilmektedir. Bazı siteler kullanıcı cevaplarını URL yapısında açığa çıkartmaktadır (örneğin 1=evet, 0=hayır olmak üzere *duzensiz-uyku=1&istah=0*). Bazıları ise Hotjar gibi web sitesi davranışlarını kayıt altına alan üçüncü taraf hizmetleri barındırmaktadır. Bu hizmeti sağlayan şirketler, izleyici olarak bulundukları sitelerdeki tüm etkileşimleri daha sonradan bir video gibi izlenebilecek şekilde kaydetmektedir. Kullanıcının bilgi arayışında bulunduğu süreç metalaşarak, farklı şirketler tarafından farklı endüstrilerin farklı amaçları doğrultusunda kullanılmaktadır. Paylaşılan ve metalaşan verinin hassas verilerden oluşması, durumun ciddiyetini daha da artırmaktadır.

Sağlık verilerinin toplanması ve üretiminde, diğer ifadeyle büyük çaplı genişlemesinde, mobil cihazlarda çalışan sağlık uygulamaları etkili olmuştur. Mobil sağlık uygulamaları, kullanıcıların sağlık durumlarını izlemeleri ve yönetmelerine olanak tanıyan mobil cihaz hizmetleri olarak ifade edilmektedir. Kalp atış hızı, adım sayıcı, uyku düzeni, beslenme alışkanlıkları, kadın sağlığı vb. uygulamalar, mobil uygulama mağazalarında Sağlık ve Fitness kategorisinde yer almaktadır. Bu uygulamalar, kullanıcıların günlük sağlık rutinlerini görüntülemelerine yardımcı olmakta ve genellikle çeşitli öneriler sunarak sağlığa ilişkin farkındalıklarını artırmayı amaçlamaktadır. Gerek cihazdan gerekse sensörler aracılığıyla toplanan veriler ile kullanıcının sağlığını takip etmesine, sağlıklı yaşam tarzı benimsemesine, kişiselleştirilmiş öneriler almasına ve anlık bildirimler ile hatırlatmalar almalarına yardımcı olmaktadır.

Mobil sağlık uygulamalarının hayatımızdaki yeri gün geçtikçe artmaktadır. Genel olarak bakıldığında, Statista'nın Aralık 2023 verilerine göre Google Play Store'da yaklaşık 2.5 milyon mobil uygulama yer almaktadır. 2022 itibariyle Sağlık ve Fitness kategorisinde yaklaşık 60 bin uygulama mağazada bulunmaktadır (Ceci, 2024). 2023 yılında bir önceki yıla göre %3.9 artışla yaklaşık 150 milyar mobil uygulama cihazlara

indirilmiş; bunun %70'i Google Play Store'da gerçekleşmiştir (Iqbal, 2024). Akıllı telefonlarda geçirilen zamanın %85'ini mobil uygulamalar kapsamaktadır (Zippia, 2023). Küresel mobil uygulama pazarının büyüklüğü ise 2023'te 467,12 milyar dolarken 2027'ye kadar 673,79 milyar dolar olması beklenmektedir. 2023 itibariyle pazar büyüklüğündeki en yüksek payı mobil oyun (172,4 milyar dolar) ve sosyal ağlar (143 milyar dolar) almaktadır. Sağlık ve Fitness kategorisinin pazardaki payı ise 2016 yılında 1,27 milyar dolarken 2023'te 4,52 milyar dolar olmuş; 2027'de ise 6,73 milyar dolar olması beklenmektedir (Statista, 2024). Uygulamaların kullanıcıların sağlıklarını izlemeleri ve yönetmeleri için sunduğu imkanlar, popüleritesinin artmasına katkıda bulunmaktadır.

Mobil sağlık uygulamalarının artan kullanımı, beraberinde mahremiyet ve veri güvenliği konularındaki endişeleri de gündeme getirmektedir. Kişisel verinin mülkiyeti, veriyi paylaşanlara ve hakkında öngörülenlere erişim, düzenleme ve paylaşım hakkı verilmesiyle ilişkidir. Mülkiyet, hassas veri olmaları sebebiyle sağlık verisi bakımından ele alındığında ise kritik bir öneme sahiptir (Sherwani ve Bates, 2021). Kullanıcıların sağlık uygulamalarındaki verileri izinsiz olarak üçüncü taraflarla paylaşılabilir ve veriler uzak sunucularda barındırılarak kuruluşların kendi çıkarlarına hizmet edebilir. Sağlık verisinin kaotik bir biçimde dolaşımı bireysel zararlara neden olabileceği gibi, toplulukları ve hatta devletleri de etkileyecek şekilde kötü amaçlı kullanımlar doğurabilir.

Fitness uygulaması olan Strava, 2017 yılında kullanıcı aktivitelerinden oluşan ve anonim olarak topladığı konum verilerinden küresel bir ısı haritası yayımlamıştır. Üç trilyondan fazla GPS veri noktasından (Hern, 2018) ve 700 milyon aktiviteden (Robb, 2017) oluşan bu haritanın paylaşımından bir süre sonra 20 yaşında bir analist olan Nathan Ruser, harita aracılığıyla askeri birliklerin hareket rutinlerini ve gizli askeri üslerin konumlarını ortaya çıkarmıştır (Ruser, 2018). Strava'nın anonimleştirerek paylaştığı açık veriler bize toplulukların güvenliği ve gizliliği bakımından nasıl bir risk oluşturabileceğini göstermektedir.

Sağlık ve Fitness uygulamalarının yarattığı mahremiyet endişelerinin başında risk altındaki grupları belirleme işlemi yer almaktadır. Bu gruplar kişiselleştirilmiş reklam pazarından, sigortacılık ve bankacılık faaliyetlerinde ihtiyaç duyulan bilgi eksikliğini giderme amacına kadar birçok ilgili alanda sürece dahil edilmektedir (Metzger vd., 2021). Algoritmalar, riskli ve dezavantajlı grupları belirlemede kritik bir öneme sahiptir. Belli adımları ve rutinleri takip ederek örüntüler oluştururlar ve bireyleri bu örüntülerin içerisine eklerler. Metzger ve arkadaşlarının ifade ettiği kullanım alanlarını, sağlık verileri ve algoritma çıkarsamaları bağlamında biraz daha açabiliriz.

Genel olarak veri, pazarlama ve reklam faaliyetlerinin merkezinde yer almaktadır. Örneğin, Jon Keegan ve Joel Eastwood, dijital reklam pazarı Xandr'da 650 binden fazla pazarlanabilir veri etiketinin olduğunu ortaya çıkarmışlardır (Keegan ve Eastwood, 2023). Başka bir ifadeyle, Xandr aracılığıyla reklam vermek isteyen bir kuruluş, platform üzerinde hedeflenebilir 650 bin adet kitle grubunu seçebilmekte ve onlara doğrudan reklamla erişebilmektedir. Ayrıntılı şekilde etiketlenmiş gruplarda kimlerin olduğunu ise çeşitli kaynaklardan toplanan ve işlenen veriler belirlemektedir. Bu kaynaklar genellikle çevrim içi ve çevrim dışı etkinlikler ile açık veriler gibi geniş bir yelpazeden oluşmaktadır. Hedeflenebilir kitle gruplarının yaratımındaki nihai hedef, reklam

verenlerin mesajlarını doğru biçimde yönlendirmesi ve kullanıcıların ilgi duyma olasılığı yüksek olan ürün ve hizmetlerle buluşması olarak kabul edilmektedir. Bu ön kabul ile yola çıkıldığında süreç için "reklam veren ile reklam görüntüleyenlerin mükemmel eşleşmesi" tanımı yapılabilir. Öte yandan bu birliktelikte kullanıcıların hassas verileri işin içine dâhil edildiğinde mahremiyet ihlali olmak üzere birçok açıdan sorunlu alan gün yüzüne çıkmaktadır.

Aşağıdaki tabloda Keegan ve EastWood'un Github üzerinden paylaştığı, Xandr'da bulunan 650 bin veri etiketi içerisinde yazarın rastgele seçtiği sağlık verileri yer almaktadır. Verilere bakıldığında hastalıklar, psikografik durumlar, sağlık kuruluşu ziyaretleri, ruh sağlığı ve kişilik tipi gibi birçok alandan hassas sağlık verisinin veri tabanında bulunduğu görülmektedir.

Tablo-1: Xandr reklam platformunda hedeflenebilir kullanıcı grupları arasından sağlıkla ilişkili rastgele seçilmiş veri setleri

Alerjik Astım	Kolestrol	Gebelik ve Cinsel Sağlık Klinikleri
Şeker Hastalığı (Tip 1, Tip 2)	Duyma Kaybı	Aile Hekimliği Eczaneleri
Uyku Apnesi	Menopoz	Fizik Tedavi ve Spor Hekimliği Klinikleri
Sigarayı Bırakma	Kireçlenme	Rehabilitasyon Merkezleri
Seboreik Dermatit	Kalp Krizi	Acil Bakım Merkezi
Uykusuzluk	Eklem Ağrısı	Doğum Öncesi Programa Katılma
Diz Protezi	Protein Tozu Kullananlar	Kayropraktik
Migren	Bağımlı	Nevrotik Bozukluklar
Kuru Göz	Depresyon	İşkolikler
Reflü İlacı Alanlar	Fibromiyalji	Hayalperestler
Kırmızı Göz Hastalığı	Hızlı Kilo Verenler	Duygusallar
Sarı Nokta	Yeme Bozukluğu	Romantikler
Laktoz İntorelansı	Kalp Yetmezliği	Açık Gönüllüler
Hamile (12-24 Hafta)	Miyokard Enfarktüsü	Yalnız Kurtlar
Uyku İlacı Alanlar	Crohn Hastalığı	Aşırıcılar
Hipertansiyon	Hepatit C	Hapsolmuş
Parkinson	Sedef Hastalığı	Kışkırtıcı
	Otoimmün Hastalıklar	İddialı

Kullanıcıların çevrim içi platformlara kendi sağladığı veriler çoğunlukla ad, soyad, doğum tarihi, e-posta adresi ve cep telefonu gibi kişisel veri kabul edilebilecek bilgilerden oluşmaktadır. Yukarıdaki tabloda görülen veri etiketlerinin neredeyse hepsi çıkarımsal yöntemle, yani birden çok veriyi bir araya getirip, işleyip yeni bir anlam çıkartarak üretilmiştir. Bu verilerin kaynaklarını irdelemek istediğimizde ucunun nereye varacağını kestirmek oldukça zordur. Yalnızca tahmin edilebilir yöntemler üzerinden yorum yapılabilir. Örneğin, klinik vb. sağlık kuruluşu ziyaretleri kullanıcıların konum verisini

toplayan herhangi bir mobil uygulama kaynaklı olabilir. Bir kullanıcıyı hayalperest olarak tanımlamak için satın alma davranışları, arama geçmişi ve takip ettiği içerikler gibi genel yöntemlere başvurulabilir. Diğer yandan mobil oyun uygulamaları da tek başına bir kişinin yüksek ihtimalle "hayalperest" olduğunu öngörebilir. Oynadığı oyun türleri (fantastik, rol yapma), oyun içindeki davranışları, hikâye akışındaki tercihleri ve topluluk sohbetleri kullanıcının kişiliği hakkında bilgi verebilir.

Tablodaki daha ayrıntılı sağlık verileri, doğrudan sağlıkla ilişkili uygulamalardan, web sitelerinden; çevrim içi veya çevrim dışı aktivitelerden toplanan veriler neticesinde oluşturulmuştur. Bu hassas verilerin reklam verenler tarafından hedeflenebilir olması etik sorunlar ortaya çıkarabildiği gibi, banka ve sigorta kuruluşlarının potansiyel veya mevcut müşterileri hakkındaki derinlemesine bilgi ihtiyaçlarını gidermesi ve bunu izinsiz yapması bakımından da sorunludur.

Lokke, günlük hareket kalıplarının birkaç kez gözlenmesiyle kişiye atfedilecek özgün bir düzenin ortaya çıkması için yeterli olduğunu belirtir (2018, s. 42). Bugün bir nabız uygulaması kullanan ve bunu akıllı saatiyle bütünleştiren bir kullanıcının uyku apnesi olduğu nasıl anlaşılabilir? Sathyanarayana ve arkadaşlarının (2016) derin öğrenme yöntemiyle giyilebilir cihazlardan elde ettiği veriler, söz konusu cihazların uyku kalitesi ve verimliliğini doğru tahmin edebildiğini bize göstermektedir. Buradan yola çıkarsak şu öngörülerle ilerleyebiliriz; uyku apnesi olan kişilerde oksijen azalır, kalp ritmi artar. Nabızda belirgin değişiklikler olur. Uyku sırasında kesintiler ve sık uyanmalar olabilir. Uyku süresi ve kalitesi uygulama tarafından takip edilip, kayıt altına alınır. Rutin uyuma düzeninin dışında farklı örüntüler gözlemlenir. Nefes alma güçlüğü veya horlama sesleri uygulama tarafından dinlenebilir. Bu bilgiler bir araya getirildiğinde kişinin yüksek oranda uyku apnesi olduğu anlaşılabilir. Akıllı telefonunda nabız uygulaması kullanan ve uyku apnesi olduğu etiketlenen bir kullanıcının yaşayabileceği etik sorunlar ve mahremiyet ihlalleri şu şekilde sıralanabilir:

- Kalp ritmi verisi; parmak izi, yüz tanıma ve ses tanıma gibi kişinin benzeriz özelliklerini ifade eden biyometrik veri kapsamında yer almaktadır. Toplama, saklama ve paylaşma koşulları açıkça ifade edilmeli ve açık rızaya bağlı gerçekleşmelidir. Şartlar yerine getirilmediğinde mahremiyet ihlali yaşandığı anlamına gelir.
- Toplanan sağlık verilerinin güvenliği sıkı biçimde sağlanmazsa veri sahipleri kalıcı zararlar görebilir.
- Uygulamada yer alan üçüncü taraf şirketlerin izleyicileri (Google, Meta, Adcolony vb.) uygulamadaki etkinlikleri ve verileri kayıt altına alabilir; kendi sunucularına göndererek başka ortaklarından topladıkları veriler ile bir kullanıcı hakkında detaylı bir bilgi havuzu oluşturabilir.
- Kullanıcıların rızası veya bilgisi olmadan toplanan verilerin algoritmalar ile işlenerek onlardan habersiz onlar hakkında yeni öngörüler üretmesi (bkz: uyku apnesi) etik ve mahremiyet bakımından sorunludur.
- Verilerin veri şirketleriyle izinsiz paylaşılması ve veri ticaretinin metası olması, kullanıcıları mağdur edebilir. Sağlık ve sigorta kuruluşları biyometrik veriler aracılığıyla kullanıcıları doğrudan tanımlayabilir, risk analizleri yapabilir ve sağladığı hizmetlere erişimi maddi ve manevi olarak zorlaştırabilir. Bankalar kredi

başvurularında bu verileri kullanarak kendi çıkarları doğrultusunda önyargılı kararlar alabilir.

- Xandr gibi reklam platformları bu veri etiketlerini pazarlanabilir metalar olarak reklam verenlere sunabilir. Mahrem bilgilere dayalı hassas verilerin hedeflenebilir olması etik sorunlara yol açabilir. Uyku apnesi etiketi içerisindeki kullanıcıları sağlık durumlarıyla ilgili korkutacak, kaygılarını artıracak, hızlı karar almalarına teşvik edecek, tıbbi geçerliliği olmayan ilaçlara yönlendirecek reklamlar kalıcı zararlara neden olabilir.

Belirli bir hizmet doğrultusunda ve bir amaca dayanarak kullanılan mobil sağlık uygulamaları mahremiyet odaklı ele alındığında görüldüğü gibi birçok açıdan sorunlu ve hassas alanlar barındırmaktadır. Sağlık verilerinin hassasiyeti ve yaratabileceği potansiyel tehlikeler göz önüne alındığında bu alanda hizmet sağlayan uygulamalarında üçüncü taraf hizmetlerin kullanımı için açık rıza almaları, kullanıcıların istediği zaman açık rızalarını geri çekebilecekleri alanlar yaratmaları, iş birliklerinin sınırlarını belirten şeffaf sözleşmeler oluşturmaları ve cihazlardan talep ettikleri sıradan ve özel izinlerle ilgili bilgilendirme yapmaları gerekmektedir.

Amaç ve Yöntem

Bu çalışma, kullanıcı mahremiyetini merkeze alarak Sağlık ve Fitness kategorisindeki mobil uygulamaları incelemek üzere tasarlanmıştır.

Araştırmanın Amacı ve Önemi

Akıllı cihaz kullanımı, çeşitliliği ve mobil uygulama sayısındaki paralel artışlar birbirini tetikleyerek veri pazarının daha da büyümesine yol açmıştır. Cihaz ve uygulamaları ilk etapta insanın uzantısı olarak kabul edersek, günümüz çevrim içi problemlerin başında bu uzantılara kimlerin eriştiği ve ne amaçla kullandığı gelmektedir. Şeffaf ve açık biçimde belirtilmeden kullanıcı ile uygulama arasındaki etkileşime dâhil edilen farklı şirketler, bu etkileşimleri izin almadan toplayabilmektedir. Uygulamaların sağlık hizmetleri sunması ise etkileşimlerin "hassas" ve "özel" olması nedeniyle mevcut problemi daha da önemli hâle getirmektedir.

Çalışmanın genel amacı, sağlıkla ilgili hizmet veren ve sağlık verisi toplayan mobil uygulamaların hangi üçüncü taraf izleyicilerle iş birliği içinde olduğu, kullanıcıların cihazlarından hangi izinleri talep ettikleri ve gizlilik sözleşmelerinde iş birliği ve izinlere nasıl değindiklerini ortaya çıkarmaktır. Çalışma, sağlık verilerinin hassasiyetine dikkat çekerken; uygulamalar aracılığıyla sağlık verilerinin nasıl işlendiğini ve paylaşıldığını açığa çıkarması bakımından önemlidir.

Araştırma Soruları

Mobil sağlık uygulamalarının mahremiyet odaklı incelenmesine yönelik araştırmada beş genel araştırma sorusuna cevap aranmıştır:

1. Mobil sağlık uygulamalarında hangi üçüncü taraf izleyiciler yer almaktadır?
2. Mobil sağlık uygulamalarında reklam ve pazarlama hizmeti sağlayan hangi firmaların izleyicileri bulunmaktadır?
3. Mobil sağlık uygulamaları, kullanıcı cihazlarından hangi izinleri talep etmektedir?

4. Mobil sağlık uygulamalarının gizlilik sözleşmeleri hangi dilde hazırlanmış ve ne kadar anlaşılır metinlerdir?
5. Gizlilik sözleşmelerinde üçüncü taraf izleyicilere ve erişim izinlerine nasıl yer verilmiştir?

İlk soruda uygulamalarda üçüncü taraf izleyicilerin olup olmadığı; varsa bunların kimler olduğu ve kullanım amaçları araştırılmıştır. İkinci soruda uygulamaların reklam firmalarıyla ilişkisi göz önünde bulundurularak söz konusu firmaların açığa çıkartılması amaçlanmıştır. Üçüncü soruda uygulamaların mobil cihazlardan talep ettikleri izinler irdelenmiş; bu izinlerin hangilerinin güvenlik seviyesi normal hangilerinin özel/tehlikeli olduğuna cevap aranmıştır. Dördüncü soruda gizlilik sözleşmelerinin dili ve hukukî metinler oldukları için anlaşılırlık seviyeleri mercek altına alınmıştır. Son soruda, varsa üçüncü taraf izleyicilerin ve alınan cihaz izinlerinin sözleşmelerde yer alıp almadığına yanıt aranmıştır.

Araştırmanın Yöntemi

Çalışmanın amacını gerçekleştirmek ve soruları cevaplandırmak için nicel araştırma yöntemi benimsenmiştir. IOS işletim sistemindeki App Store ve Android işletim sistemindeki Google Play mağazalarında bulunan sağlıkla ilişkili tüm mobil uygulamalar çalışmanın evrenini oluşturmaktadır.

Android ile IOS arasındaki temel farklardan birisi Android'in Linux temelli (Stevens vd., 2012) ve açık kaynaklı bir işletim sistemi olmasıdır. Açık kaynak, yazılımın herkes tarafından erişilebilir, değiştirilebilir, dağıtılabilir ve yeniden üretilebilir olduğu bir geliştirme modelidir. Bir nevi tüm geliştiricilerin aynı anda üzerinde çalıştıkları, ekleme ve çıkarma yaptıkları bir yazılım sistemidir (Raymond, 2001). Android'in açık kaynak olması geliştiricilerin, güvenlik uzmanlarının ve araştırmacıların uygulama paketlerini (APK) analiz edebilmelerine olanak tanır. Dolayısıyla üçüncü taraf izleyiciler ve cihazdan talep edilen izinlerin tespiti Android için hazırlanan uygulamalarda daha mümkündür. Bu nedenle çalışmada IOS App Store'daki uygulamalar araştırma evreninden çıkartılmıştır. Çalışma kapsamında amaca yönelik örneklem kullanılarak Google Play mağazasında "Sağlık ve Fitness" kategorisinde yer alan ve Türkiye'de en çok tercih edilen 20 mobil uygulama incelenmiştir. Amaca yönelik örneklemde, belirli bir amaçla örnek olay seçilir (Neuman, 2014, s. 322). Araştırma sorularına cevap bulma potansiyeli en yüksek uygulamalar, en çok kullanıcıya sahip popüler uygulamalar olacağı için ilk 20 uygulama örnekleme dâhil edilmiştir.

İlk 20 uygulamanın belirlenmesi için Google Play mağazasında Sağlık ve Fitness kategorisindeki "ücretsiz en popüler" uygulamalar listelenmiştir. https://play.google.com/store/apps/category/HEALTH_AND_FITNESS adresinden görüntülenen uygulamalara 22 Mart 2024 tarihinde erişilmiştir.

Mobil uygulamaların üçüncü taraf izleyicileri ve cihazdan talep ettikleri izinleri ortaya çıkarmak için iki farklı platformdan yararlanılmış ve sağlanan veriler kontrol edilmiştir. Söz konusu platformlar;

- *Exodus Privacy:* Kullanıcı mahremiyetini korumak için bir araya gelmiş kâr amacı gütmeyen Fransız bir kuruluştur. Android uygulamalarını analiz etmeye

yarayan yazılımları ile uygulamaların röntgenini çekmektedir. Web sitesi: https://exodus-privacy.eu.org/en/

- *ImmuniWeb:* Uluslararası alanda faaliyet gösteren, İsviçre merkezli bir mobil uygulama güvenliği şirketidir. https://www.immuniweb.com/mobile adresi aracılığıyla mobil uygulamalar analiz edilebilmektedir.

Çalışmada veriler nicel içerik analizi yöntemi ile çözümlenmiştir. İçerik analizi, iletişimin "sistematik, nesnel ve nicel betimlenmesi için" oluşturulmuş bir araştırma tekniğidir (Berelson, 1952). Örneklem dâhilindeki uygulamaların üçüncü taraf izleyici verilerini toplamak, kaç farklı izleyicileri olduğunu saptamak, izleyicilerin sıklığını ve türlerini belirlemek için söz konusu yöntem tercih edilmiştir. Bunun yanında kullanıcı cihazlarından hangi tür izinler talep edildiğinin ve bu izinlerin hangilerinin özel/tehlikeli izinler olduğunun belirlemesi süreci de içerik analiziyle gerçekleştirilmiştir. Yine içerik analizinin kullanıldığı çalışmanın üçüncü basamağındaki gizlilik sözleşmeleri, diline göre iki farklı yolla çözümlenmiştir. Türkçe sözleşmeler, iki tema etrafında incelenmiştir. İlk tema, araştırmacının tespit ettiği üçüncü taraf izleyicilerin adlarının ve hizmet verme amaçlarının açık ve şeffaf şekilde yer alıp almadığı; ikinci tema, kullanıcı cihazlarından aldıkları izinlerin açık ve şeffaf şekilde paylaşılıp paylaşılmadığı olmuştur. İngilizce sözleşmelerde metnin yapısı ve diliyle ilgili bir analiz yapılmıştır. İngilizce sözleşmelerde böyle bir yol izlenmesinin nedeni, Türkçe desteği olan uygulamaların sözleşmelerini İngilizce bırakarak zaten kullanıcı mahremiyetini ihlal etmeleri ve anadili İngilizce olan kullanıcılar için sözleşmelerin zorluk derecesini ortaya çıkartma isteği olmuştur. Çalışma kapsamındaki İngilizce gizlilik sözleşmeleri *readabilityformulas.com* aracılığıyla okunabilirlik testine tabi tutulmuştur. Otomatik Okunabilirlik Endeksi (ARI), İngilizce metnin zorluğunu ölçen popüler bir okunabilirlik formülüdür. Metni anlamak için gereken sınıf seviyesine ilişkin bir tahmin sunar. ARI puanı, 1 ile 14 veya daha yüksek arasında değişen belirli bir sınıf seviyesine karşılık gelir. Örneğin, ARI puanının 7.0 olması metnin 7. sınıf okuma seviyesinde yazıldığı anlamına gelir. ARI'nin hesaplanma formülü $ARI = 4.71 \times (karakter/kelime) + 0.5 \times (kelime/cümle) - 21.43$ şeklindedir. Karakter sayısı metindeki tüm harfleri, sayıları, noktalama işaretlerini ve sembolleri içermektedir; boşluklar hesaplamaya dâhil değildir. Araştırmada İngilizce gizlilik sözleşmeleri düz metin olarak eklenmiş ve hesaplama yapılmıştır.

Çalışmada "üçüncü taraf izleyici" olarak tanımlanan yazılımlar, iki olguya işaret etmektedir. İlki, bir uygulama veya web sitesi tarafından doğrudan kullanıcıya hizmet sunmayan, kullanıcıların çevrim içi davranışlarını izlemek ve veri toplamak için kullanılan hizmetleri vurgulamaktadır. İkincisi, yazılım geliştirme kitleridir (software development kit). Bu sistemler yazılım geliştiricilerinin uygulamalarına belirli özellikler eklemek için kullandıkları araç ve kütüphane paketleri olarak tanımlanmaktadır. Örneğin, reklam hizmeti veren şirketler uygulamalarda reklam göstermek için uygulama geliştiricisine bir yazılım geliştirme kiti sağlamak durumundadır (Stevens vd., 2012). Diğer yandan bir platforma *Google ile Kayıt Olma* veya *Facebook ile Giriş Yapma* özelliği de buna örnek verilebilmektedir.

Araştırma, 22 – 29 Mart 2024 tarihleri arasında gerçekleştirilmiştir.

Araştırmanın Bulguları

Bu bölümde araştırma bulguları üçüncü taraf izleyiciler, cihazdan alınan izinler ve gizlilik sözleşmeleri olmak üzere üç başlık ile verilmiştir.

Üçüncü Taraf İzleyiciler

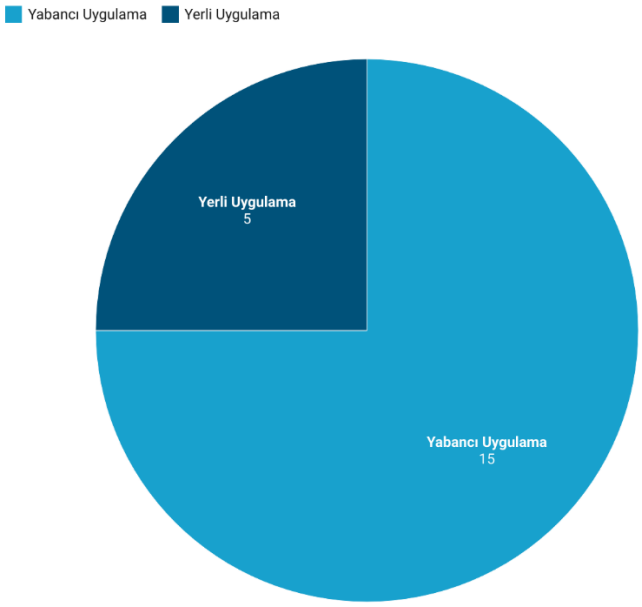
Google Play Store'da Sağlık ve Fitness kategorisindeki ilk 20 ücretsiz en popüler mobil uygulama listesi aşağıdaki Tablo 2'de yer almaktadır.

Tablo-2: Google Play Store'da Sağlık ve Fitness kategorisindeki en popüler ilk 20 mobil uygulama

	Uygulama Adı	Uygulama Kimlik Numarası
1	**e-Nabız**	tr.gov.saglik.enabiz
2	**MAC+: Online Fitness Deneyimi**	com.marsathletic.android.macfit.app
3	**senCard Mobil**	com.acibadem.sencard
4	**Ev Egzersizleri - Ekipmansız**	homeworkout.homeworkouts.noequipment
5	**Adet Takibi - Regl Takvimi**	com.popularapp.periodcalendar
6	**Kilo Verme Programı, Zayıflama**	weightloss.weightlossforwomen.workoutforwomen.womenworkout
7	**Adım Sayar - Pedometre**	stepcounter.pedometer.stepstracker
8	**Adet Takibi - Adet Döngüsü**	com.periodtracker.periodcalendar.ovulation.periodcycle
9	**Pepapp - Adet Takvimi**	com.pepapp
10	**Sağlık Kiti**	com.mearsure.heartratepro.manage
11	**Mi Fitness (Xiaomi Wear)**	com.xiaomi.wearable
12	**Kadınlar için Kilo Verme Spor**	loseweightapp.loseweightappforwomen.womenworkoutathome
13	**Nabız Monitörü ve İzleyici**	com.pulse.heartrate
14	**Wearfit Pro**	com.wakeup.howear
15	**Tansiyon**	com.bpfit.bloodpressure.health
16	**BetterMe: Sağlık Koçluğu**	com.gen.workoutme
17	**Tansiyon Uygulaması**	bloodpressure.bloodpressureapp.bloodpressuretracker
18	**Adım Sayar**	com.tayu.tau.pedometer
19	**AdımPara - Adım At Kazan**	com.omicron.adimpara
20	**Acemiler İçin Yoga-Günlük Yoga**	yoga.beginners.workout.dailyyoga.weightloss

Söz konusu uygulamaların 5 tanesi yerli firmalara, geri kalan 15'i ise yabancı firmalara ait olduğu görülmektedir.

Tablo-3: Google Play Store'da Sağlık ve Fitness kategorisindeki en popüler ilk 20 mobil uygulamanın kökeni



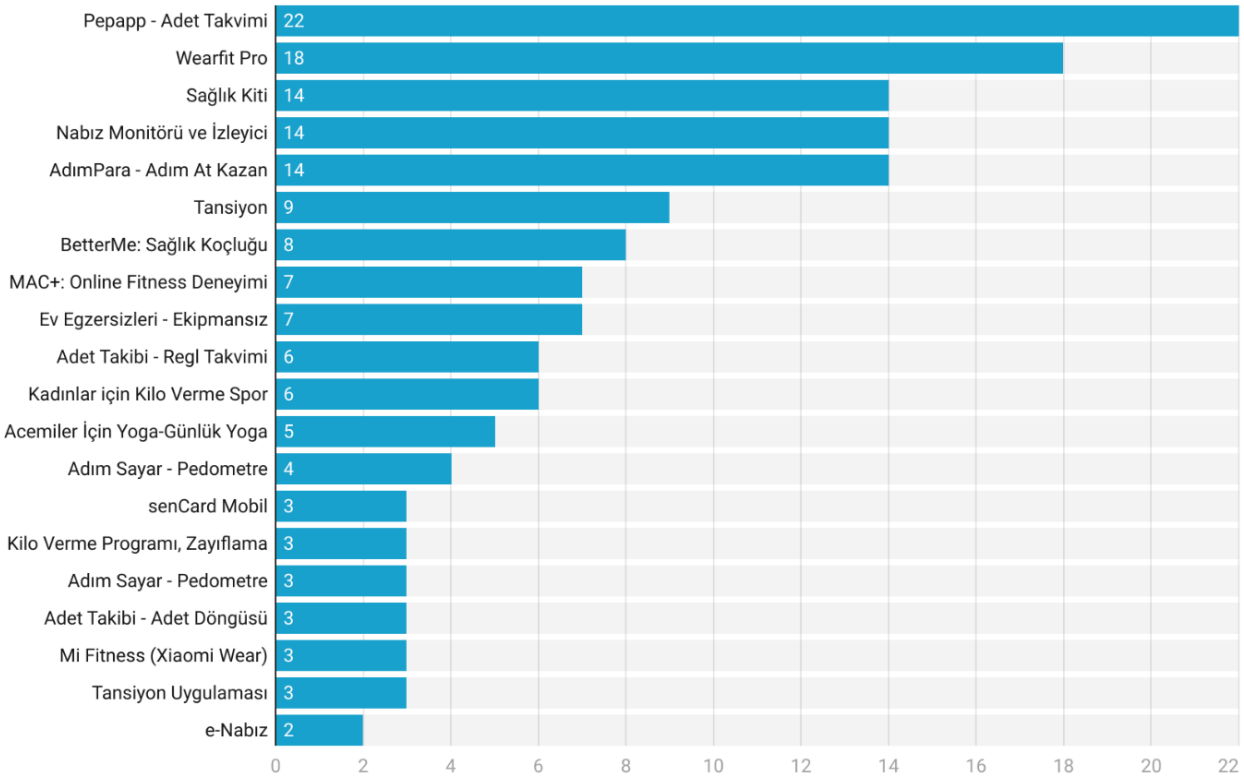
Yerli uygulamalar;

- e-Nabız (T.C. Sağlık Bakanlığı)
- MAC+: Online Fitness Deneyimi (Mars Sportif Tesisler İşletmeciliği A.Ş.),
- senCard Mobil (Acıbadem Grubu),
- Pepapp – Adet Takvimi (Pepapp Teknoloji A.Ş.),
- AdımPara – Adım At Kazan (Yaya Teknoloji A.Ş.)

şeklinde sıralanmaktadır.

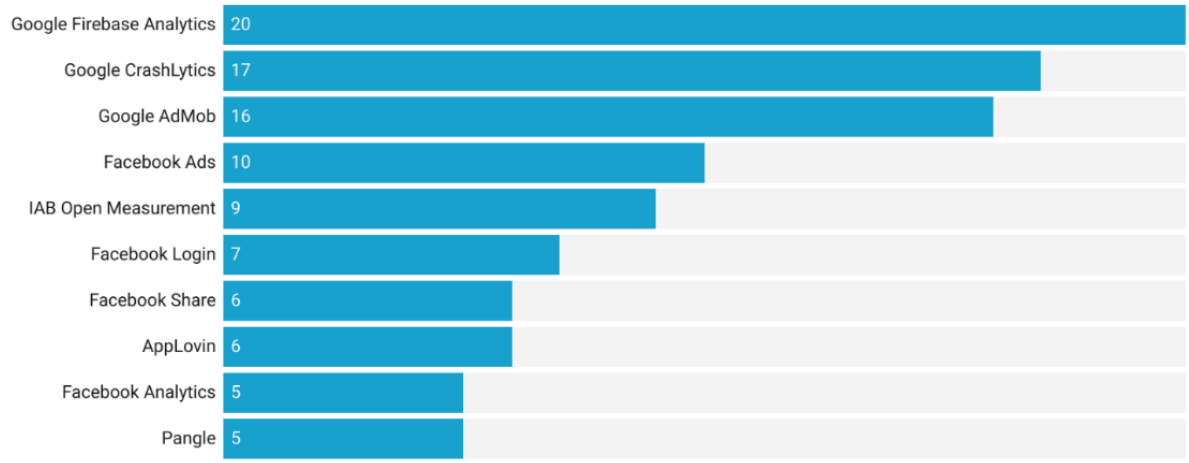
Uygulamaların tamamında üçüncü taraf izleyiciler bulunmaktadır (Tablo 4). Uygulamalar arasında üçüncü taraflarla en az iş birliğini e-Nabız, en çoğunu ise yerli uygulama Pepapp – Adet Takvimi yapmaktadır.

Tablo-4: Mobil uygulamalarda yer alan üçüncü taraf izleyicilerin sayısı. En çoktan en aza doğru sıralanmıştır



Uygulamaların en sık kullandığı ilk 10 üçüncü taraf izleyici Tablo 5'te yer almaktadır. Buna göre tüm uygulamalarda Google ve Meta hizmetlerinin hegemonyası olduğu görülmektedir.

Tablo-5: Mobil uygulamalarda en çok yer alan üçüncü taraf izleyiciler / yazılım geliştirme kitleri



En çok tercih edilen üçüncü tarafların kullanım alan ve amaçları aşağıdaki gibidir:

- *Google Firebase Analytics:* Kullanıcı davranışlarını analiz etmek için kullanılır. Uygulama içindeki etkileşimleri, kullanım sürelerini, hangi özelliklerin kullanıldığını takip eder.
- *Google Crashlytics:* Uygulamanın çökme raporlarını toplamak ve analiz etmek için kullanılır.
- *Google AdMob:* Reklam hizmetleri için kullanılır. Reklam gösterimleri ve tıklamaları gibi reklam etkinliğini izler ve bu verileri reklamverenlere sunar.
- *Facebook Ads:* Facebook reklamlarının etkinliğini ölçmek için kullanılır. Kullanıcıların reklamlara nasıl tepki verdiğini, dönüşüm oranlarını ve diğer reklam metriklerini izler.
- *IAB Open Measurement:* Reklam gösterimlerinin görünürlüğünü ve etkisini ölçmek için kullanılır. Reklamverenlere reklamın ne kadar görünür olduğunu ve hedef kitlenin nasıl etkileşimde bulunduğunu belirlemede yardımcı olur.
- *Facebook Login:* Uygulama ile Facebook arasında bağlantı kurarak uygulama kullanıcılarının Facebook hesapları ile uygulamaya kaydolmalarına / giriş yapmalarına yardımcı olur.
- *Facebook Share:* Uygulama içerisindeki içerikleri Facebook profilinde veya sayfasında paylaşmak için kullanılan bir yazılım geliştirme kitidir.
- *AppLovin:* Uygulama içi reklamların performansını izlemek için kullanılır. Reklam gösterimleri, tıklamalar ve dönüşümler gibi reklam metriklerini izler ve reklamverenlere bu verileri sunar.
- *Facebook Analytics:* Kullanıcı davranışlarını analiz etmek için kullanılır.
- *Pangle:* TikTok'a ait reklam hizmetleri için kullanılır. Uygulamalarda TikTok reklamlarının gösterimini sağlar.

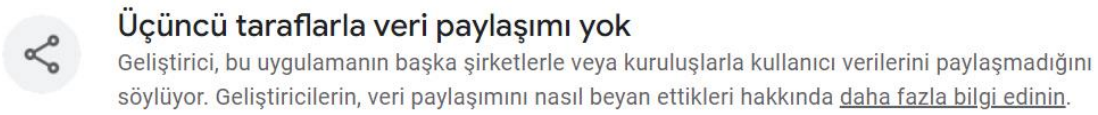
Üçüncü taraf hizmetlerin yoğunlukla analitik ve reklam hizmetleri için kullanıldığı görülmektedir.

Mobil uygulamalar arasında en çok üçüncü taraflarla iş birliği içinde olan uygulama 22 adet ile Pepapp – Adet Takvimi olmuştur (bkz: Tablo 6). Google Play verilerine göre 1 ile 5 milyon arasında kullanıcı olan uygulamada 17 farklı şirketin 22 farklı üçüncü taraf izleyicisi bulunmaktadır. İzleyicilerin neredeyse tamamı reklam ve analitik faaliyetler amacıyla kullanılmaktadır.

Tablo-6: En çok üçüncü taraf izleyiciye sahip uygulama Pepapp – Adet Takvimi uygulamasındaki izleyiciler

1	AdColony	13	Google AdMob
2	Adform	14	Google CrachLytics
3	Adjust	15	Google Firebase Analytics
4	Admost	16	Huawei Movile Services
5	AppLovin	17	IAB Open Measurement
6	AppsFlyer	18	ironSource
7	Criteo	19	Mintegral
8	Facebook Ads	20	OneSignal
9	Facebook Analytics	21	Unity3d Ads
10	Facebook Login	22	Vungle
11	Facebook Share		
12	Fyber		

Google Play'de 11 uygulamanın veri güvenliği sayfasına girildiğinde *"üçüncü taraflarla veri paylaşımı yok"* beyanı yer almaktadır (bkz: Grafik 1).



Grafik-1: Uygulamaların veri güvenliği sayfasındaki veri paylaşımı yok ifadesinin görüntüsü

Oysaki söz konusu uygulamalarda en az 2 (e-nabız uygulaması) en çok ise 14 (Sağlık Kiti ve Nabız Monitörü ve İzleyici uygulamaları) üçüncü taraf izleyici yer almaktadır. Örneğin, Nabız Monitörü ve İzleyici uygulamasındaki üçüncü taraflar Tablo 7'de gösterilmektedir.

Tablo-7: Nabız Monitörü ve İzleyici uygulamasındaki üçüncü taraf izleyicilerin listesi

1	Amazon Ads	9	Google AdMob
2	AppLovin	10	Google CrashLytics
3	AppsFlyer	11	Google Firebase Analytics
4	Facebook Ads	12	IAB Open Measurement
5	Facebook Analytics	13	Mintegral
6	Facebook Login	14	Pangle
7	Facebook Share		
8	Flurry		

Nabız Monitörü ve İzleyici adlı mobil uygulama aracılığıyla bu izleyiciler cihaz bilgisi, uygulamada geçirilen süre, etkileşimler, konum ve tahmini demografik bilgiler gibi kullanıcı verilerini toplayabilmektedir. Uygulamanın bir sağlık uygulaması olduğu dikkate alındığında ise uygulamanın sunduğu hizmet bağlamında arşivlediği nabız gibi temel sağlık verileri de takip edilebilmektedir. Aynı üçüncü tarafların aynı kullanıcıları farklı mobil uygulamalarda da izlediği düşünüldüğünde, örneğin hem nabız hem de adım sayar uygulamasında, her iki kaynaktan topladığı veriler ile yeni veri setleri üretilmesi de kaçınılmazdır.

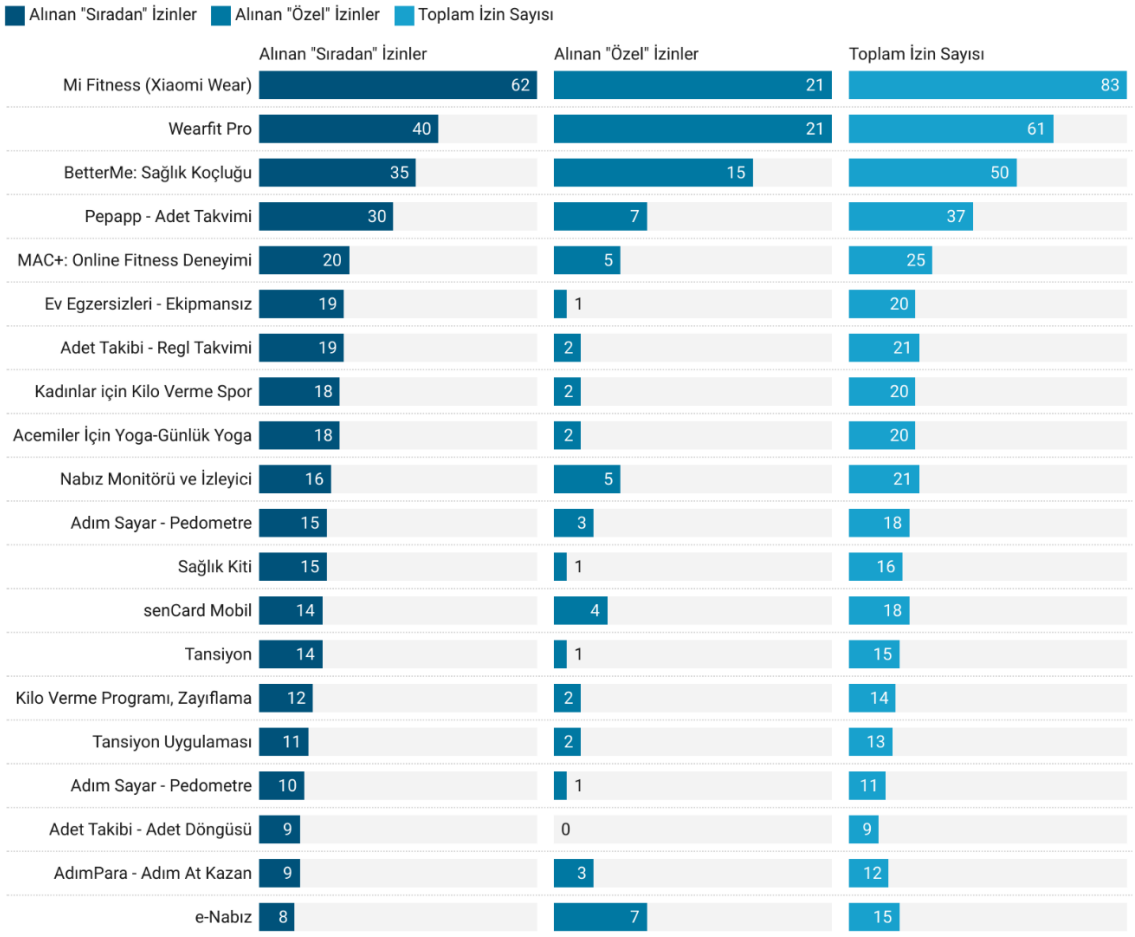
Cihazdan Alınan İzinler

Mobil uygulamalar, sundukları hizmetlerin doğru çalışması için yüklendikleri mobil cihazlardan çeşitli izinler istemektedir. Örneğin, bir fotoğraf uygulaması cihazın kamerasını; ses uygulaması cihazın mikrofonunu, harita uygulaması cihazın konumunu kullanmak için ilgili cihazdan izin istemektedir. Genel olarak izinler aşağıdaki gibi sıralanmaktadır;

- Cihaz modeli,
- İşletim sistemi,
- Cihaz kimliği (IMEI),
- Depolama
- Batarya durumu,
- Yaklaşık konum,
- Tam konum,
- Konum geçmişi,
- Fotoğraf çekme,
- Video çekme,
- Ses kaydı (Mikrofon),
- Dosyalara erişim,
- Dosya silme,
- Dosya oluşturma,
- Arama yapma,
- Bildirim gönderme,
- Hareket sensörü,
- Yakınlık sensörü,
- Bluetooth kullanımı,
- Rehber listesi,
- Rehber bilgileri,
- Takvim,
- SMS mesajları,
- WI-FI bağlantıları.

Tablo 8'de araştırmada kapsamında çözümlenen mobil uygulamaların cihazlardan talep ettiği izinlere yer verilmiştir. Tabloda her bir uygulamanın toplam aldığı izin sayısıyla birlikte bu izinlerin kaçının özel/tehlikeli kategorisinde olduğu paylaşılmaktadır. 83 izinle en çok izni Mi Fitness (Xiaomi Wear) uygulaması istemektedir.

Tablo-8: Mobil uygulamaların kullanıcı mobil cihazlarından istediği izinler



Güvenlik seviyesi özel veya tehlikeli olarak tanımlanan izinler[1], kişisel veriler ile doğrudan ilişkili olabilen hassas izinler olarak ifade edilmektedir. Kamera, konum, SMS mesajları, IP adresi ve cihaz kimliği gibi izinler bu kategori altında değerlendirilir. Mi Fitness (Xiaomi Wear) ve Wearfit Pro'nun cihazdan istediği izinlerin %25'inden fazlasının hassas olduğu görülmektedir.

Araştırmadaki mobil uygulamaların Android işletim sisteminden en çok erişmek istediği hassas izinler ve genel tanımlamaları aşağıda listelenmektedir:

- GET_ACCOUNTS: Cihazdaki hesapların listesine erişim sağlar.
- READ_CONTACTS: Rehbere erişim sağlar.
- READ_EXTERNAL_STORAGE: Harici depolama alanına erişim izin verir.
- WRITE_EXTERNAL_STORAGE: Harici depolama alanındaki dosyaları düzenleme ve silme izni verir.
- READ_PHONE_STATE: Hücresel ağ bilgileri ve arama/aranma bilgileri de dahil olmak üzere cihazın kimlik bilgisine erişim sağlar. Bu bilgi içerisinde cihazın

[1]https://developer.android.com/guide/topics/permissions/overview?hl=tr, Erişim Tarihi: 6 Haziran 2024.

bağlı olduğu telefon numarası ve mobil cihaz kimliği de yer alır. (Bkz: Pepapp ve BetterMe)

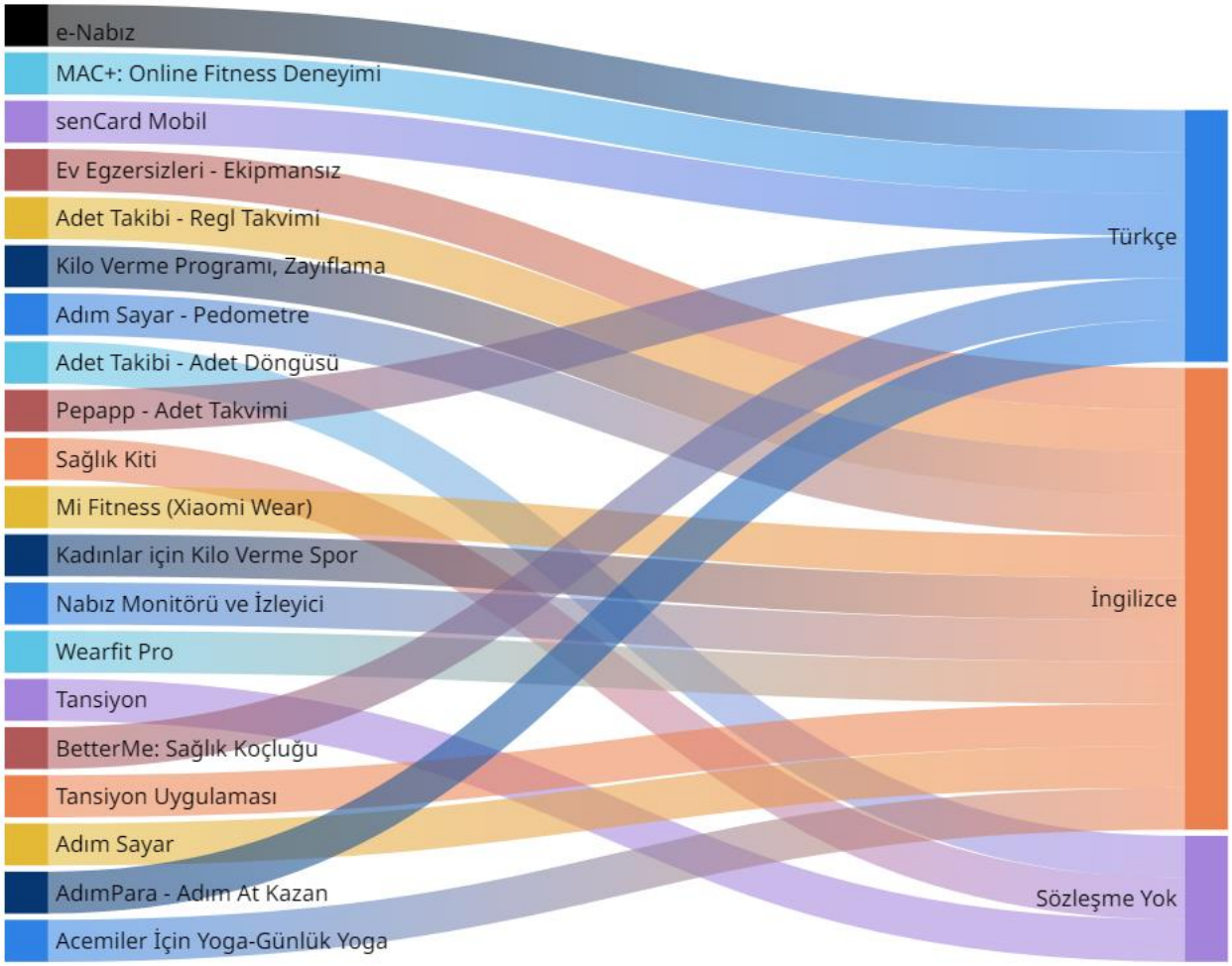
- ACCESS_COARSE_LOCATION: Bir uygulamanın yaklaşık konuma erişmesine izin verir.
- ACCESS_FINE_LOCATION: Bir uygulamanın kesin konuma erişmesine izin verir.
- ACCESS_MEDIA_LOCATION: Bir uygulamanın, kullanıcının paylaşılan koleksiyonunda kalıcı olarak bulunan tüm coğrafi konumlara erişmesine izin verir.
- ANSWER_PHONE_CALLS: Uygulamanın gelen bir telefon aramasını yanıtlamasını sağlar.
- CALL_PHONE: Bir uygulamanın, kullanıcının aramayı onaylaması için Dialer kullanıcı arayüzünden geçmeden bir telefon araması başlatmasına izin verir.
- ACTIVITY_RECOGNITION: Bir uygulamanın fiziksel aktiviteyi tanımasını sağlar.

Mobil uygulamaların sundukları hizmetlerle ilişkili olarak izin talep etmesi beklenmektedir. Fakat konum bilgisine ihtiyaç duymayan ve bununla ilgili hizmet sunmayan bir uygulama, konum bilgisini kendi çıkarı doğrultusunda isteyebilmektedir. Cihazdaki konum bilgisi kapalı olsa bile *ACCESS_FINE_LOCATION* izni ile cihazın konumu uydu sinyallerinden, wi-fi ağlarından veya hücresel ağ üzerinden tespit edilebilmektedir.

Gizlilik Sözleşmeleri

Araştırma kapsamındaki mobil uygulamaların yerli veya yabancı fark etmeksizin hepsi Türkçe dil desteğine sahiptir. Fakat Google Play Store'da uygulamaların gizlilik sözleşmelerine bakıldığında bunların 10 tanesinin İngilizce, 7 tanesinin Türkçe dilinde olduğu görülmektedir. 3 uygulamada ise gizlilik sözleşmesi yer almamaktadır (Bkz: Tablo 9).

Tablo-9: Mobil uygulamaların gizlilik sözleşmelerinin dili



Google Play'de sözleşmesi olmayan uygulamalar Adet Takibi - Adet Döngüsü (3 izleyici, 9 izin), Sağlık Kiti (14 izleyici, 16 izin) ve Tansiyon (9 izleyici, 15 izin) uygulamalarıdır.

Türkçe olan mobil uygulamaların yarısının İngilizce gizlilik sözleşmesine sahip olduğu tespit edilmiştir. Bu durum, Hidaka ve arkadaşlarının (2023) *dilsel çıkmaz* kavramıyla tanımladığı etik sorunun Türkiye'de de geçerli olduğunu göstermektedir. Sözleşmelerin İngilizce bırakılması şeffaflık ve eşitlik bakımından temel hak ihlali oluşturabildiği gibi kullanıcıları bilgilendirme yükümlüğünü yerine getirmemesiyle de büyük bir eksiklik oluşturmaktadır.

Araştırma kapsamında üçüncü taraf izleyicilerin varlığı ile cihazdan alınan izinlerin şeffaf şekilde bilgilendirilmesi temel bir mahremiyet hakkı olarak değerlendirilmektedir. Bu bağlamda sözleşmelerde hangi üçüncü taraf izleyicilerin olduğu ve ne amaçla bulunduğunun yer alması ve cihazdan hangi izinlerin talep edildiğinin paylaşılması gerekmektedir. Türkçe gizlilik sözleşmeleri çözümlendiğinde söz konusu şeffaflık kriterlerinde eksiklik olduğu gözlemlenmiştir (Bkz: Tablo 10).

Tablo-10: Türkçe gizlilik sözleşmelerindeki şeffaflık durumu

	Bağlantı	**Üçüncü Taraf İzleyici Bilgilendirmesi**	**Cihazdan Alınan İzin Bilgilendirmesi**
e-Nabız	https://web.archive.org/web/20240808101408 /https://enabiz.gov.tr/Gizlilik.html	Yok	Yok
MAC+: Online Fitness Deneyimi	https://web.archive.org/web/20240808102045/ https://www.macfit.com/kisisel-verilerin-korunmasi	Kısmen	Yok
senCard Mobil	https://web.archive.org/web/20240808102230/ https://www.sencard.com.tr/gizlilik-politikasi	Yok	Yok
Peppap – Adet Takvimi	https://web.archive.org/web/20240808082551/ https://www.letspepapp.com/hukum_ve_kosullar	Yok	Yok
Mi Fitness (Xiaomi Wear)	https://web.archive.org/web/20240808102739/ https://watch.iot.mi.com/html/privacy/ index.html?locale=tr_TR&type =watch_privacy_policy&model=app	Kısmen	Var
BetterMe: Sağlık Koçluğu	https://web.archive.org/web/20240808103020/ https://betterme.world/privacy-policy	Var	Var
AdımPara - Adım At Kazan	https://web.archive.org/web/20240808103415/ https://www.adimpara.com/kvkk	Yok	Kısmen

Tablo 10'da yer alan verilerde üçüncü taraf izleyici bilgilendirmesin "Yok" olarak ifade edilenler, araştırma kapsamında tespit edilen üçüncü taraf izleyicilerin hiçbirinin gizlilik sözleşmesinde yer almadığını belirtmektedir. "Kısmen", izleyicilerin bir kısmının yer aldığını; "Var" ise izleyicilerin tamamının sözleşmede bulunduğunu açıklamaktadır. Aynı şekilde, cihazdan alınan izin bilgilendirmesinde "Yok" olarak ifade edilenler, araştırma kapsamında tespit edilen cihaz izinlerinin hiçbirinin gizlilik sözleşmesinde yer almadığını, "kısmen" olanlar bir kısmının yer aldığını, "Var" ise hepsinin sözleşmede bulunduğunu göstermektedir.

En çok üçüncü taraf izleyicisi olan yerli uygulama Pepapp – Adet Takvimi'nin Türkçe[2] gizlilik sözleşmesinde Amsterdam; İngilizce[3] sözleşmesinde İstanbul adres olarak gösterilmiştir. Sözleşmenin İngilizcesinde üçüncü taraf izleyiciler ve kullanıcı verilerinin toplanmasıyla ilgili oldukça detaylı bilgilerin paylaşıldığı, Türkçesinde ise daha yüzeysel bilgilerin yer aldığı görülmektedir. Tablo 6'da bulunan Pepapp'a ait üçüncü taraf izleyicilerin hiçbiri Türkçe gizlilik sözleşmesinde yer almamaktadır. Bu izleyicileri

[2]https://web.archive.org/web/20240808082551/https://www.letspepapp.com/hukum_ve_kosullar/, Erişim Tarihi: 8 Ağustos 2024.
[3]https://web.archive.org/web/20240808081416/https://letspepapp.com/terms_and_conditions/privacycommitment.html, Erişim Tarihi: 8 Ağustos 2024.

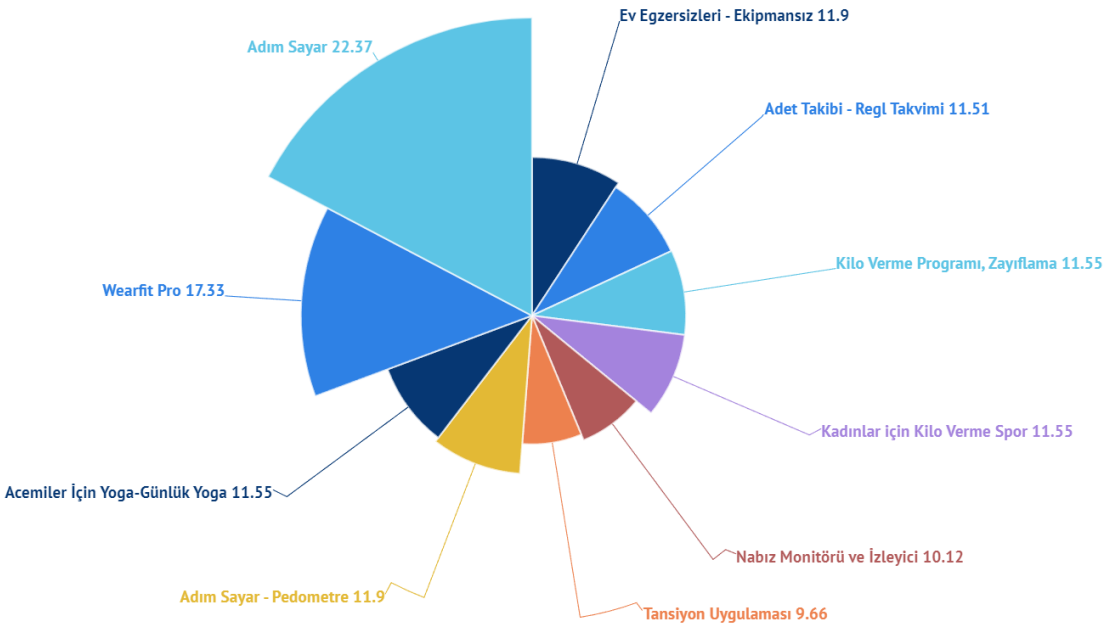
uygulamanın iş ortakları olarak değerlendirirsek sözleşmedeki şu ifade sürecin bilinmezliği hakkında fikir vermektedir:

> *Pepapp, Uygulama kullanımı sırasında Kullanıcı'nın izlediği, ziyaretçi hareket ve tercihlerini analiz ederek yorumlamaktadır. Kişisel bilgiler içermeyen bu istatistiksel veriler, Pepapp Kullanıcılarına daha özel bir deneyim yaşatmak amacıyla Pepapp iş ortakları ile paylaşılabilecektir.*

Sözleşmede üçüncü taraf izleyiciler ile analiz edilen ve yorumlanan veriler, yine onlarla veya başkalarıyla paylaşıldığı belirtilmektedir. Diğer bir deyişle, kişisel veri olmadığı iddia edilen kullanıcıların kendi verileri, "iş ortakları" adı verilen bilinmeyen grup ve kuruluşlara iletilmektedir.

Uygulamaları kullanan kullanıcıların İngilizce bilme ve okuma zorunlulukları olduğu söylenemez. Fakat, İngilizce sözleşmelerin dil yapısı ve zorluğunun ölçülmesi uygulamaların sıradan bir kullanıcının nasıl bir metinle karşılaştığını anlamak için değerlidir. Bu nedenle araştırma kapsamında ortaya çıkan İngilizce dilindeki gizlilik sözleşmelerine Otomatik Okunabilirlik Testi (ARI) uygulanmıştır. Tablo 11'de görüleceği üzere metin dili en zor ve karmaşık olan gizlilik sözleşmesi Adım Sayar[4] uygulamasıdır.

Tablo-11: İngilizce dilindeki gizlilik sözleşmelerinin otomatik okunabilirlik endeksine göre zorluk dereceleri



ARI'ye göre Adım Sayar uygulamasının okuma zorluğu son derece zor, sınıf derecesi üniversite mezunu ve yaş aralığı 23 ve üzeridir. İkinci anlaşılması zor uygulama 17.33 ile Weaferfit Pro olurken diğer uygulamaların da ortalama lise mezunu veya

[4]https://web.archive.org/web/20240808111025/https://www.ito-technologies.com/en/pedometer/privacy/, Erişim Tarihi: 8 Ağustos 2024.

üniversite öğrencisi seviyesindeki kişilerin anlayabileceği seviyede olduğu görülmektedir. Buna göre Türkçesi olmayan sözleşmelerin İngilizcesinin, ana dili İngilizce olan kişiler için bile zor olduğu söylenebilir.

Tartışma ve Sonuç

Mobil sağlık uygulamaları, kullanıcıların sağlık durumlarını takip etmek, yönetmek ve sağlık farkındalığı bakımından kıymetli hizmetler sunmaktadır. Uygulamaların çalışma prensibi kullanıcıdan çeşitli sağlık verilerini toplayarak bu hassas verileri analiz etmesi ve yorumlamasını içermektedir. Bu verilerin toplanma ve işlenme süreçleri, özellikle hassas olmaları sebebiyle, beraberinde olası mahremiyet sorunlarını da getirmektedir.

Yapılan araştırmalarda mobil uygulamalardaki mahremiyet ihlallerinin sıklıkla açık rıza alınmadan üçüncü taraf izleyicilerin aktif hâle gelmesi (Paci vd., 2023), gizlilik sözleşmeleri ziyaret edildiği anda üçüncü taraflarla veri paylaşımına başlanıyor olunması (Kollnig, 2021), gizlilik politikalarının çoğunda eksik ve yanıltıcı içeriklerin yer alması (Yu vd., 2021) ve uygulamaların kullanıcılara neler yapabileceği konusunda tatmin edici kontroller sağlamaması (Kern ve Sametinger, 2012) gibi durumlarla gerçekleştiğin göstermektedir. Mobil uygulamalardaki izleyiciler üzerine yapılan benzer çalışmalarda ise uygulamaların %90'ından fazlasının en az bir üçüncü taraf izleyici içerdiği (Binns vd., 2018; Kollnig vd., 2021; Qayyum vd., 2022), izleyicilerin büyük çoğunluğunun Google ve Meta gibi ABD merkezli şirketler olduğu (Binns vd., 2018; Razaghpanah vd., 2018) ve yasal mevzuatların sıkılığına rağmen çoğu uygulamanın hâlen geçerli rıza koşullarını sağlamadığı (Kollnig vd., 2021) tespit edilmiştir.

Sağlık verilerinin öneminin ve başka gruplar tarafından başka amaçlar doğrultusunda kullanımının bireyin mahremiyetine nasıl zarar vereceğinin birçok kez vurgulandığı bu çalışmada, mobil sağlık uygulamalarındaki üçüncü taraf izleyiciler, cihazdan alınan izinler ve gizlilik sözleşmelerinde bu durumların nasıl ele alındığı irdelenmiştir.

Araştırmada taranan, Türkiye'deki 20 en popüler Sağlık ve Fitness uygulamasının 15'inin yabancı firmalara, 5'inin yerli firmalara ait olduğuna ulaşılmıştır. Uygulamaların hepsinde üçüncü taraf izleyici veya yazılım geliştirme kitine ait bulgulara rastlanmıştır. En çok izleyiciye sahip uygulamanın 22 izleyici ile yerli bir kadın sağlığı uygulaması olan Pepapp - Adet Takvimi olduğu görülmüştür. En az izleyiciye sahip ise Sağlık Bakanlığına ait e-Nabız uygulaması olmuştur.

20 sağlık uygulamasında toplam 153 adet üçüncü taraf izleyiciye ulaşılmıştır. Google'a ait Firebase Analytics (Analitik) tüm uygulamalarda yer alırken, CrashLytics (Analitik) 19 uygulamada, AdMob (Reklam) ise 16 uygulamada bulunmaktadır. Bir diğer silikon vadisinin büyük şirketi Meta'ya ait Facebook Ads (Reklam) uygulamaların yarısında, Facebook Login (Kimlik) 7'sinde, Facebook Share (Sosyal Medya Entegrasyonu) ise 6'sında yer almaktadır. Geri kalan en popüler üçüncü taraflar IAB Open Measurement (Reklam) 8 uygulamada, AppLovin (Reklam) 6 uygulamada ve Pangle (Reklam) 5 uygulamada saptanmıştır. e-Nabız ve Mi Fitness (Xiaomi Wear) haricindeki bütün mobil uygulamalarda reklam kategorisindeki üçüncü taraf izleyicilere rastlanmıştır.

Mobil uygulamaların cihazlardan aldığı en çok izin 83 izinle Mi Fitness (Xiaomi Wear) olurken, en az izni 9 izinle Adet Takibi - Adet Döngüsü adlı kadın sağlığı uygulaması talep etmiştir. Google'ın tehlikeli olarak işaretlediği özel izinler ele alındığında yine en çok özel izni 21'er izin ile Mi Fitness (Xiaomi Wear) ile Wearfit Pro uygulamaları istemiştir. Özel izinler arasında cihazın kimlik numarasına erişme, telefon numarasını öğrenme, depolama alanlarına erişim, rehberi görüntüleme, gelen ve giden aramaları yönetme, yaklaşık ve kesin konumu görüntüleme ve fiziksel aktiviteleri tanımlamaları yer almaktadır.

20 mobil sağlık uygulamasının Google Play mağazası içindeki sayfaları görüntülendiğinde 3 uygulamada gizlilik sözleşmesinin olmadığı belirlenmiştir. Bunlar Tansiyon (9 izleyici, 15 izin), Sağlık Kiti (14 izleyici, 16 izin) ve Adet Takibi - Adet Döngüsü (3 İzleyici, 9 İzin) adlı uygulamalardır. Geri kalan 17 gizlilik sözleşmesinin ise yalnızca 7 tanesi Türkçedir. Geri kalan sözleşmeler için sağlanan bağlantıların hepsi İngilizce metinlere gitmektedir. Dolayısıyla en popüler 20 mobil sağlık uygulamasının hepsinde Türkçe desteği olmasına rağmen yarısının gizlilik sözleşmesinin İngilizce olduğu ve bu yönüyle yasal ve etik sorunlar yarattıklarını söylemek mümkündür.

İngilizce gizlilik sözleşmelerinin metinleri otomatik okunabilirlik endeksine göre çözümlendiğinde, metinlerin ortalama anlaşılma seviyesi lise mezunu veya üniversite öğrencisi düzeyinde olduğuna ulaşılmıştır. Gizlilik sözleşmelerini okuyan çoğu kullanıcının içeriği anlamada zorluk yaşadığı düşünüldüğünde (Ibdah vd., 2021), bu metinlerin daha sade, anlaşılır ve şeffaf olması gerekmektedir.

Türkçe gizlilik sözleşmeleri üçüncü taraf izleyicilerin kimler olduğu ve cihazdan hangi izinler alındığı çerçevesinde çözümlenmiştir. Her bir uygulama için araştırmada tespit edilen üçüncü taraf izleyicilerin tam listesinin yalnızca BetterMe: Sağlık Koçluğu uygulamasının sözleşmesinde yer aldığı saptanmıştır. Mi Fitness (Xiamoi Wear) ve Mac+: Online Fitness Deneyimi uygulamalarının sözleşmelerinde tespit edilen izleyicilerin bir kısmı yer alırken; e-Nabız, senCard Mobil, Peppap ve AdımPara uygulamalarında izleyicilerin listesi yer almamaktadır. Cihazdan alınan izinlerin şeffaf şekilde paylaşıldığı sözleşmeler ise yine Better Me: Sağlık Koçluğu ve Mi Fitness (Xiaomi Wear) olmuştur. AdımPara uygulamasında izinler kısmen yer alırken; e-Nabız, MAC+, senCard Mobil ve Peppap uygulamalarında yer almamaktadır. Genel bir değerlendirme yapıldığında, yabancı menşeili uygulamalardan Türkçe sözleşmesi olanların izleyiciler ve izinler konusunda şeffaf bilgilendirme yaptıkları söylenebilmektedir. Yerli uygulamaların Türkçe sözleşmeleri ise bilgilendirme konusunda eksiktir.

Mahremiyet, konu sağlık verileri olduğunda daha da önemli bir hâle gelir. Fiziksel ve zihinsel tüm sağlık verileri son derece hassas verilerdir. Bu verilerin toplandığı, üretildiği, saklandığı ve paylaşıldığı mobil uygulamalar sistemlerini açık rızaya dayalı, anlaşılır ve şeffaf şekilde inşa etmelidir. Yazılımlar, tüketicisi olacak kullanıcıları merkeze alarak geliştirilmelidir. Kullanıcı merkezli yaklaşım, ürün veya hizmetin kullanıcının beklenti ve ihtiyaçlarını önceleyerek geliştirilmesini sağlamaktır. Yaklaşımın amacı, sistemin kullanıcılar tarafından daha etkin kullanılması ve ihtiyaçlarını onlar farkında olmadan karşılamasıdır. Kullanıcı mahremiyeti bağlamında ele alındığında yaklaşım, sistemlerin etik standartlara uyumlu olmasına ve mahremiyet endişelerine odaklanır.

Kullanıcıları merkeze alarak geliştirilen ürün ve hizmetler veri gizliliğine ilişkin herhangi bir endişe barındırmamalıdır, veri güvenliğini sağlamalıdır, gizlilik sözleşmeleri şeffaf ve anlaşılır olmalıdır, kullanıcıyı aldatacak girişimlere önayak olmamalıdır, kullanıcının sağladığı ve kullanıcıdan gözlemlenen veriler kullanım amacıyla sınırlı ve açık rızaya dayalı olarak toplanmalı ve saklanmalıdır. Geliştirilecek uygulamalarda mahremiyetin varsayılan bir özellik olarak yer alması özel yaşama ve bireysel özgürlüklere saygı için gereklidir. Bununla birlikte toplumsal güven, eşitlik ve adaletin gelişimine de katkı sağlayacaktır. Gelecek çalışmalarda mobil uygulamaların veri toplama süreçlerinin yasal mevzuatlara uyumluluğunu araştırma, başta sağlık olmak üzere farklı türdeki hassas verilerin toplanmasının sosyal etkilerini inceleme ve uygulama sahiplerinin veya geliştiricilerin veri toplama süreçlerine yönelik düşünce ve yaklaşımlarını ortaya çıkartma alana dair yeni perspektiflerin oluşmasına destek olacaktır.

Etik Beyanı: Yazar çalışmanın, etik kurul izni gerektirmeyen çalışmalar arasında yer aldığını beyan eder. Aksi bir durumun tespiti halinde Kastamonu İletişim Araştırmaları Dergisi'nin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarına aittir.

Yazar Katkıları: Yazarın katkı oranı %100'dür.

Çıkar Çatışması Beyanı: Yazar, herhangi bir çıkar çatışması olmadığını beyan etmektedir.

Kaynakça

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Lukács, A. (2016). What is privacy? The history and definition of privacy. (Yayımlanmamış çalışma). https://api.semanticscholar.org/CorpusID:190478776

Berelson, B. (1952). *Content analysis in communication research*. Free Press.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third-party tracking in the mobile ecosystem. H. Akkermans & K. Fontaine (Ed.), *Proceedings of the 10th ACM Conference on Web Science* içinde (s. 23–31). Association for Computing Machinery. https://doi.org/10.1145/3201064.3201089

Bloustein, E. J. (1964). *Privacy as an aspect of human dignity: An answer to Dean Prosser*. New York University, School of Law.

Ceci, L. (2024, 19 Ocak). Google Play Store: Number of apps 2023. *Statista*. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store

DeBrabander, F. (2020). *Life after privacy: Reclaiming democracy in a surveillance society.* Cambridge University Press.

Dolgun, U. (2015). *Şeffaf hapishane yahut gözetim toplumu* (3. bs). Ötüken Neşriyat.

Fry, H. (2019). *Merhaba dünya* (İ. Çıgay Güneş, Çev.). Hep Kitap.

Hartmann, T. (2022). *The hidden history of Big Brother in America: How the death of privacy and the rise of surveillance threaten us and our democracy*. Berrett-Koehler Publishers.

Hern, A. (2018, 28 Ocak). Fitness tracking app Strava gives away the location of secret US Army bases. *The Guardian*. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases 4o

Hidaka, S., Kobuki, S., Watanabe, M., & Seaborn, K. (2023). Linguistic dead-ends and alphabet soup: Finding dark patterns in Japanese apps. A. Schmidt, K. Väänänen, T. Goyal, P. O. Kristensson, A. Peters, S. Mueller, J. R. Williamson & M. L. Wilson (Ed.), *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* içinde (s. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3544548.3580942

Ibdah, D., Lachtar, N., Raparthi, S. M., & Bacha, A. (2021). "Why should I read the privacy policy, I just need the service": A study on attitudes and perceptions toward privacy policies. *IEEE Access, 9,* 166465–166487. https://doi.org/10.1109/ACCESS.2021.3130086

Iqbal, M. (2024, 24 Ocak). App download data (2024). *Business of Apps.* https://www.businessofapps.com/data/app-statistics/

Keegan, J., & Eastwood, J. (2023, 8 Haziran). From "heavy purchasers" of pregnancy tests to the depression-prone: We found 650,000 ways advertisers label you. *The Markup*. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you

Kern, M., & Sametinger, J. (2012). Permission tracking in Android. J. L. Mauri & P. Lorenz (Ed.), *Proceedings of UBICOMM 2012 – The 6th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies* içinde (s. 148-155). IARIA. https://doi.org/10.13140/RG.2.1.4353.5764

Kim, J. (2023). Data brokers and the sale of Americans' mental health data. *Duke University, Sanford School of Public Policy.* https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-americans-mental-health-data/

Knight, T. (2021). Data ownership: Legalities concerning wearable technologies. D. Sen & R. Ahmed (Ed.), *Privacy concerns surrounding personal information sharing on health and fitness mobile apps* içinde (s. 60–82). IGI Global.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kollnig, K. (2021). *Tracking in apps' privacy policies.* arXiv. https://doi.org/10.48550/arXiv.2111.07860

Kollnig, K., Binns, R., Van Kleek, M., Zhao, J., Lyngs, U., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review, 10*(4). https://doi.org/10.14763/2021.4.1611

Lauer, J. (2012). Surveillance history and the history of new media: An evidential paradigm. *New Media & Society, 14*(4), 566–582. https://doi.org/10.1177/1461444811420986

Lokke, E. (2018). *Mahremiyet: Dijital toplumda özel hayat* (D. Başak, Çev.). Koç Üniversitesi Yayınları.

Lynch, M. P. (2016). *The internet of us: Knowing more and understanding less in the age of big data.* W. W. Norton & Company.

Metzger, M. J., Suh, J. J., Reid, S., & Abbadi, A. E. (2021). What can fitness apps teach us about group privacy? D. Sen & R. Ahmed (Ed.), *Privacy concerns surrounding personal information sharing on health and fitness mobile apps* içinde (s. 1–30). IGI Global.

Neuman, W. L. (2014). *Toplumsal araştırma yöntemleri* (S. Özge, Çev.; 7. bs., Cilt 1). Yayınodası Yayıncılık.

Paci, F., Pizzoli, J., & Zannone, N. (2023). A comprehensive study on third-party user tracking in mobile applications. *Proceedings of the 18th International Conference on Availability, Reliability and Security* içinde (s. 1–8). Association for Computing Machinery. https://doi.org/10.1145/3600160.3605079

Privacy International. (2019). Your mental health for sale: How websites about depression share data with advertisers and leak depression test results. https://privacyinternational.org/campaigns/your-mental-health-sale

Qayyum, H., Salman, M., Sentana, I. W. B., Nguyen, D. L. G., Ikram, M., Tyson, G., & Kaafar, M. A. (2022). A first look at Android apps' third-party resources loading. X. Yuan, G. Bai, C. Alcaraz & S. Majumdar (Ed.), *Network and system security: NSS 2022. Lecture notes in computer science* içinde (s. 193–203). Springer. https://doi.org/10.1007/978-3-031-23020-2_11

Raymond, E. (2001). *The cathedral & the bazaar: Musings on Linux and open source by an accidental revolutionary*. O'Reilly Media.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018* içinde (s. 1–15). DBLP. http://dx.doi.org/10.14722/ndss.2018.23353

Robb, D. (2017, 1 Kasım). Building the global heatmap. *Strava Engineering*. https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de

Ruser, N. [@nrg8000]. (2018, 27 Ocak). Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option)… [Tweet]. X. https://x.com/nrg8000/status/957318498102865920

Sathyanarayana, A., Joty, S., Fernandez-Luque, L., Ofli, F., Srivastava, J., Elmagarmid, A., Arora, T., & Taheri, S. (2016). Sleep quality prediction from wearable data using deep learning. *JMIR mHealth and uHealth, 4*(4), e125. https://doi.org/10.2196/mhealth.6562

Schechner, S., & Secada, M. (2019, 22 Şubat). You give apps sensitive personal information. Then they tell Facebook. *The Wall Street Journal.* https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

Sherwani, S. I., & Bates, B. R. (2021). Role of wearable technology and fitness apps in obesity and diabetes: Privacy, ownership, and portability of data. D. Sen & R. Ahmed (Ed.)*, Privacy concerns surrounding personal information sharing on health and fitness mobile apps* içinde (s. 31–59). IGI Global.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087–1155. https://doi.org/10.2307/3481326

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security.* Yale University Press.

Statista. (2024). *App—worldwide | statista market forecast*. https://www.statista.com/outlook/amo/app/worldwide

Stevens, R., Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012). Investigating user privacy in Android ad libraries. *Proceedings of the 1st Workshop on Mobile Security Technologies (MoST 2012)* içinde (s. 195–197). IEEE Computer Society. https://www.cs.ucdavis.edu/~hchen/paper/most2012ad.pdf

Strömholm, S. (1967). *Right of privacy and rights of the personality: A comparative study.* P.A. Norstedt & Söners Förlag.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220. https://doi.org/10.2307/1321160

Yu, L., Luo, X., Chen, J., Zhou, H., Zhang, T., Chang, H., & Leung, H. K. N. (2021). PPChecker: Towards accessing the trustworthiness of Android apps' privacy policies. *IEEE Transactions on Software Engineering*, *47*(2), 221–242. https://doi.org/10.1109/TSE.2018.2886875

Zippia. (2023, 20 Mart). 40 fascinating mobile app industry statistics [2023]: The success of mobile apps in the U.S. https://www.zippia.com/advice/mobile-app-industry-statistics

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.