

# COVID-19 DİJİTAL KİŞİ İZLEME UYGULAMALARINDA MAHREMİYET

## PRIVACY IN COVID-19 DIGITAL CONTACT TRACING APPLICATIONS

**Gizem GÜRSON DOLAR\***  
**Esma ERGÜNER ÖZKOÇ\*\***

### Öz

COVID-19 süresince, temas takibi ve gözetimi için mobil uygulamaların kullanılması, hükümetlerin virüsün nasıl yayıldığı ve toplulukları nasıl etkilediği konusundaki bilgileri elde etmelerine, bu etkileri azaltmak için önlemleri daha hızlı uygulamaya koymalarına önemli ölçüde yardımcı olmuştur. Fakat bu uygulamalar aracılığıyla kişilerin tanımlanmasına sebep olan hassas veriler toplanıp işlenmektedir. Mahremiyet koruyucu önlemlerin, veri ihlallerinin kişilere, kurumlara ve ülkelere verdiği zararların azaltılması amacıyla alınması gerekmektedir.

Bu çalışmada, dünya genelinde COVID-19 süresince resmi kurumlar tarafından geliştirilmiş 72 temas takibi ve gözetimi mobil uygulaması incelenmiş, uygulamaların mahremiyet öncelikli olma durumları, kullandıkları sunucu mimarisinin dağıtık veya merkezi olması durumuna göre değerlendirilmiştir. Veri mahremiyetine verilmesi gereken önceliklendirmenin ilgili kurumlar tarafından şeffaf bir şekilde ele alınmadığı sonucuna varılmıştır. Son olarak uygulama geliştiricilerin, veri sahiplerinin mahremiyeti ile veri paylaşımının taraflara sağlayacağı fayda arasındaki dengeyi bulabilmesi için önerilerde bulunulmuştur.

**Anahtar Kelimeler:** Dijital Kişi İzleme Teknolojileri, COVID-19 Mobil Uygulama, Veri Mahremiyeti.

### Abstract

During COVID-19, the use of mobile apps for contact tracing and surveillance is essential in helping governments gain knowledge of how the virus spreads and how it affects communities, and then more quickly implement measures to mitigate those impacts. However, through these applications, it collects and processes sensitive data that causes the identification of individuals. Privacy protection measures should be taken in order to reduce the damage caused by data breaches to individuals, institutions and countries.

\* Arş. Gör., Başkent Üniversitesi Ticari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü, nggdolar@baskent.edu.tr

\*\* Dr.Öğr.Üyesi, Başkent Üniversitesi Ticari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü, eozkoc@baskent.edu.tr

In this study, 72 contact tracing and surveillance mobile applications developed by official institutions throughout the world during the COVID-19 period were examined, and the privacy priority status of the examined applications was evaluated according to whether the server architecture they used was distributed or centralized. It has been concluded that the prioritization that should be given to data privacy is not handled transparently by the relevant institutions. Finally, suggestions have been made for application developers to find the balance between the privacy of data owners and the benefits that data sharing will provide to the parties.

**Keywords:** Digital Contact Tracing Technologies, COVID-19 Mobile app., Data Privacy.

## 1. GİRİŞ

Geçmişte birçok salgın hastalık yaşanmış olsa da COVID-19 bilgi çağının ilk salgın hastalığı olarak karşımıza çıkmaktadır. Salgının ilk günlerinden itibaren Dünya Sağlık Örgütü (WHO), pandemiye ilişkin küresel mücadeleyi yönlendirmek ve koordine etmek amacıyla istatistiki verileri anlık olarak dijital ortamda tüm dünya ile paylaşmıştır (WHO, 2021).

Pandemi süresince, vatandaşlar pandeminin ilerlemesini anlamaya çalışırken, çeşitli kuruluşlarda çalışan veri bilimcileri enfeksiyon, test ve ölüm rakamlarını derleme, doğrulama ve bunları etkili veri görselleştirmeleriyle çevrimiçi olarak halka erişilebilir hale getirme çabalarına öncülük etmiştir (FT Visual & Data Journalism Team, 2021).

Bu süreçte web ve mobil tabanlı birçok uygulama geliştirilmiştir. Özellikle, COVID-19 ile mücadele sürecinin ortalarında bir mobil uygulama seli ortaya çıkmıştır. Bazı mobil uygulamalar salgınla ilgili sadece istatistiki veri sağlarken bazıları bireyleri ve temas ettikleri kişileri izlemeye yöneliktir. Nisan 2020'den başlayarak tüm Dünyada, virüsün yayılmasını önlemeye yardımcı olmak için "kişi izleme (contact tracing)" mobil uygulama kategorisinin sayısında bir artış görülmüştür. Örneğin, Polonya'da karantinaya alınan hastalara yönelik bir uygulama, rastgele coğrafi konumlu özçekimler yapılmasını isterken, Rusya'daki benzer bir uygulama, Moskova'da COVID-19 olduğundan şüphelenilen vatandaşların yetkililere günde üç kez özçekim göndermelerini istemektedir. Türkiye'de ise, vatandaşları izlemek için karantina takibi yapılabilen "Hayat Eve Sığar" uygulaması kullanılmaktadır. Çin'in ilk koronavirüs vakasının bildirildiği Wuhan bölgesine giriş/çıkış yapabilmek için bir devlet gözetim mobil uygulamasının yüklenmesi zorunlu kılınmıştır. Çin hükümeti daha sonra toplanan bu verileri analiz ederek, bireyleri sağlık durumlarına ve COVID-19 risk düzeylerine göre renk kodlu kategorilere (kırmızı, sarı veya yeşil) ayırarak izlemiştir. Temmuz 2020 itibarıyla, Dünya genelinde 29 ülke için en az 47 kişi izleme uygulaması mevcuttur (Kassab & Graciano Neto, 2021).

İzleme uygulamalarının topladığı verilerin büyük ölçekli olması ve hassas doğası nedeniyle, savunmasız grupları orantısız şekilde etkileyebilecek etik kaygılar doğurmaktadır. COVID-19 süresince topluma ve devletlere fayda amacıyla toplanan ve işlenen bu veriler içerisinde kişileri tanımlayan kişisel veriler yer almaktadır. Uygulamalar, kişilerin konum, temas bilgilerinin yanında COVID-19'a eşlik eden hastalıklarını da etiketlemektedir. Bu tür tanımlayıcı verilerin toplanması ve işlenmesi veri mahremiyeti konusunda ciddi problemler doğurmakta ve kişiler, kurumlar ve hatta

ülkeler zarar görmektedir. Bu sebeple mahremiyeti koruyucu uygulamalar geliştirilmeli ve bireyler bu konuda bilinçlendirilmelidir. Burada önemli olan nokta, mahremiyet kavramının sınırlarını belirlemek ve net bir tanım sağlamaktır. Bireyler mahremiyeti “benimle ilgili bilgilerin başkalarının eline geçmesini engelleme” ifadesiyle tanımlamaktadır. Ancak COVID-19 izleme uygulamaları gibi iyi niyetli olduğu düşünülen uygulamalarda bu kişisel verilerin kullanılması söz konusu olduğunda, bireyler bu durumdan rahatsız olmaz ve mahremiyetin ihlal edildiği düşünülmez (Clifton, Kantarcioglu, & Vaidya, 2002). Burada gözden kaçan şey, bu verilerden işlenen bilgi yayınlandıktan sonra kötüye kullanımın önlenmesinin zorluğudur.

COVID-19 öncesi dönemde de dünyada bilgi gizliliğine, kişi mahremiyetine ilişkin çeşitli düzenlemeler vardı. Örneğin ABD’de “HIPAA Gizlilik kuralları”, “California Tüketici Gizliliği Yasası (CCPA)” ve Federal Anayasal Haklar kapsamında, 1977 yılında Whalen/Roe davası, 2001 yılında Ferguson/Charleston Şehri davası, 2018 yılında Carpenter/ABD davasında Yüksek Mahkemenin verdiği kararlar doğrultusunda tanınan haklar mevcuttur. Avrupa Birliği’nde ise 25 Mayıs 2018 tarihinden itibaren yürürlükte olan “Genel Veri Koruma Yönetmeliği (General Data Protection Regulation-GDPR)” nin daha etkili ve kapsamlı olduğu düşünülmekteydi. Salgınla birlikte, ABD yukarıda açıklanan güncel veri koruma planlarının, bireyleri COVID-19 dijital kişi izleme uygulamalarına katılan risklerden korumak için yetersiz olduğunu kabul etti (Oliva, 2020). Türkiye’de ise kişisel sağlık verileri ile ilgili temel düzenleme 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda yer almıştır. Türkiye’de elektronik sağlık kayıtlarının tutulması, kişisel sağlık verilerine erişim, kişisel sağlık verilerinin gizlenmesi ve düzeltilmesi, imha edilmesi ve aktarılması, kişisel sağlık verilerini bilimsel amaçlarla işleme ve açık sağlık verilerine dönüştürme, sağlık verileri ve bilgilerinin güvenliği T.C. Sağlık Bakanlığının yükümlülüğündedir. Bakanlık kişisel sağlık verileri ile ilgili yürütülen süreç ve uygulamalarda uyulacak usul ve esasları 21 Haziran 2019 tarih ve 30808 sayılı Resmî Gazete’de yayınlanan “Kişisel Sağlık Verileri Hakkında Yönetmelik” ile belirlemiştir.

COVID-19 için dijital kişi takibi henüz emekleme aşamasında olsa da, uygulanması ve vatandaşlara mahremiyetlerinin korunmasıyla ilgili güvence verilmesi konusunda fikir birliği olmamasının, söz konusu mobil uygulamaların pandemi sürecine katkıda bulunma kapasitesini engellediği ileri sürülmektedir (Fahey & Hino, 2020). Öte yandan kişi izleme uygulamaları, doğru ve yaygın COVID-19 testi olmadan etkisizdir ve kamu aktörlerinin elindeki teknoloji ve veri gücünü kötüye kullanmayacağı güvenine dayanan yaygın bir benimseme olmadan başarılı olamaz. Yakın zamanda yapılan bir çalışma, tüm akıllı telefon kullanıcılarının en az %80’inin veya genel nüfusun en az %56’sının uygulamayı kullanmasıyla COVID-19 pandemisinin kontrol edilebileceğini göstermektedir (Cohen, Gostin, & Weitzner, 2020).

Dijital kişi izleme uygulamaları, genellikle COVID-19’a maruz kalma riski yüksek; yaşlılar, düşük gelirli bireyler, yasal statü sorunları olan bireyler, kırsal kesimde yaşayanlar gibi akıllı telefona veya yeterli teknoloji kullanımına sahip olma imkânı olmayanlar dahil olmak üzere birçok grubu kapsamaz, bu nedenle, kişi izleme uygulamalarının salgında etkili olabilmesi için söz konusu grupların erişimine de açmak gerekmektedir (Oliva, 2020).

Bu sebeplerle çalışmada, COVID-19 süresince dünyanın farklı ülkelerinde geliştirilen dijital kişi takibi mobil uygulamaları, mahremiyet penceresinden incelenmiştir.

## 2. YÖNTEM

Çalışmada dünya genelinde 58 ülke tarafından geliştirilen ve vatandaşların kullanımına sunulan 72 adet COVID-19 dijital kişi takibi mobil uygulaması derlenerek; değerlendirme notu/kişi sayısı, işletim sistemi desteği, indirilme sayısı, geliştirici kurum ve kullanılan veri güvenliği protokolü açısından incelenmiştir. (İncelenen uygulama listesi ve detayları EK’te verilmiştir.)

### Veri Mahremiyeti

Kişisel veriler, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bilgilerdir. Bu kavram, verilerin bir kişiye ait olduğu ve bu kişinin de tanımlanabileceği bileşenlerden oluşmaktadır. Kişisel veriler, “ego” ya ait olan ve isimlerden tercihlere, duygu ve düşüncelere kadar geniş bir yelpazede ele alınan bir kavramdır. Kimliği belirlenebilir bir kişi, özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen kişidir. Bu nedenle bireyin bu veriler üzerindeki kontrol yetkisini kaybetmesi, bireyin özgürlüğünü, özerkliğini, mahremiyetini kısacası ben olma özelliğini kaybetmesini beraberinde getirmektedir (İzgi, 2014). Bu verilerin kişilerin mahremiyetine zarar vermeden kullanılmasını sağlamanın temel yolu kişinin kimliğinin ortadan kaldırılmasıdır.

Veri mahremiyeti, verinin yaşam döngüsü (veri toplama, verileri işleme ve analiz etme, verileri yayınlama ve paylaşma, verileri koruma, verileri yeniden kullanma) boyunca hukuka ve etik kurallara uygun olarak korunması gereken gerçek kişi, kurum ve kuruluşların (veri sahibi) korunması olarak tanımlanmaktadır (Vural, 2018).

Bu süreçte verilerin hangi amaçla işleneceği, kimlerle paylaşılacağı, nereye aktarılacağı ve şeffaf ve kontrol edilebilir düzeyde veri sahibi tarafından kontrol edilebilmesi veri mahremiyetinin önemli gereklilikleridir. Öte yandan, mahremiyetin kesin bir tanımı yoktur, uygulamaya özel tanımlama yapılabilir. Örneğin, COVID-19 kişi izleme uygulamalarında bir bireyin enfekte olarak veya yüksek riskli olarak tanımlanan bir bölgede ikamet ettiğinin kamuoyunda duyurulmasından kaynaklanan damgalama ve ayrımcılık mahremiyet ihlali olarak tanımlanabilir. İndirilen uygulamanın (gönüllü olsa dahi), verileri paylaşmaya zorlamak, Benzer şekilde, Bluetooth ve GPS teknolojileri aracılığıyla virüse maruz kalmanın yanlış tespit edilmesi (yanlış pozitif), bireyin kaygı düzeylerini olumsuz yönde etkileme ve potansiyel olarak gereksiz yere hareket özgürlüğünü kısıtlamak mahremiyet ihlalleri arasında sıralanabilir.

Veri ihlallerini önlemek için mahremiyet önlemleri alması gereken veri sorumlularının güvenilir ve yasal yükümlülöklere sahip oldukları varsayılır; dijital uygulamalarla topladığı verileri uygun

yöntemlerle saklar, kullanır ve gerektiğinde anonim hale getirerek paylaşır. Toplanan veriler dört gruba ayrılır (Pramanik, ve diğerleri, 2021);

- Tanımlayıcılar (Kimlik): Tam ad ve sosyal güvenlik numarası gibi bireyleri benzersiz ve doğrudan tanımlayan bilgileri içerir.
- Yarı tanımlayıcılar (QID): Harici verilerle birleştiğinde, bir bireyin dolaylı olarak tanımlanmasına yol açan tanımlayıcılar. Bu özellikler cinsiyet, yaş ve posta kodu gibi benzersiz olmayan verilerdir.
- Hassas nitelikler (SA): Hastalık ve maaş gibi kişiye özel ve hassas olan verileri içerir.
- Duyarsız nitelikler: Diğer niteliklerin kapsamadığı genel ve riskli olmayan verileri içerir.

### Dijital Kişi İzleme Uygulamaları

Dijital kişi izleme uygulamalarını konum izleme ve temas izleme olarak iki gruba ayırmak mümkündür. Konum izleme uygulamaları kullanıcıların fiziksel hareketlerini izlemek için akıllı telefonlar tarafından oluşturulan küresel konumlandırma sistemini (GPS) ve CSLI (Cell Site Location Information) verilerini kullanır. Temas (yakınlık) izleme uygulamaları, geliştiriciler ve halk sağlığı yetkilileri arasında tercih edilen seçenek olarak ortaya çıkmıştır. Bu uygulamalar, iki cihaz arasındaki mesafeyi yaklaşık olarak tahmin etmek için kullanıcıların akıllı telefonları tarafından yayılan Bluetooth sinyallerinin gücünü kullanır. Apple ve Google tarafından geliştirilen API protokolleri de dahil olmak üzere birçok temas izleme tasarımı, dinamik (benzersiz) bir akıllı telefon tanımlayıcısı oluşturur ve ardından kullanıcı gizliliğini artırmak için bu tanımlayıcıları rutin olarak döndürür (Oliva, 2020).

GPS, RFID, GSM gibi teknolojilerden faydalanan izleme teknolojileri COVID-19 salgınından önce de kullanılmakta ve veri mahremiyeti konusu tartışılmaktaydı, birçok araştırmacı veri mahremiyetinin konum bilgilerinin toplanması ile değil; söz konusu toplu bilgilerin merkezileştirilmesi ve konum bilgilerinin diğer kişi bilgileri ile birleştirilmesi sonucunda ihlal edildiği görüşünü savunmaktadır. Mahremiyeti ihlaline neden olabilecek durumlarda kişilerin bilgilendirilmemiş olması da bir başka eleştiri konusudur. Örneğin, günümüzde Amerika Birleşik Devletleri'nde kolluk kuvvetleri, suçlu, şüpheli ve şartlı tahliye edilenleri farkında olmadan izlemek için kişinin arabasına GoogleEarth ile entegre bir GPS veri kaydedici olan Trackstick gibi bir cihaz kullanmaktadır. Kolluk görevlileri, konuşmaları kaydetmedikleri gerekçesiyle, GPS cihazlarının telefon dinleme ve benzeri elektronik gözetleme biçimlerini düzenleyen yasaların kapsamı dışında kaldığını iddia etmektedir. Diğer bir izleme teknolojisi olan RFID'ler Singapur'da, toplu tren ve otobüslerde temassız ödeme için kullanılan akıllı kartlara (EZLink kartları) yerleştirilmiştir. Her bir EZ-Link kartı bireyin ulusal kimlik numarasıyla ilişkilendirildiğinden toplu taşıma sağlayıcıları, müşterilerinin bireysel seyahat geçmişlerini takip edebilmektedirler. Her seyahat işlemi merkezi bir sunucuda saklanmaktadır. EZ-Link kartı bir tren istasyonunda bir kart okuyucusuna sunulduğunda, müşterinin son elli işlemi görüntülenebilmektedir (Loui & Wang, 2009).

## 1. Veri Saklama

COVID-19 pandemisinin ortaya çıkmasıyla birlikte, salgının yayılmasını azaltmaya yardımcı olmak amacıyla dünya çapında, izleme teknolojilerinin bir bölümünü oluşturan dijital kişi izleme (contact tracing) uygulamalarının kullanılması, kişisel verilerin, şimdiye kadar denenmiş en büyük ölçekli ve en iddialı kullanımlarından birinin oluşmasına neden olmuştur.

Kişisel verilerden oluşan bu büyük ölçekli kamu verisi, en başta halk sağlığı kurum ve kuruluşları, araştırmacılar ve epidemiyologlar için pandemi sürecinin yönetilmesi açısından ölçülemez bir öneme sahiptir. Fakat söz konusu veriler, veri mahremiyeti ihlaline sebep olduğu için güvenliği ve gizliliğine ilişkin tartışmaların ortaya çıkması kaçınılmaz olmuştur (Fahey & Hino, 2020). Cambridge Analytica skandalı gibi ciddi boyutlara ulaşan veri ihlallerinin ortaya çıktığı örnekler, söz konusu kişisel verilerin, pazarlama ve seçim kampanyalarında nasıl kullanıldığının anlaşılması, insanların veri mahremiyeti konusunda, bu tarz dijital kişi takibi uygulamalarına olan yaklaşımlarının daha dikkatli ve seçici olmasına sebep olmuştur (Isaak & Hanna, 2018).

Veri mahremiyeti konusunda, dijital kişi izleme ile ilgili temelde iki sorun mevcuttur. Bu iki sorun, veri güvenliği ve gizliliği açısından riskin ciddiyet ve boyutlarını belirler. Sorunlardan ilki; her bir kişiden toplanacak verinin türü iken, ikincisi ise; verilerin toplayıcısı (kurum, devlet, toplum kuruluşları vs.) açısından hangi yaklaşım ile saklandığıdır (Fahey & Hino, 2020). Bunlardan “**mahremiyet öncelikli (merkezi olmayan)**” yaklaşımda kişisel veriler, yetkili kişilerin (sağlık yetkilileri, araştırmacılar ve kolluk kuvvetlerinin) sınırlı erişimi pahasına korunur ve bireyler kendi verileri üzerinde kontrol sahibidir. Başka bir ifade ile veri mahremiyetini sağlamak için verileri feda eder, tanımlanabilir bireylerin hareketlerini ve etkileşimlerini yetkililere ifşa etmeden etkili derecede temas takibi sağlamaya çalışır. Diğer yaklaşım ise, sağlık yetkililerinin kişisel verilere erişebilirliğine öncelik veren ve büyük miktarda veri depolayan “**veri öncelikli (merkezi)**” yaklaşımdır (Fahey & Hino, 2020).

Her iki yaklaşım da birbirinin zıttı olmamakla birlikte, iki yaklaşım arasında çok büyük farklılıklar da mevcuttur. **Veri öncelikli yaklaşımlarda**, kullanıcıların iletişim bilgileri (telefon numaraları, e-posta adresleri vb.) ve test bilgileri gibi tanımlayıcı, yarı tanımlayıcı veriler, halk sağlığı kurumu gibi merkezi bir otoritede toplanır. Örneğin; Singapur dijital kişi izleme uygulaması olan TraceTogether kullanıcısı COVID-19 testi pozitif sonuçlandığında, bu bilgi Singapur Sağlık Bakanlığı ile paylaşılır ve uygulama bu bilgi doğrultusunda virüs bulaşan kullanıcıda kayıtlı olan kişilerle telefon veya e-posta yoluyla iletişime geçer. **Mahremiyet öncelikli yaklaşımlar**, daha çok, yetkililerden tanımlayıcı/yarı tanımlayıcı verileri saklama eğilimindedir. Örneğin, gerçek kullanıcı iletişim bilgilerini depolamak ve merkezi bir yetkili (otorite) ile paylaşmak yerine, virüs bulaşmış kullanıcıların kendi anonimleştirilmiş kişi günlüklerini bir veritabanına yüklemelerine izin verir. Sistem daha sonra her bir kullanıcının benzersiz tanımlayıcısını kullanarak risk altındaki tüm kullanıcılara bildirir veya ping gönderir, yani aynı networkte bulunan tüm benzeriz tanımlayıcılara bilgi verir. **Mahremiyet öncelikli yaklaşımlar**, sağlık verilerinin hükümet tarafından toplanması ve saklanmasıyla ortaya çıkan mahremiyet endişelerinin tamamını olmasa da bir kısmını ortadan

kaldırır. Bu yaklaşımda yeniden tanımlama teknikleri o kadar yaygın ve etkilidir ki, merkezi olmayan sistemler aracılığıyla veritabanına asgari düzeyde kişisel veri sağlanması bile kullanıcı tanımlamasını riske atar. Bu endişeler, sağlam şifreleme güvenlik önlemleri ile daha da hafifletilmeli ve azaltılmalıdır (Oliva, 2020).

Veri öncelikli yaklaşım, sağlık yetkililerinin virüsle temas eden potansiyel hasta olarak görülen kişileri doğrudan belirlemesine ve iletişim kurmasına olanak tanırken, Mahremiyet öncelikli yaklaşım, bireyleri tanımlamaz ve yalnızca akıllı telefonlarından bilgilendirilmelerine izin verir. Mahremiyet öncelikli yaklaşımda, sağlık yetkilileriyle temasa geçmek veya bir test yaptırmak kişinin kendi inisiyatifine bırakılmaktadır. İnsanların kendilerini “risk altında” olarak tanımlamalarına olanak tanınır. Yeterli kamu desteği ve güveni ile yatırım yapılan böyle bir yaklaşım, virüse sahip olabileceğine inanan bireylerin potansiyel temasları isimsiz olarak tanımlamasına ve kendi kendini izole etmesini seçmesine izin verecektir. Bu yaklaşımın değeri, yalnızca test kitlerinin kıt olduğu yerlerde baskının azaltılmasında değil, aynı zamanda mahremiyetin korunmasında ve kişisel verilerin kontrolünün sağlanmasında ve bir teşhise iliştilmiş potansiyel damgalanmanın önlenmesinde yatmaktadır (Berman, Carter, García-Herranz, & Sekara, 2020). Veri öncelikli yaklaşım, aynı zamanda, temas etkileşim günlüğü ile birlikte GPS konum verilerini de içerir ve sağlık yetkililerinin enfeksiyon kümelerinin meydana geldiği belirli yerleri bulmasına olanak tanır; bu, mahremiyet öncelikli yaklaşımla mümkün değildir. Mahremiyet öncelikli yaklaşım, kümenin nerede oluştuğunu veya enfeksiyonun kimden bulaştığını gizli tutar, fakat yine de potansiyel olarak enfeksiyon kümesine maruz kalan kişileri bilgilendirir. Son olarak, veri öncelikli yaklaşım, bireylerin hareketi, bireyler arasındaki temaslar ve bunun virüsün nüfusa yayılmasında nasıl etkili olduğu hakkında büyük miktarda veri üretir (Fahey & Hino, 2020).

İki yaklaşımın veri mahremiyetine ilişkin temel farklarından bir diğeri ise; veri öncelikli yaklaşımın Merkezi (Centralised) Sunucu Mimarisi, mahremiyet öncelikli yaklaşımın ise Dağıtık-Merkezi Olmayan (Decentralised) Sunucu Mimarisi ile işliyor olmasıdır.

Veri öncelikli yaklaşımda verilerin saklanması (depolanması) ve yetkililerin verilere ulaşması söz konusudur. Veri yönetimi perspektifinden bakıldığında veri öncelikli yaklaşım, genellikle her bir bireye (veya akıllı telefon cihazına) sabit bir tanımlayıcı atamayı, hareketlerinin ve etkileşimlerinin bazı veya tüm ayrıntılarını erişilebilecek merkezi bir sunucuya iletmeyi içerir.

Mahremiyet öncelikli yaklaşımda bireylerin kendi verileri üzerinde kontrolü önem taşır ve bireyler için düzenli olarak değiştirilen dinamik tanımlayıcılar kullanılır. İletişim etkileşimleri kriptografik olarak güvenli bir şekilde yerel cihazlarda saklanır, merkezi bir sunucuda çok az veri tutar veya hiç veri tutmaz. Buradaki veritabanının rolü, bir uyarı gönderilmesi gerektiğinde telefonları kimlik kodlarına göre tanımlamakla sınırlıdır.

## 2. Kişi İzleme Uygulamalarında Kullanılan Protokoller

COVID-19 dijital kişi izleme uygulamalarının büyük çoğunluğu ilgili ülkenin kamu sağlığı otoritesi tarafından yönetilse de söz konusu uygulamalar akademik iş birlikleri ya da özel şirketler

tarafından geliştirilmiştir. Salgınının yayılmasını izlemeyi ve kontrol altına almayı amaçlayan heterojen bir dizi “akıllı” teknoloji protokolü ve uygulaması mevcuttur. (Oliva, 2020). İlk uygulamalar, merkezi (centralised) ve dağıtık (decentralised) mimari seçiminin kişi izleme uygulamaları için en önemli kırılım noktalarından biri olacağını göstermiştir.

Bu amaçla geliştirilen teknolojik altyapı çeşitlerinin ilk örneklerinden bazıları da Temporary Contact Numbers Protocol (TCN) ve BlueTrace protokolleri olmuştur. TCN, blok zincir teknolojisi ile dağıtık bir mimari benimserken, BlueTrace geleneksel yaklaşım olan merkezi sunucu mimarisi kullanmayı tercih etmektedir. 20 Mayıs 2020’de, Google ve Apple, bireylerin COVID-19 pozitif vakalarla yakın temasa maruz kalıp kalmadıklarının tespit edilmesini kolaylaştırmaya yönelik “teknolojiyi halk sağlığı otoritelerine yardım için kullanmak” sloganıyla – kamu sağlığı otoritelerinin oluşturdukları – dijital kişi izleme uygulamaları tarafından kullanılabilen Exposure Notifications System (ENS) protokolünü tanıtmıştır (Altuncu & Altuncu, 2021) (Google & Apple, 2020). ENS protokolü virüs bulaşmış kullanıcıların benzersiz tanımlayıcılarını, yine virüs bulaşmış kullanıcıların yakın oldukları kişilerin akıllı telefon uygulamalarına gönderen genel bir veritabanı oluşturur (Oliva, 2020). Bu protokolün diğer merkezi kişi izleme uygulamalarına nazaran dağıtık bir sistemle işliyor olması, kullanıcıların mahremiyeti açısından bu sisteme güven oluşturmaktadır (Altuncu & Altuncu, 2021).

Süreç içerisinde farklı yeni protokoller üretildiği hâlde henüz kullanılacak mimari türü konusunda bir uzlaşma bulunmamaktadır. Örneğin, Fransa’da kullanılan “ROBERT” protokolü merkezi sunucu mimarisi kullanırken, ENS protokolü dağıtık mimari kullanmaktadır (Altuncu & Altuncu, 2021), (Bay, ve diğerleri, 2020) .

İki mimari arasında kullanıcı mahremiyeti açısından kritik öneme sahip bir fark olmasına rağmen ENS protokolünü tercih eden devletlerin en önemli motivasyonu, protokolün daha pratik bulunmasıdır. Örneğin, İngiltere başlangıçta geliştirdiği kişi izleme uygulamasında merkezi mimari kullanmayı denese de Google ve Apple’ın desteğini almadan başarılı bir sonuca ulaşması mümkün olmamış ve dağıtık mimariyi tercih etmek durumunda kalmıştır (Kelion, 2020), (Vincent, 2020). Google ve Apple, aynı zamanda en popüler iki mobil telefon işletim sistemi üreticisi oldukları için ENS protokolü, işletim sistemi seviyesinde çalışabilirliği ve diğer protokoller gibi işletim sisteminin yaptığı engelleyici müdahalelerin etrafından dolaşacak hileli tekniklere ihtiyaç duymadığı için de bir tercih sebebidir (Altuncu & Altuncu, 2021).

Dikkat edilmelidir ki hangi amaçla olursa olsun, veriyi elinde bulunduran gücün tekelleşmeye bir eğilimi vardır. Tüm bunlardan hareketle mahremiyeti koruma adına, dağıtık mimarilerin daha çok tercih edilebilir olduklarını söylemek mümkündür. Dağıtık modellerde gücün dağıtılmış olması, bir aktörde toplanmıyor olması, kullanıcıda mahremiyetinin korunacağına dair bir güven oluşturmaktadır. Daha önce de bahsedildiği üzere, günümüzde dağıtık modelin kullanıldığı en büyük örnek, Google ve Apple gibi iki teknoloji şirketinin ortak olarak tasarladıkları ENS protokolüdür. Bu iki şirketin, sistemi bir arayüz olarak tasarlamaları ve kişi izleme uygulamalarını belli şartlar altında COVID-19 salgınına ilişkin teknolojik önlemler kapsamına almaları, ortak iyiyi hedefledikleri izlenimini vermektedir. Bu sistem için dağıtık verinin Google ve Apple ile paylaşılmıyor olması bu veri ile bir reklam optimizasyonu yapılamayacağını da göstermiş oluyor, böylece kullanıcıyı ortak iynin hedeflendiği konusunda ikna edebilmektedir (Altuncu & Altuncu, 2021).

Kişi izleme uygulamalarında kullanılan protokoller ve mimari seçimleri Tablo1 de özetlenmiştir.

**Tablo 1. Protokoller ve Sunucu mimarileri**

| PROTOKOL          | SUNUCU MİMARİSİ |
|-------------------|-----------------|
| Blue Trace        | Merkezi         |
| ENS               | Dağıtık         |
| ReCoVer           | Merkezi         |
| TCN               | Dağıtık         |
| ROBERT // PEPP-PT | Merkezi         |
| DP-3T             | Dağıtık         |

### 3. BULGULAR

Temaslı izleme ve gözetim ihtiyacını karşılamak için ülkeler COVID-19 süresince bir dizi teknolojiyi kullanmıştır. Bu teknolojiler, daha geleneksel manuel temas izleme ve gözetim yaklaşımlarına göre maliyeti düşürürken daha hızlı sonuç elde edilmesine de olanak tanımaktadır. Dijital kişi takibi için kullanılan temel bilgi kaynağından biri cep telefonları ve mobil verilerdir. Cep telefonu izleme, bireysel bilgilerin veri tabanı ile paylaşılmasına izin verilmesi dahil, bir kişi izleme uygulamasının gönüllü olarak indirilmesini gerektirir. Diğer durumlarda ise Çin örneğinde olduğu gibi bu tür uygulamaları kullanmak zorunlu tutulmaktadır. Mobil şebeke operatörlerinden gelen konum verileriyle, insanların nerede toplandıkları ve sosyal mesafe önlemlerinin işe yarayıp yaramadığını tespit edilebilmektedir. Cep telefonunun yanı sıra, tanımlama ve doğrulama için bir dizi biyometrik özelliği içeren biyometrik teknolojiler de yüz tanıma, temaslı izleme ve halk sağlığı gözetimi için en yaygın ve ilgili teknolojilerdendir.

Çalışmada dünya genelinde hükümetler tarafından geliştirilen ve vatandaşların kullanımına sunulan COVID-19 mobil kişi izleme uygulamaları: değerlendirme notu/kişi sayısı, işletim sistemi desteği, indirilme sayısı, geliştirici kurum ve kullanılan veri güvenliği protokolü açısından incelenmiştir. (İncelenen uygulama listesi ve detayları EK’te verilmiştir.)

Dünya genelinde toplam 58 ülke tarafından 72 uygulama bu çalışma kapsamında incelenmiştir. Ancak coğrafi konum ve uygulamanın ana dili gibi kısıtlar sebebi ile bazı uygulamaların detaylı bilgilerine erişilememiştir. ABD, Hindistan ve Malezya gibi ülkeler farklı eyaletleri veya bölgelerinde kullanıma sürülen farklı uygulamalar geliştirdiği için bir ülkeye ait birden fazla uygulama bulunabilmektedir.

İndirilme sayısı, ülkenin nüfusuna ve uygulama kullanmanın ülkede zorunlu tutulup tutulmadığı ile bağlantılıdır. Almanya, Endonezya, Fransa, Hindistan, İngiltere, Türkiye, Kolombiya ve Vietnam’da sunulan uygulamaların indirilme sayılarının 10 milyonun üzerinde olduğu görülmüştür. Hindistan 100 milyonun üzerinde indirilme sayısı ile başı çekmektedir. Burada Çin bu kıstasa göre değerlendirme dışında tutulmuştur, çünkü geliştirilen kişi izleme uygulaması Alipay ve WeChat gibi uygulamalara küçük bir ek program ile ekstra bir uygulama indirmenize gerek kalmadan çalışabilmektedir. Bu sebeple Çin’de salt izleme uygulaması indirenlerin sayısına erişilememiştir.

Kullanılan veri güvenliği protokolü ve sunucu mimarisi açısından incelenen 72 uygulamanın 32 tanesi dağıtık mimari kullanırken, 7 tanesi merkezi sunucu mimarisini kullanmayı tercih etmiştir (Bu konuda bilgi sunmayan 33 uygulama mevcuttur). BlueTrace, ReCoVer ve ROBERT gibi protokolleri kullanan merkezi sunucu mimarisini tercih eden Singapur, Kanada, İtalya, Fransa, Fiji, Gürcistan ve Avusturalya veri mahremiyeti konusunda riski yüksek ülkeler olarak tanımlanabilir.

Uygulama geliştiriciler, ülkeye ait Teknoloji Bakanlığı, İçişleri Bakanlığı, Sağlık Bakanlığı gibi kamu kurumlarının yanı sıra, üniversiteler, gönüllü gruplar ve teknoloji şirketlerini de kapsamaktadır.

Kullanıcılar tarafından 100 binin (100B) üzerinde değerlendirme alan uygulamalar Tablo 2 de verilmiştir. (Tablo2 de ve Ek de verilen detaylı tabloda kullanılan “\*” ilgili değerlere ulaşamadığını ifade etmektedir.) Tabloda bulunan uygulamaların hepsi 10 Milyonun (10 Mn+) üzerinde indirilme oranına sahiptir. Ancak indirilme sayısı 10 Milyonun üzerinde olan Kolombiya’da kullanılan uygulamanın yorum sayısı 100B altındadır. Yine bu tabloda bulunan uygulamalardan Almanya ve İngiltere de kullanılan uygulamalar dağıtık mimariyi kullanırken Tablodaki diğer ülkeler bu konuda bilgi vermemiştir.

İncelenen uygulamaların tamamına yakın Android ve iOS mobil işletim sistemleri desteğini sağlamaktadır.

**Tablo 2. COVID-19 Kişi izleme Uygulamalarının Değerlendirilme Sayıları**

| Ülke      | Mobil Uygulama Adı | Değerlendirme Notu / Kişi Sayısı | İşletim Sistemi Desteği | İndirilme Sayısı | Geliştirici                                                     |
|-----------|--------------------|----------------------------------|-------------------------|------------------|-----------------------------------------------------------------|
| Almanya   | Corona-Warn-App    | 3,5/131B                         | Android                 | 10Mn+            | Robert Koch Institute                                           |
| Endonezya | PeduliLindungi     | 3,6/162B                         | Android                 | 10Mn+            | Indonesian Ministry of Communication and Information Technology |
| Fransa    | TousAntiCovid      | 4,2/143B                         | Android                 | 10Mn+            | Government of France                                            |
| Hindistan | Aarogya Setu       | 3,8/1.6M                         | Android                 | 100Mn+           | Union Government of India + National Informatics Centre         |
|           |                    | 4,4/278.2B                       | iOS                     | *                |                                                                 |
| İngiltere | NHS COVID-19       | 4,2/131.B                        | Android                 | 10Mn+            | Pivotal Software for NHSX                                       |
|           |                    | 4,6/409.2B                       | iOS                     | *                |                                                                 |
| Türkiye   | Hayat Eve Sığar    | 3,7/186B                         | Android                 | 10Mn+            | T.C. Sağlık Bakanlığı                                           |
| Vietnam   | Bluezone           | 4,4/243B                         | Android                 | 10Mn+            | Ministry of Health + Ministry of Information and Communications |

#### 4. DEĞERLENDİRME ve SONUÇ

Dijital kişi izleme uygulamaları, mahremiyet tartışmalarının yanında şüphesiz ki COVID-19 süresince, daha fazla sayıda insana ulaşarak manuel kişi takibine göre maliyetleri düşürmüş ve ilgili verilerin daha hızlı ve daha kolay toplanmasına ve analizine olanak tanımıştır. Fakat mobil kişi izleme uygulamalarının bu süreçteki belirgin faydalarına rağmen, uygulamaların mimari tasarımları

ve bu tasarımların altında yatan politikalara karşı, kişilerin mahremiyet ihlalleri doğuracak verilerin toplanması birtakım endişelere yol açmıştır.

Salgın psikolojisinin yanında teknolojilerin yayılma hızı, sorumlu kuruluşları acele ettirerek kontrol mekanizmalarının atlanmasına sebebiyet verebilir. Özellikle bu süreçte toplanan verinin türü, kim tarafından toplandığı denetlenmeli ve veri analizleri sonucunda ortaya konulacak mahrem bilgilerinin yayılmasını, farklı amaçlarla yeniden kullanımını önleyici tedbirler alınması gerekmektedir. Bu sebeple alınması gereken önlemler aşağıdaki şekilde özetlenebilir (Berman, Carter, García-Herranz, & Sekara, 2020);

- Temas takibi veya gözetimi için geliştirilen uygulamaların amacı açıkça tanımlanmalı ve herkesin erişebileceği şekilde belgelendirilmelidir. Bunun yanı sıra sistemin nasıl çalıştığına dair açık bir şekilde toplum bilgilendirilmelidir. Uygulamaları geliştiren kuruluşlar tarafından, kullanıcıların endişelerini giderecekleri ve geri bildirim alabilecekleri erişilebilir şeffaf mekanizmalar tasarıma dahil edilmelidir.
- Veri toplamadan önce, verinin türü, verilerin saklama süresi ve imha zamanıyla ilgili olarak ilgili düzenlemelerde net şartlar oluşturulmalıdır.
- Veri türü, uygulamanın temel amacına ulaşmak için doğrudan gerekli olan veriler ile sınırlandırılmalıdır ve başka amaçlar için yeniden kullanılmalıdır. Tanımlanabilir veriler yerine kimliksizleştirilmiş veya anonimleştirilmiş veriler kullanılmalıdır.
- Veriler merkezi olarak depolanmamalı, eğer depolanıyorsa anonim veriler şifreli olarak tutulmalıdır. Sistem tanımlanabilir verileri kullanıcının cihazında saklayacak şekilde tasarlanmalıdır.
- Veri toplayan kuruluşların, veri transferine kısıtlama getirilmeli, veri ihlalleri sonucunda yasal yükümlülüklerinin tanımlanması gerekmektedir.

Sağlık verilerinin yüksek değeri, olağanüstü hassasiyeti, ülkelerin kapsamlı sağlık veri koruma yasaları ve düzenlemelerinin eksikliği dijital kişi izleme uygulamaları hakkında ciddi endişeler doğurmaktadır. Dünya genelinde kullanılan COVID-19 dijital kişi izleme uygulamalarına bakıldığında birçoğunun mahremiyet konusunda gerekli açıklamayı yapmamış olması, kullanılan mimari konusunda şeffaf olmayışı veri mahremiyeti konusunun öncelikli olmadığını göstermektedir. Öte yandan kullanılan protokol ve mimari konusunda açıklama bulunan uygulamalardan çok azının (7adet) veri öncelikli uygulama olması ümit vericidir. Uygulamalar pek çok hükümet tarafından özellikle halka açık ve kalabalık alanları kullanmak isteyen vatandaşlara zorunlu tutulmuştur. Bu sebeple kullanıcılar veri mahremiyeti algısı yüksek olan vatandaşlar dahi kendi iradeleri dışında sisteme veri sağlamak durumdadır.

## KAYNAKLAR

- Altuncu, S., & Altuncu, M. (2021). Mahremiyet, Verileştirme ve Dijital Kovid-19 Takip Uygulamaları. *TRT Akademi*, 72-87.
- Anandarajan, M., Devine, P., & Simmers, C. (2004). A personal web usage in the workplace: A guide to effective human resources management. *Information Science Publishing*.

- Arif Ali Khan, M. S. (2020). Multi-criteria decision making taxonomy for DevOps challenging factors using analytical hierarchy process. *Journal of Software: Evolution and Process*, 32(10).
- Arsan Ayazlar, R., Sayman, E., & Çınar, M. (2018). Turizm Öğrencilerinin Stajda Sanal Kaytarma Eylemleri. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 5(3): 24-37.
- Babadağ, M. (2018). İşe Yabancılaşmanın Sanal Kaytarma Üzerindeki Etkisi. *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 21(39): 207-239.
- Bay, J., Kek, J., Tan, A., Hau, C., Yongquan, L., Tan, J., & Quy, T. (2020, 04 09). BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency Singapore*, s. 1-9.
- Berman, G., Carter, K., Garcia-Herranz, M., & Sekara, V. (2020). *Digital contact tracing and surveillance during COVID-19 – General and Child-specific Ethical Issues*. Unicef Office of Research – Innocenti.
- Blancard, A., & Henle, C. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, 24: 1067-1084.
- Blau, G., Yang, Y., & Ward-Cook, K. (2006). Testing a Measure of Cyberloafing. *Journal of Allied Health*, 35: 9-17.
- Buyruk Akbaba, A. (2019). Sanal Kaytarmanın Verimliliğe ve Maliyete Etkisi: Bir Alan Araştırması. *Verimlilik Dergisi*, 3: 161-179.
- Clifton, C., Kantarcioglu, M., & Vaidya, J. (2002). Defining Privacy for Data Mining. *In National science foundation workshop on next generation data mining*, 127-133.
- Cohen, I., Gostin, L., & Weitzner, D. (2020, 05 27). Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension. *Journal of the American Medical Association*, s. E1-E2.
- Çavuşoğlu, S., & Palamutçuoğlu, B. (2017). İş Tatmininin Sanal Kaytarma Üzerindeki Etkisi. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 9(19): 430-444.
- Çivilidağ, A. (2017). İş Yaşamında Sanal Kaytarmanın İş Stresi ve İş Doyumu İle İlişkisi Üzerine Bir Araştırma. *Akademik Bakış Dergisi*, 59: 355-373.
- Dağ, İ. (2014). ETKİLİ İLETİŞİMİN EĞİTİM YÖNETİMİNDE ROLÜ. *JOURNAL OF QAFAZ UNIVERSITY – PHILOLOGY AND PEDAGOGY*, 199-214.
- Erden, M. (1998). *Öğretmenlik Mesleğine Giriş*. İstanbul: Alkım Yayınları.
- Erich, F. M. (2017). A qualitative study of DevOps usage in practice. *Journal of Software: Evolution & Process*, 29(6).
- Fahey, R., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, 1-5.
- FT Visual & Data Journalism Team. (2021, 07 06). Coronavirus tracker: the latest figures as countries fight the Covid-19 resurgence. *Financial Times*.
- Glaser, B. G. (2016). Open Coding Descriptions. *Grounded Theory Review*, 108-110.
- Google, & Apple. (2020). *Privacy-Preserving Contact Tracing*. <https://covid19.apple.com/>: <https://covid19.apple.com/contacttracing> adresinden alındı
- Isaak, J., & Hanna, M. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *THE POLICY CORNER*, 56-59.
- İzgi, C. (2014). The concept of privacy in the context of personal health data. *Türkiye Biyoetik Dergisi*, 25-37.
- Kaplan, M., & Çetinkaya, A. Ş. (2014). Sanal Kaytarma ve Demografik Özellikler Açısından Farklılıklar: Otel İşletmelerinde Bir Araştırma. *Anatolia: Turizm Araştırmaları Dergisi*, 25(1), 26-34. doi:10.17123/atad.vol25iss114

- Kaplan, M., & Ögüt, A. (2012). Algılanan Örgütsel Adalet ile Sanal Kaytarma Arasındaki İlişkinin Analizi: Hastane çalışanları örneği. *Dokuz Eylül Üniversitesi İşletme Fakültesi Dergisi*, 13(1), 1-13.
- Kassab, M., & Graciano Neto, V. (2021). Digital Surveillance Technologies to Combat COVID-19: A Contemporary View. *Procedia Computer Science*, 37-44.
- Kaya, E., & Gürtürk, M. (2021). Sanal Kaytarma Davranışının Grup Çatışması ve Yaratıcı Davranış Üzerine Etkisi: Öğretmenler Üzerinde Bir Araştırma. *Parion Akademik Bakış Dergisi (PABD)*, 1(1): 1-18.
- Keklik, B., Kılıç, R., Yıldız, H., & Yıldız, B. (2015). Sanal Kaytarma Davranışlarının Örgütsel Öğrenme Kapasitesi Üzerindeki Etkisinin İncelenmesi . *Business and Economics Research Journal*, 6(3): 129-144.
- Kelion, L. (2020, 04 27). NHS rejects Apple-Google coronavirus app plan. *BBC News*.
- Kristian Nybom, J. S. (2016). On the Impact of Mixing Responsibilities Between Devs and Ops. *Agile Processes, in Software Engineering, and Extreme Programming*. içinde Springer International Publishing.
- Leah Riungu-Kalliosaari, S. M. (2016). DevOps Adoption Benefits and Challenges in Practice: A Case Study. *International Conference on Product-Focused Software Process Improvement*.
- Leonardo Leite, C. R. (2019). A Survey of DevOps Concepts and Challenges . *ACM Computing Surveys*.
- Lim, V. (2002). The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, 23: 675-694.
- Lim, V., & Chen, D. (2012). Cyberloafing at the Workplace: Gain or Drain at Work? *Behavior & Information Technology*, 31(4): 343-353.
- Loui, M., & Wang, J. L. (2009). Privacy and Ethical Issues in Location-Based Tracking Systems. *University of Illinois at Urbana-Champaign*.
- Lucy Ellen Lwakatare, P. K. (2015). Dimensions of DevOps. *Agile Processes in Software Engineering and Extreme Programming* . Oulu, Finland: Springer International Publishing.
- Lucy Ellen Lwakatare, P. K. (2016). An exploratory study of DevOps – extending the dimensions of DevOps with practices. *Proceedings of the Eleventh International Conference on Software Engineering Advances*. Springer International Publisher.
- Muhammad Zulfahmi Toh, S. S. (2019). Adoption Issues in DevOps from the Perspective of Continuous Delivery Pipeline. *International Conference on Software and Computer Applications*.
- Oliva, J. (2020, 08). Surveillance, Privacy, and App Tracking. *Assessing Legal Responses to Covid-19*, s. 40-46.
- Örücü, E., & Yıldız, H. (2014). İşyerinde Kişisel İnternet ve Teknoloji Kullanımı: Sanal Kaytarma. *Ege Akademik Bakış*, 14(1): 99-114.
- Özkalp, H., & Yıldız, H. (2018). Olumlu ve Olumsuz Sanal Kaytarma Davranışlarının İşteki Stres Üzerindeki Etkisi. *“İş, Güç” Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 20: 57-74.
- Özkan, S., & Erbay, E. (2021). Örgüt ikliminin çalışanların sanal kaytarma davranışları üzerindeki etkisi. *Sakarya Üniversitesi İşletme Enstitüsü Dergisi*, 3: 145-153.
- Pramanik, M., Lau, R., Hossain, M., Rahoman, M., Debnath, S., Rashed, M., & Uddin, M. ( 2021). Privacy preserving big data analytics: A critical analysis of state-of-the-art. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 1-26.
- Ramtin Jabbari, N. B. (2016). What is DevOps?: A Systematic Mapping Study on Definitions and Practices. *the Scientific Workshop XP2016*.
- Semerci, A., Ergeneli, A., & Yılmaz, Z. (2021). İş Yeri Yalnızlığının İki Yüzü: Sanal Kaytarma ve Yenilikçi İş Performansı. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 39(1): 133-147.

- Sheikh, A., Aghaz, A., & Mohammadi, M. (2019). Cyberloafing and personality traits: an investigation among knowledge-workers across the Iranian knowledge-intensive sectors. *Behaviour & Information Technology*, 38(12): 1213-1224.
- Singh, R. (2020). DevOPS Now and Then.
- Tan, M., & Demir, M. (2017). İşgörenlerin kişilik özelliklerinin sanal kaytarma davranışı üzerindeki etkisi. *International Journal of Social Sciences and Education Research*, 4(1): 49-68.
- Telli Yamamoto, G., & Altun, D. (2020). Coronavirüs ve Çevrimiçi (Online) Eğitimin Önlenemeyen. *Üniversite Araştırmaları Dergisi*, 25-34.
- Ulusoy, H., & Gültekin Benli, D. (2017). Akademisyenlerin Sanal Kaytarma Davranışları: Bir Kamu Üniversitesi Örneği. *Uluslararası Sosyal Araştırmalar Dergisi*, 10(54): 924-934.
- Uzunsakal, E., & Yıldız, D. (2018). Alan Araştırmalarında Güvenilirlik Testlerinin Karşılaştırılması Ve Tarımsal Veriler Üzerine Bir Uygulama. *Uygulamalı Sosyal Bilimler Dergisi*, 2(1), 14 – 28.
- Vincent, J. (2020, 05 05). Without Apple and Google, the UK's contact-tracing app is in trouble. *The Verge*.
- Vural, Y. (2018). Veri Mahremiyeti: Saldırıları, Korunma ve Yeni Bir Çözüm Önerisi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 21-34.
- Welder Pinheiro Luz, G. P. (2019). Adopting DevOps in the real world: A theory, a model, and a case study. *Journal of Systems and Software*, 157.
- WHO. (2021). <https://www.who.int/> adresinden alındı
- Yarlagadda, R. T. (2018). How Public Sectors Can Adopt the DevOps Practices to Enhance the System. *International Journal of Emerging Technologies and Innovative Research*, 5(9), 796-801.
- Yıldız, H., Yıldız, B., & Ateş, H. (2015). Sanal Kaytarma Davranışının Sergilenmesinde Örgütsel Adalet Algısının Rolü Var mıdır ? *Bilgi Ekonomisi ve Yönetimi Dergisi*, 10(2), 55-66.

## EK

| Ülke        | Mobil Uygulama Adı      | Değerlendirme Notu / Kişi Sayısı | İşletim Sistemi Desteği | İndirilme Sayısı | Geliştirici                                                      | Veri Güvenliği Protokolü | Mimari  |
|-------------|-------------------------|----------------------------------|-------------------------|------------------|------------------------------------------------------------------|--------------------------|---------|
| ABD         | CovidSafe               | *                                | Android – iOS           | *                | Microsoft Volunteers + University of Washington                  | *                        | *       |
|             | Covid Watch             | 3,6/123                          | Android                 | 10B+             | Covid Watch                                                      | ENS                      | Dağıtık |
|             |                         | 3,8/83                           | iOS                     | *                |                                                                  |                          |         |
|             | NOVID                   | 4,4/243                          | Android                 | 10B+             | Expil + Carnegie Mellon University                               | TCN                      | Dağıtık |
|             |                         | 4,7/237                          | iOS                     | *                |                                                                  |                          |         |
|             | Private Kit: Safe Paths | *                                | Android                 | *                | Massachusetts Institute of Technology                            | *                        | *       |
|             |                         | 3,7/121                          | iOS                     | *                |                                                                  |                          |         |
| Almanya     | Corona-Warn-App         | 3,5/131B                         | Android                 | 10Mn+            | Robert Koch Institute                                            | ENS                      | Dağıtık |
|             |                         | 4,2/62B                          | iOS                     | *                |                                                                  |                          |         |
|             | Ito                     | *                                | Android                 | *                | WirVsVirus Hackathon                                             | TCN                      | Dağıtık |
| Avustralya  | COVIDSafe               | 3,7/22B                          | Android                 | 1Mn+             | Australian Department of Health                                  | BlueTrace                | Merkezi |
|             |                         | 4,0/13B                          | iOS                     | *                |                                                                  |                          |         |
| Avusturya   | Stopp Corona            | 3,6/3B                           | Android                 | 500B+            | Austrian Red Cross                                               | ENS                      | Dağıtık |
|             |                         | 2,8/763                          | iOS                     | *                |                                                                  |                          |         |
| Azerbaycan  | e-Tabib                 | 3,8/3B                           | Android                 | 500B+            | Force Task under the Cabinet of Ministers of Azerbaijan          | *                        | *       |
|             |                         | 2,2/12                           | iOS                     | *                |                                                                  |                          |         |
| Bahreyn     | BeAware Bahrain         | 4,3/14B                          | Android                 | 1Mn+             | The Information & eGovernment Authority                          | *                        | *       |
|             |                         | 3,8/4                            | iOS                     | *                |                                                                  |                          |         |
| Bangladeş   | Corona Tracer BD        | 3,7/4B                           | Android                 | 1Mn+             | Directorate General of Health Services                           | *                        | *       |
| Belçika     | Coronalert              | 3,2/5B                           | Android                 | 1Mn+             | Belgian government + Sciensano                                   | DP-3T ve ENS             | Dağıtık |
|             |                         | 4,3/9                            | iOS                     | *                |                                                                  |                          |         |
| Brezilya    | Tô de Olho              | 3,6/217                          | Android                 | 10B+             | Ministério Público do Rio Grande do Norte                        | *                        | *       |
|             |                         | *                                | iOS                     | *                |                                                                  |                          |         |
| Cebelitarık | BEAT Covid Gibraltar    | 3,2/92                           | Android                 | 10B+             | Gibraltar Health Authority                                       | ENS                      | Dağıtık |
|             |                         | 4,1/17                           | iOS                     | *                |                                                                  |                          |         |
| Çekya       | eRouška (eFacemask)     | 3,5/10B                          | Android                 | 1Mn+             | Czech Ministry of Health and Hygiene                             | ENS                      | Dağıtık |
|             |                         | 4,3/4B                           | iOS                     | *                |                                                                  |                          |         |
| Çin         | Health Code             | *                                | Android,iOS             | *                | Alipay and WeChat, Chinese government                            | *                        | *       |
| Danimarka   | Smittestop              | 3,2/2B                           | Android                 | 500B+            | Ministry of Health (Denmark)                                     | ENS                      | Dağıtık |
|             |                         | 3,6/1B                           | iOS                     | *                |                                                                  |                          |         |
| Ekvator     | ASI                     | 3/1B                             | Android                 | 500B+            | Ministry of Telecommunications and Information Society (Ecuador) | ENS                      | Dağıtık |
|             |                         | 44.3/12                          | iOS                     | *                |                                                                  |                          |         |

|              |                                                                   |            |         |        |                                                                                |                                                 |         |
|--------------|-------------------------------------------------------------------|------------|---------|--------|--------------------------------------------------------------------------------|-------------------------------------------------|---------|
| Endonezya    | PeduliLindungi                                                    | 3,6/162B   | Android | 10Mn+  | Indonesian Ministry of Communication and Information Technology                | *                                               | *       |
|              |                                                                   | 3,0/7.8B   | iOS     | *      |                                                                                |                                                 |         |
| Fas          | Wiqaytna                                                          | *          | Android | *      | Ministry of Interior                                                           | Bluetooth                                       | *       |
|              |                                                                   | 4,4/126    | iOS     | *      |                                                                                |                                                 |         |
| Fiji         | careFIJI                                                          | 4/2B       | Android | 100B+  | Government of Fiji                                                             | Blue Trace                                      | Merkezi |
|              |                                                                   | 3,1/57     | iOS     | *      |                                                                                |                                                 |         |
| Finlandiya   | Koronavilkku                                                      | 3,1/5B     | Android | 1Mn+   | Finnish Institute for Health and Welfare                                       | ENS                                             | Dağıtık |
|              |                                                                   | 4,4/2.1B   | iOS     | *      |                                                                                |                                                 |         |
| Fransa       | TousAntiCovid                                                     | 4,2/143B   | Android | 10Mn+  | Government of France                                                           | *                                               | *       |
|              |                                                                   | 3,9/184    | iOS     | *      |                                                                                |                                                 |         |
|              | ROBERT (ROBust and privacy-presERving proximity Tracing protocol) | *          | *       | *      | The National Institute for Research in Computer Science and Automation (INRIA) | PEPP-PT (presERving proximity Tracing protocol) | Merkezi |
| Gana         | GH COVID-19 Tracker App                                           | 3,7/39     | Android | 10B+   | Ministry of Communication and Technology, Ministry of Health                   | *                                               | *       |
|              |                                                                   | *          | iOS     | *      |                                                                                |                                                 |         |
| Güney Afrika | COVID AlertSA                                                     | 3,3/3B     | Android | 1Mn+   | Department Of Health                                                           | ENS                                             | Dağıtık |
|              |                                                                   | 3,5/399    | iOS     | *      |                                                                                |                                                 |         |
| Güney Kore   | Corona 100m                                                       | *          | *       | *      | *                                                                              | *                                               | *       |
| Gürcistan    | Stop Covid                                                        | *          | *       | *      | Novid20 + Georgian Ministry of Health                                          | PEPP-PT                                         | Merkezi |
| Hırvatistan  | Stop COVID-19                                                     | *          | Android | *      | Croatian government                                                            | *                                               | *       |
|              |                                                                   | *          | iOS     | *      |                                                                                |                                                 |         |
| Hindistan    | Aarogya Setu                                                      | 3,8/1.6M   | Android | 100Mn+ | Union Government of India + National Informatics Centre                        | *                                               | *       |
|              |                                                                   | 4,4/278.2B | iOS     | *      |                                                                                |                                                 |         |
|              | COVA Punjab                                                       | 3,6/35B    | Android | 1Mn+   | Government of Punjab                                                           | *                                               | *       |
|              |                                                                   | 3,5/1.5B   | iOS     | *      |                                                                                |                                                 |         |
|              | COVID-19 Quarantine Monitor                                       | 3,9/225    | Android | 100B+  | Government of Tamil Nadu + Pixxon AI Solutions                                 | *                                               | *       |
|              | Mahakavach                                                        | 3,9/1.1B   | Android | 100B+  | Government of Maharashtra                                                      | *                                               | *       |
|              | Quarantine Watch                                                  | 3,6/1.1B   | Android | 100B+  | Government of Karnataka                                                        | *                                               | *       |
| Hollanda     | CoronaMelder                                                      | 3,2/8.5B   | Android | 1Mn+   | Ministry of Health, Welfare and Sport                                          | ENS                                             | Dağıtık |
|              |                                                                   | 3,6/5.9B   | iOS     | *      |                                                                                |                                                 |         |
|              | PrivateTracer                                                     | *          | Android | *      | Milvum                                                                         | ENS                                             | Dağıtık |
|              |                                                                   | *          | iOS     | *      |                                                                                |                                                 |         |



|           |                                                 |            |         |       |                                                                                                |                        |         |
|-----------|-------------------------------------------------|------------|---------|-------|------------------------------------------------------------------------------------------------|------------------------|---------|
| Hong Kong | LeaveHomeSafe                                   | 3,3/19.3B  | Android | 1Mn+  | The Office of the Government Chief Information Officer                                         | QRCode, Self-Developed | *       |
|           |                                                 | 2,0/76     | iOS     | *     |                                                                                                |                        |         |
| İngiltere | NHS COVID-19                                    | 4,2/131.B  | Android | 10Mn+ | Pivotal Software for NHSX                                                                      | ENS                    | Dağıtık |
|           |                                                 | 4,6/409.2B | iOS     | *     |                                                                                                |                        |         |
| İrlanda   | COVID Tracker                                   | 3,9/5.3B   | Android | 1Mn+  | Health Service Executive (HSE)                                                                 | ENS                    | Dağıtık |
|           |                                                 | 5,0/1      | iOS     | *     |                                                                                                |                        |         |
| İskoçya   | Protect Scotland                                | 3,3/3.1B   | Android | 500B+ | NearForm for NHS Scotland Test and Protect                                                     | ENS                    | Dağıtık |
|           |                                                 | 4,4/1.3B   | iOS     | *     |                                                                                                |                        |         |
| İspanya   | Radar COVID                                     | 2,7/19.9B  | Android | 5Mn+  | Ministry of Economic Affairs and Digital Transformation, Indra Sistemas                        | ENS                    | Dağıtık |
|           |                                                 | 3,5/4      | iOS     | *     |                                                                                                |                        |         |
| İsrail    | HaMagen                                         | 3,1/5.2B   | Android | 1Mn+  | Israeli Health Ministry                                                                        | *                      | *       |
|           |                                                 | 2,9/70     | iOS     |       |                                                                                                |                        |         |
| İsviçre   | SwissCovid                                      | 3,3/4.3B   | Android | 1Mn+  | École polytechnique fédérale de Lausanne + the Swiss Federal Institute of Technology in Zurich | ENS                    | Dağıtık |
|           |                                                 | 4,7/40     | iOS     | *     |                                                                                                |                        |         |
| İtalya    | Immuni                                          | 2,8/51.9B  | Android | 5Mn+  | Bending Spoons + Ministry of Health (Italy)                                                    | ENS                    | Dağıtık |
|           |                                                 | 3,4/66     | iOS     | *     |                                                                                                |                        |         |
|           | SM-COVID-19                                     | 3,3/874    | Android | 100B+ | Softmining                                                                                     | ReCoVer                | Merkezi |
|           |                                                 |            | iOS     |       |                                                                                                |                        |         |
| İzlanda   | Rakning C-19                                    | 4,1/502    | Android | 100B+ | Iceland's Department of Civil Protection + Emergency Management and Directorate of Health      | *                      | *       |
|           |                                                 | 4.03.2016  | iOS     | *     |                                                                                                |                        |         |
| Japonya   | COVID-19 Contact-Confirming Application (COCOA) | 2,4/21.8B  | Android | 5Mn+  | COVID-19 Radar Japan                                                                           | ENS                    | Dağıtık |
|           |                                                 | 2,9/1.9B   | iOS     | *     |                                                                                                |                        |         |
| Jersey    | Jersey COVID Alert                              | 3,5/60     | Android | 10B+  | Digital Jersey                                                                                 | ENS                    | Dağıtık |
|           |                                                 | 4,4/43     | iOS     |       |                                                                                                |                        |         |
| Kanada    | COVID Alert                                     | 3,6/8.5B   | Android | 1Mn+  | Shopify, Blackberry, Canadian Government                                                       | ENS                    | Dağıtık |
|           |                                                 | 4,3/4.9B   | iOS     | *     |                                                                                                |                        |         |
|           | ABTraceTogether                                 | 2,5/1.1B   | Android | 100B+ | Alberta Government                                                                             | Blue Tace              | Merkezi |
|           |                                                 | 2,0/1B     | iOS     | *     |                                                                                                |                        |         |
| Katar     | Ehteraz                                         | 4,5/46B    | Android | 1Mn+  | Ministry Of Interior - Qatar                                                                   | *                      | *       |
|           |                                                 | 3,4/2.2B   | iOS     | *     |                                                                                                |                        |         |
| Kolombiya | CoronApp                                        | 3,5/73.B   | Android | 10Mn+ | Colombian Government                                                                           | *                      | *       |
|           |                                                 | *          | iOS     | *     |                                                                                                |                        |         |

|                 |                          |            |         |       |                                                                         |           |         |
|-----------------|--------------------------|------------|---------|-------|-------------------------------------------------------------------------|-----------|---------|
| Kuzey İrlanda   | Stop Covid NI            | 3/661      | Android | 100B+ | NearForm                                                                | ENS       | Dağıtık |
|                 |                          | 3,4/402    | iOS     | *     |                                                                         |           |         |
| Kuzey Makedonya | StopKorona               | 3,5/327    | Android | 50B+  | Ministry of Health (North Macedonia), Nextsense                         | *         | *       |
|                 |                          | *          | iOS     | *     |                                                                         |           |         |
| Letonya         | Apturi Covid             | 3/1.3B     | Android | 100B+ | Consortium of volunteers + Ministry of Health of the Republic of Latvia | ENS       | Dağıtık |
|                 |                          | 4,6/9      | iOS     | *     |                                                                         |           |         |
| Macaristan      | VirusRadar               | *          | Android | *     | Ministry of Innovation and Technology + NextSense                       | *         | *       |
|                 |                          | *          | iOS     | *     |                                                                         |           |         |
| Malezya         | MyTrace                  | *          | Android | *     | Ministry of Science, Technology and Innovation (Malaysia) (MOSTI)       | *         | *       |
|                 |                          | *          | iOS     | *     |                                                                         |           |         |
|                 | Gerak Malaysia           | 3,7/7.5B   | Android | 1Mn+  | Royal Malaysia Police + Ministry of Health                              | *         | *       |
|                 |                          | *          | iOS     | *     |                                                                         |           |         |
|                 | SELangkah                | 4,2/3B     | Android | 500B+ | Government of Selangor                                                  | QR Code   | *       |
|                 |                          | 2,0/ 376   | iOS     | *     |                                                                         |           |         |
| Nepal           | COVIRA                   | *          | Android | *     | Science Hub Nepal                                                       | *         | *       |
|                 |                          | *          | iOS     | ???   |                                                                         |           |         |
| Norveç          | Smittestopp              | 3,2/814    | Android | 100B+ | Simula Research Laboratory + Norwegian Institute of Public Health       | ENS       | Dağıtık |
|                 |                          | 4,3/6      | iOS     | ???   |                                                                         |           |         |
| Polonya         | ProteGO Safe             | 4,4/18.8B  | Android | 1Mn+  | Ministry of Digital Affairs of Poland                                   | ENS       | Dağıtık |
|                 |                          | 4,5/6.1B   | iOS     | *     |                                                                         |           |         |
| Portekiz        | Stayaway COVID           | 2,5/9.8B   | Android | 1Mn+  | INESC TEC + ISPUP + Keyruptive + Ubirider                               | ENS       | Dağıtık |
|                 |                          | 3,5/1.1B   | iOS     | *     |                                                                         |           |         |
| Rusya           | Contact Tracer           | *          | Android | *     | SoftTree                                                                | ENS       | Dağıtık |
| Singapur        | TraceTogether            | 3,9/22.3B  | Android | 1Mn+  | Government Technology Agency of Singapore                               | BlueTrace | Merkezi |
|                 |                          | 3,4/189    | iOS     | *     |                                                                         |           |         |
| Suudi Arabistan | Tabaud                   | 4,4/4.7B   | iOS     | *     | Saudi Data and Artificial Intelligence Authority (SDAIA)                | ENS       | Dağıtık |
| Tayvan          | Taiwan Social Distancing | 3,8/11.6B  | Android | 1Mn+  | Taiwan AI Labs + Taiwan Centers for Disease Control                     | ENS       | Dağıtık |
|                 |                          | 3,9/4.5B   | iOS     | *     |                                                                         |           |         |
| Türkiye         | Hayat Eve Sığar          | 3,7/186B   | Android | 10Mn+ | T.C. Sağlık Bakanlığı                                                   | *         | *       |
|                 |                          | 3,3/16.6 B | iOS     | *     |                                                                         |           |         |
| Ürdün           | AMAN App – Jordan        | 3,1/7.6B   | Android | 1Mn+  | Jordan's Ministry of Health                                             | GPS       | *       |
|                 |                          | 3,5/151    | iOS     | *     |                                                                         |           |         |



|                 |                          |          |         |       |                                                                          |                |         |
|-----------------|--------------------------|----------|---------|-------|--------------------------------------------------------------------------|----------------|---------|
| Vietnam         | Bluezone                 | 4,4/243B | Android | 10Mn+ | Ministry of Health<br>+ Ministry of<br>Information and<br>Communications | *              | *       |
|                 |                          | 4,1/31B  | iOS     | *     |                                                                          |                |         |
| Yeni<br>Zelanda | NZ COVID Tracer          | 4,2/6.6B | Android | 1Mn+  | Ministry of Health                                                       | ENS+QR<br>Code | Dağıtık |
|                 |                          | 3,3/2B   | iOS     | *     |                                                                          |                |         |
| Yunanistan      | DOCANDU Covid<br>Checker | *        | Android | 1B+   | DOCANDU+ Region<br>of Attica + Athens<br>Medical Association             | *              | *       |
|                 |                          | *        | iOS     | *     |                                                                          |                |         |



MARMARA  
ÜNİVERSİTESİ