TRTakademi
ISSN 2149-9446 | Cilt 06 | Sayı 11 | Ocak 2021 | Büyük Veri

Mahremiyet, Verileştirme ve Dijital Kovid-19 Takip Uygulamaları

SAFA NUR ALTUNCU
MUHAMMED TARIK ALTUNCU

Öz

İlk dalga Kovid-19 salgınının ardından otoriteler ve bazı özel şirketler salgınla mücadeleyi ve filyasyonu yaygınlaştırmak adına çeşitli dijital uygulamalar üretme hazırlıklarına başlamıştır. Kullanıcıların riskli kişilerle temas kurup kurmadığını takip eden bu uygulamaların kişilerin Küresel Konumlama Sistemi (GPS) ve bluetooth gibi teknolojiler vasıtasıyla lokasyonlarını ve bireyler arası mesafeleri ölçmesi, güvenlik ve mahremiyet kaygısını da beraberinde getirmektedir. Google ve Apple, 20 Mayıs 2020 tarihinde, bireylerin Kovid-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 filyasyon uygulamaları tarafından kullanılabilen maruz kalma arayüzünü tanıtmıştır. Bu arayüzün diğer merkezî (centralised)filyasyon uygulamalarına nazaran dağıtık (decentralised) bir sistemle işliyor olması, bu sisteme kullanıcıların mahremiyeti açısından güven oluşturmaktadır.

Koronavirüs salgını sırasında teknolojik çözümlerin kullanılması temas takibi için avantajlı görünse de bazı kısıtlamaları da beraberinde getirmektedir. Sosyolojik bir perspektiften bakıldığında, bu çözümleri kullanmanın kritik bir sonucu, insanların verileştirilmesidir ve bu durum bireylerin metalaştırılmasına giden yolu açmaktadır. Bu makale, farklı aktörler tarafından oluşturulmuş dijital filyasyon uygulamaları aracılığıyla üretilen verinin, veri sahipliğinin ve mahremiyet ölçülerinin biyopolitika üzerinden güncel bir okumasını yaparak dijital filyasyon uygulamaları hakkında bir durum değerlendirmesi sunmayı amaçlamaktadır. Aynı zamanda, uygulama kullanıcılarının mahremiyeti ihlal edecek durum ve sistemlerin farkına varmak adına veri okuryazarı olmalarının ehemmiyetini göstermeyi hedeflemektedir.

Anahtar Kelimeler: Verileştirme, Kovid-19, Dijtal Filyasyon Uygulamaları, Google&Apple API

Araştırma Makalesi

Geliş Tarihi: 16.11.2020
Kabul Tarihi: 19.01.2021

ORCID ID: 0000-0003-2874-2623 E-mail: safanuraltuncu@gmail.com DOI: 10. 37679/trta.826421
ORCID ID: 0000-0003-0516-1201 E-mail: tarikaltuncu@gmail.com

TRTakademi
ISSN 2149-9446 | Volume 06 | Issue 11 | January 2021 | Big Data

Privacy, Datafication and COVID-19 Digital Contact-tracing Apps

SAFA NUR ALTUNCU
MUHAMMED TARIK ALTUNCU

Abstract

After the first wave of the COVID-19 outbreak, public health authorities and some private companies started preparations to produce various digital applications in order to ease contact tracing in the fight against the pandemic. The fact that these applications use Global Positioning System (GPS) and/or bluetooth technologies to obtain location of their users and measure their distances to other individuals constantly brought the question of security and privacy. On May 20, Google and Apple introduced the exposure notifications API to be used by contact tracing applications of public health authorities to make it easier to identify whether individuals have been in close contact with COVID-19 positive cases with the slogan of 'Using technology to help public health authorities'. The fact that this interface operates with a distributed system compared to the other centralised contact tracing applications has created trust in this system in terms of privacy.

Although using technological solutions seems advantageous for contact-tracing during Coronavirus pandemic; it brings some limitations as well. From a sociological perspective, a critical outcome of using these solutions is datafication of people; hence, pave the way towards commodification of them. This research aims to describe the present situation about the ownership and privacy measures of the data obtained via the digital contact tracing applications of different actors over the concept of `biopolitics'. Meanwhile, it aims to project the significance of being data literate in order to protect the application users in any case of violation of privacy.

Keywords: Datafication, COVID-19, Contact-tracing Apps, Google&Apple API

Research Paper

Recieved: 16.11.2020
Accepted: 19.01.2021

ORCID ID: 0000-0003-2874-2623 E-mail: safanuraltuncu@gmail.com DOI: 10. 37679/trta.826421
ORCID ID: 0000-0003-0516-1201 E-mail: tarikaltuncu@gmail.com

1. Giriş

Koruyucu başka faktörler olmaksızın (maske, siperlik vb.) Kovid-19 virüsü taşıyan bir kişi ile temasta bulunulması ya da sosyal mesafeye dikkat edilmeksizin bu kişiyle uzun süre geçirilmesi enfekte olma riskini artıran önemli faktörlerdendir. Bugün geleneksel filyasyon uygulamaları, test sonucu pozitif çıkan kişinin hastalığın kuluçka süresi için üst sınır olarak belirlenen süre (mesela 5 gün) içerisinde birlikte bulunduğu kişilerin tespit edilmesi, bilgilendirilmesi ve takip eden bir müddet (örneğin 14 gün) boyunca kendilerini diğer insanlardan izole etmesi gerektiği konusunda uyarılması şeklinde uygulanmaktadır. Ancak bu süreç her gün çok sayıda tanımadığı insanla bir arada vakit geçiren bir kişi için -mesela bir taksi şoförü- takip edilmesi imkânsız pek çok ciddi kısıtlamayı barındırmaktadır.

Öte yandan sosyal mesafenin korunması ve filyasyon teknikleri için dijital teknolojilerin kullanılması hakkında gün geçtikçe daha çok araştırma yapılmaktadır. Örneğin, bazı araştırmacılar bir ortamda var olan görüntüleme sistemlerini kullanarak insanların uzay-zamansal hareketlerini iki boyutlu bir düzlemde analiz ederek sosyal mesafe takibi yapmayı ve benzer bir teknoloji ile kritik yoğunluk ölçümü yaparak kapalı alanlara giriş çıkışı düzenlemeyi teklif etmektedir. (Yang vd. 2020). Bir başka araştırma grubu, geliştirdikleri giyilebilir cihazlarda bulunan manyetik alan sensörleri yardımı ile insanların birbirlerine fiziksel mesafesini ölçerek daha hassas bir ölçüm vaad etmektedir (Bian vd. 2020). Bahsedilen her iki yöntem de ihtiyaç duydukları özel cihazlar nedeniyle sadece belirli sınırlar içerisinde işlev görebilmektedir. Diğer bir açıdan, bu yöntemler ancak nüfusun çok az bir kısmını kapsayabilecek niteliğe sahiptir. Başka pek çok özel sensör ya da gelişmiş teknoloji çözümleri önerilmiş olmasına rağmen genel eğilim, modern kapitalist toplumlarda kitlelerde hâlihazırda yaygınlaşmış akıllı telefonların çoğunda mevcut teknolojileri kullanmak yönündedir.

Bu sebeple ilk koronavirüs dalgasının ardından virüsün ikinci bir dalga durumunda tekrar ve belki daha hızlı yayılmasının önüne geçebilmek için teknolojik imkânlardan faydalanmak isteyen pek çok ulusal kamu sağlığı otoritesi, filyasyon çalışmalarını destekleyecek dijital temas takip uygulamaları geliştirmiştir. Bireylerin verileştirilmesi ve mahremiyetin ihlali sorunlarının kısmi olarak arka planda kaldığı bu küresel kriz döneminde, kamu sağlığı otoriteleri tarafından geliştirilen bu uygulamaları bireyin mahremiyeti ile ilgili endişeleri, uygulamanın teknik anlamda kullanıcının mahremiyetini koruması açısından ve uygulamada toplanan verinin sahipliği açısından irdelemektedir.

Koronavirüs temas-takip uygulamalarının büyük çoğunluğu ilgili bölgenin kamu sağlığı otoritesi tarafından yönetilse de akademik iş birlikleri yahut özel şirketler

tarafından geliştirilmektedir. Bu amaçla geliştirilen teknolojik altyapı çeşitlerinin ilk örneklerinden bazıları TCN[1] ve BlueTrace[2] protokolleri olmuştur. Bunlardan ilki blok zincir teknolojisi ile dağıtık (decentralised) bir mimari benimserken ikincisi geleneksel yaklaşım olan merkezî (centralised) sunucu mimarisi kullanmayı tercih etmektedir. Henüz ilk uygulamalar, merkezî (centralised) ve dağıtık (decentralised) mimari seçimi filyasyon uygulamaları için en önemli kırılım noktalarından biri olacağını göstermiştir. Fakat süreç içerisinde yeni protokoller üretildiği hâlde henüz mimari türü konusunda bir uzlaşı bulunmamaktadır. Örneğin, Fransa'da kullanılan ROBERT protokolü[3] merkezî (centralised) sunucu altyapısı kullanırken Google ve Apple'ın birlikte ürettiği "Maruz Kalma Arayüzü" altyapısı[4] dağıtık (decentralised) mimari kullanmaktadır.

İki mimari arasında kullanıcı mahremiyeti açısından kritik öneme sahip bir fark olmasına rağmen maruz kalma arayüzünü tercih eden devletlerin en önemli motivasyonu beklenenden daha pratik bir sebep bulunmaktadır. Örnek vermek gerekirse İngiltere, merkezî (centralised) sunucu kullanan bir filyasyon uygulaması üreterek test etti. Başlangıçta dağıtık (decentralised) bir mimari kullanmamak için diretse de (Kelion, 2020) Apple ve Google'ın desteğini almadan başarılı bir sonuca ulaşmak mümkün olmadı (Vincent, 2020). Google ve Apple, aynı zamanda en popüler iki mobil telefon işletim sistemi üreticisi oldukları için ürettikleri arayüz, işletim sistemi seviyesinde çalışabildi ve diğer protokoller gibi işletim sisteminin yaptığı engelleyici müdahalelerin etrafından dolaşacak hileli tekniklere ihtiyaç duymadı.

Oluşturulan bu dijital filyasyon altyapılarının her birinin teknik üstünlükleri ve kısıtlamaları bulunduğu gibi, kitlelerin mahremiyetini kısıtlayan veya mahremiyetin oluşmasına imkân sağlayan tarafları da bulunmaktadır. Bu makalenin ilk kısmında takip uygulamalarının kullandıkları teknikler ve mahremiyet ilkeleri olarak kullanıcı güvenliğini sağlayıp sağlamadıkları incelenmektedir. Bu kısımda merkezî (centralised) ve dağıtık (decentralised) mimarilere spesifik örnekler sunularak bu yapıların limitasyonları tartışılacaktır.

Makalenin ikinci kısmında ise mahremiyet ve onun ihlali ile oluşan gözetim kültürü, filyasyon uygulamalarını geliştiren tarafların mahiyeti üzerinden tartışılacaktır.

[1]TCN protokolü hakkında detaylı bilgi için: https://en.wikipedia.org/wiki/TCN_Protocol

[2]BlueTrace protokolü hakkında detaylı bilgi için: https://en.wikipedia.org/wiki/BlueTrace

[3]ROBERT protokolü hakkında detaylı bilgi için: https://github.com/ROBERT-proximity-tracing/documents

[4]Maruz kalma arayüzü hakkında detaylı bilgi için: https://en.wikipedia.org/wiki/Exposure_Notification

Bu kısımda, Foucault'un modern hayatta bireyin kitlelere indirgenerek toplum ve devletin bedenleri istatistik üzerinden disipline etmesini işlediği biyopolitika kavramından yola çıkarak devlet ve şirketlerin gözetim kültürüne katkı sağlayabilecek olan Kovid-19 takip uygulamaları incelenecektir. Gözetim kültürlerine katkıları açısından bu iki oluşumdan hangisinde kullanıcıların kendi mahremiyetlerini daha iyi koruyabilecekleri tartışılacaktır.

2. Teknik Özellikleri ve Altyapıları İtibariyle Dijital Filyasyon Uygulamaları

Akıllı telefonlar; kullanıcıları tarafından yüklenecek yazılımlar aracılığıyla bağlı bulundukları Wi-Fi ve GSM ağları yardımıyla düşük hassasiyetli coğrafi konumlarını, sahip oldukları Küresel Konumlama Sistemi (GPS) özellikleri aracılığıyla da yüksek hassasiyetli uzaysal konumlarını üç boyutlu olarak tespit edebilmektedir.

Aynı zamanda, bluetooth gibi yakın mesafeli radyo frekansı özellikleri yardımıyla diğer cihazlarla aralarındaki mesafelerini tespit ederek hangi kullanıcıların birbirlerine ne zaman, nerede ve ne kadar yaklaştıklarını yapılandırılmış bir şekilde sürekli akan veri kaynakları hâline dönüştürebilmektedir. Bahsedilen tüm veri çeşitleri beraberinde farklı kısıtlamalar getirmekle birlikte, bu cihazların filyasyon amacıyla kullanımı hedeflenen kitlenin her bireyinin bir akıllı telefon sahibi olduğunu, ilgili yazılımı telefonlarına yüklemiş olduklarını ve telefonlarını sürekli yanlarında, açık ve sinyal alabilir bir durumda bulundurduklarını varsaymaktadır. Ayrıca bu veri tipleri ile yapılan risk değerlendirmelerine maske ya da benzeri koruyucu ekipmanların kullanımı gibi alınan ek tedbirler yahut fiziksel temas bilgisi dâhil edilememektedir. (Stanley & Callas, 2020) Tüm bunlara rağmen, geniş kitleler tarafından kullanılırsa bu tür uygulamaların filyasyon için etkili olabileceğine inanılmaktadır. Ancak böylesine geniş kapsamlı ve kitlesel ölçekte veri paylaşımı, beraberinde kitlesel gözetlenme tehlikesi ve mahremiyet kaygısı getirir.

Akıllı telefon pazarının neredeyse tamamında kullanılan Android ve iOS işletim sistemlerinin (Mobile OS Market Share 2019, 2020) geliştiricisi olan Google ve Apple şirketleri 2020 yılının Nisan ayında Kovid-19 ile mücadele etmek adına bir iş birliği oluşturmuştur (Apple and Google Partner on COVID-19 Contact Tracing Technology, 2020). Bu konsorsiyum, bahsi geçen iki mobil işletim sisteminde desteklenen ortak bir arayüz geliştirmiştir. "Maruz Kalma Arayüzü" ismi verilen bu sistem, bir filyasyon uygulaması değil de ulusal kamu sağlığı otoritelerinin geliştireceği filyasyon uygulamalarının kolaylıkla erişerek kullanabileceği bir uygulama programlama arayüzü (API) olarak sunulmuştur. Bu sistem, Android ve iOS işletim sistemi kullanan akıllı telefonların bluetooth üzerinden çevrelerine anonimleştirilmiş bir kimlik bilgisi yayınlamasını ve yakın çevrede bulunan diğer yayıncı

cihazlardan gelen kimlik bilgisini sinyal gücü ve yayın tarihi ile birlikte güvenli bir şekilde depolamasını sağlamaktadır. Sürekli paylaşılan bu kimliğe Dönüşümlü Mesafe Kimlikleri (RPIK) ismi verilmektedir. Bu kimlik yayınının kötü niyetli taraflarca yerleştirilebilecek dinleyicilerle takip edilmesini engellemek için RPIK'ler her 10 dakikada bir yenilenmektedir. Her bir RPIK, telefonun 24 saatte bir yenilediği Geçici Temas Anahtarları (TEK) kimliği kullanılarak üretilebilmektedir. API, TEK kimliği bilmeksizin RPIK'lerin tekil kullanıcıya ait olup olmadığı kestirilemeyen bir sisteme sahiptir.[5]

Mahremiyet kaygısını birincil planda tutan "Maruz Kalma Arayüzü" dağıtık (decentralised) bir sistem olma özelliği göstermektedir. Bu, sistemde tüm verinin aktarıldığı merkezî (centralised) bir sunucu bulunmadığını göstermektedir. Bunun yerine tüm cihazlar yakın bulundukları diğer cihazlardan yayınlanan RPIK kimlik bilgilerini kendi hafızalarında saklamaktadır. Eğer bir kullanıcı test olur ve sağlık birimleri tarafından Kovid-19 tanısı konulursa kendi isteğine bağlı olarak, sağlık ekipleri tarafından kendisiyle paylaşılan Transaction Authentication Number (TAN) kodunu kullanarak kendini bu altyapıyı kullanan filyasyon uygulaması üzerinde enfekte olarak işaretleyebilir. Yalnızca bu durumda kullanıcıya ait telefonun son 14 gün içerisinde ürettiği tüm TEK kodları kamu otoritesinin sunucusuna gönderilir. Sisteme dâhil tüm telefonlar bu sunucuyu sık sık kontrol ederek, enfekte olarak işaretlenmiş yeni TEK kodlarını temin eder. Bu TEK kodları ile üretilmesi mümkün tüm RPIK'ler her bir telefonda yeniden üretilir ve daha önce yakın cihazlardan edinilerek hafızaya kaydedilmiş RPIK listesi ile kıyaslanır. Her bir RPIK, sadece bir tek TEK kodu ile üretilebilecek özelliğe sahip olduğu için bir eşleşme tespit edilmesi durumunda, API filyasyon uygulamasını kullanıcının enfekte bir kişi ile temasa maruz kaldığı bilgisi ile birlikte maruz kalınan gün, maruz kalma süresi ve sinyal kuvveti bilgilerini paylaşır. Uygulamanın sahibi olan kamu sağlığı otoritesinin belirlediği eşik değerlerini geçerek tehlikeli olarak tespit edilen maruz kalma durumlarında kullanıcı, temaslı olduğu hususunda uyarıldığı bir bildirim alır ve süreç hakkında rehberlik edici materyallerle desteklenerek karantinaya girmesi talep edilir. Tüm bu süreç boyunca platform sahibi Google ve Apple hiçbir veri almazken arayüzü kullanan uygulamanın sahibi olan kamu sağlığı otoritesi, sadece kullanıcının arayüzü kullanma rızası, enfekte olan kullanıcının pozitif test sonucunu teyit etmek için kullanılan TAN kodu ve pozitif kullanıcının onayına bağlı olarak, paylaşılan TEK kodlarını veri olarak temin edebilir (York, 2020). Google ve Apple, arayüz kullanımını onaylamak için kamu sağlığı otoritelerine kullanıcıdan

[5]Detaylı bilgi için: https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf

lokasyon kullanım izni almamak, sadece temas uyarısı almak isteyen kullanıcıyı hiçbir kişisel bilgisini paylaşmak zorunda bırakmamak, temaslı olduğu tespit edilen kullanıcıya rehberlik edici materyaller sunmak gibi sınırlandırıcı şartlar da koymaktadır.[6] Hâlihazırda Almanya'da Corona Warn-App (York, 2020), İngiltere'de NHS Kovid-19 ve Japonya'da COCOA gibi pek çok ülkede bu API desteği ile çalışan filyasyon uygulamaları kullanılmaya başlanmıştır.

Alternatif olarak bazı ulusal kamu sağlığı otoriteleri tüm verinin kendi erişim ve yönetimlerinde olduğu merkezî (centralised) sunucularda toplanarak mahremiyetin ikinci planda kaldığı geleneksel yöntemleri kullanmaktadır. Bu yöntemin en iddialı savunucusu Fransa olmakla beraber (Kelion, 2020) Danimarka, Çek Cumhuriyeti ve Slovakya da merkezî (centralised) sunucu altyapısına sahip filyasyon uygulamaları kullanmaktadır (Ciucci & Gouardères, 2020). Bu yöntemi kullanan uygulamaların en güçlü argümanları merkezî (centralised) bir sunucunun maruz kalma verisini çok hızlı analiz edip ikinci bir kontrol için sağlık uzmanlarının müdahalesine müsaade etmesi ve virüs yayılımı için daha etkili önlemler alabilme imkânı sağlamasını içermektedir. Örneğin, merkezî (centralised) bir sunucuda toplanan veri analiz edilerek virüsün yayılım ağı gözlemlenebilmekte ve bu yayılımdaki kritik düğüm noktaları tespit edilerek mikro seviyede önlemler alınabilmektedir. Yahut bazı kötü niyetli kullanıcıların anormal etkinlikleri tespit edilerek sistemin düzgün çalışması için müdahalelerde bulunulabilir (Downey, 2020). Ancak iOS işletim sistemi ile çalışan telefonların uygulama ekranda açık değilken bluetooth ile veri alışverişi yapmayı engellemesi sebebiyle pek çok ülke merkezî (centralised) uygulamalar yerine dağıtık (decentralised) altyapıyı kullanan "Maruz Kalma Arayüzü"nü kullanmaya mecbur bırakılmış durumdadır. (Busvine & Rinke, 2020; Iacoboni, 2020; O'Brien, 2020; Rinke & Busvine, 2020).

3. Verileştirme ve Mahremiyet: Veri Kimin Elinde?

Verileştirme imkânlarının hızla artması ile hayatın birçok alanı gözetim altına alınmaktadır. Birey, her geçen gün biraz daha "bireylikten" uzaklaşarak kitleleşmektedir (Han, 2017). Sosyal medya, internet ve akıllı cihazlar ile modern teknoloji, bir gözetim araçları koleksiyonuna dönüşmüş durumdadır. Teknoloji günümüzdeki birçok pratik problemi ortadan kaldırıyor olmasının yanı sıra, mahremiyetimizi tehdit eden en önemli unsurlardan biri olarak da karşımızda durmaktadır. Bazı platformlarda bireyin üzerinde uygulanan bu gözetim özgür iradeye bağlı olsa da

[6] Detaylı bilgi için: https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf

(sosyal medyada içerik üretimi gibi) bazı alanlarda özgür iradenin ikili tercihler sunularak sınırlandığını görmekteyiz. Nitekim bir makalesinde Tamar Sharon, insanların gözetim kültürünü nasıl benimsediklerini şu örnekle açıklamaktadır: 11 Eylül olaylarının ardından devletin terörist ataklarına karşı önlem almak için geliştirdiği gözetim ve denetim araçlarının insanların kullanımına "mahremiyet vs. güvenlik" dikotomisi ile sunulmuş olması, güvenlik için mahremiyetin kurban edilmesini meşrulaştırmıştır (Sharon, 2020). Günümüzde içinde bulunduğumuz Kovid-19 salgınına önlem olarak tasarlanan filyasyon uygulamaları da Sharon'a göre kullanıma, "mahremiyet vs. toplumsal sağlık" olarak bir ölçeğin iki zıt kutbu gibi sunulmaktadır ve bu dikotomi, tıpkı 11 Eylül olaylarındaki gibi insanları kısıtlı bir tercih yapmaya zorlamaktadır (Sharon, 2020).

Merkezî (centralised) sistemlerde lokasyon verisi yoluyla kimin kiminle, ne kadar süre bir arada bulunduğu bilgisi Sharon'un makalesinde gözetim kültürünün kriz anlarında görünür hâle gelmesinden ve bu anlarda hayata olan etkisinin artmasından bahsetmesini akıllara getirmektedir (Sharon, 2020). Gözetim araçları kriz döneminde ne kadar fazlalaştıysa kriz sonrası bu araçları kullanıma kapatmak da o kadar zorlaşmış demektir. Gözetim araçlarının fazla olması da bireyler arası güvensizliği artıran bir unsur hâline gelmiştir (Bauman, 2007). Nitekim Kovid-19 salgınının ilk döneminde içinde bulunduğumuz kriz durumunu değerlendiren sosyologların temel aldığı ortak bir konu da- dijital uygulamalar hususunda olmasa da- bu tarz kriz anlarında gözetimin norm hâline gelmesi olmuştur (Agamben, Giorgio; Benvenuto, S., 2020; Cristi, R. 2020).

Michel Foucault, Discipline and Punish kitabında 17. yüzyıldaki Büyük Londra Vebası'ndan verdiği örneklerle filyasyon uygulamalarının günümüzdeki kadar yaygın olmadığı dönemlerde uygulanan prosedürlerden bahsetmektedir (Foucault, 1995: 195). Salgını yönetmek adına hareket kısıtlamalarının getirildiği Londra'da, her bölgeye hükûmet memurları atanır ve bu hükûmet memurları bölgenin sokaklarında dolaşarak bireylerin kısıtlanmış hareketlerini takip eder. Tüm nüfusun isim, yaş, cinsiyet, adres ve sağlık durumu bilgilerini düzenli olarak kayda alınır (Foucault, 1995: 196). Bu hükûmet memuru; evlerin kapılarını dışarıdan kilitler, günün belli saatlerinde aile bireyleri belirlenen pencerenin önünde toplanır ve bu memura yoklama verirler. Foucault, toplumda kriz dönemleri haricinde de bu tür regülasyonların üstü kapalı bir şekilde bulunduğunu fakat kriz dönemlerinde bu regülasyonların yüzeye çıkarak özgürlükleri kısıtlayacak boyuta geldiğini Society Must Be Defended eserinde dile getirmektedir (Foucault vd. 2003: 244). Salgın döneminde artan bu düzenlemelerin, devletin toplumu disipline etme amacıyla gerçekleştirdiği bir gözetim olduğundan bahseden Foucault, bu yöntemlerle

devletin toplum üzerinde uyguladığı gücü artırmayı hedeflediğine değinir (Foucault, 1995: 201).

Kovid-19 salgınının başlangıcında İtalyan siyaset felsefecisi Giorgio Agamben, salgın hakkındaki yazısında Foucault'un Büyük Londra Vebası üzerinden gözetim kültürüne değinerek, günümüzde hükümetlerin insanları salgın sırasında disipline etme yollarıyla 17. yüzyıl veba salgınına karşı alınan tavır arasında bir benzerlik kurmuştur (Agamben; Benvenuto, 2020). Agamben, salgın zamanında devletin gündelik hayatın her alanına nüfuz eden düzenleme gücünü bedenleri disiplin etme ve gücü artırma amaçlı kullandığının üzerinde durur. Renato Cristi ise Agamben'in devlet-fobik olduğunu iddia etmiş ve ancak cumhuriyetçi bir yönetimin bireysel özgürlüklerden öte ortak iyiyi gerçekleştirmek adına toplumu salgına karşı yönetebileceğine güvenilebileceğinden bahsetmiştir (Cristi, Renato, 2020). Kovid-19 salgını etrafında tüm bu tartışmaları değerlendirirken çağımızın diğer çağlardan en önemli farklılığı olan dijitalleşmeyi de göz önünde bulundurmak gerekir. Zira bu dijitalleşme, 19. yüzyılın ilk çeyreğinde tartışılmaya başlanan filyasyon çalışmalarını (Demirtaş & Tekiner, 2020) gerçek hâle getirebilecek potansiyele sahip olmanın yanı sıra, tüm bunları yaparken Foucault'un vebasındaki gibi bireylerin hareketlerini sınırlandırmama açısından büyük bir imkân sağlamaktadır. Hayata gelen her bir yenilik, yeni sorunları da devreye sokar. Nitekim tüm bu avantajların yanı sıra dijitalleşme, ortaya çıkan kitlelerin verisinin kime ait olacağı sorusunu meydana getirmektedir ve bu soru da meseleyi tekrardan gözetim kültürüne döndürmektedir.

Devletin, salgın döneminde, "bedenleri" iyileştirmek adına tasarlanan bu uygulamalar aracılığıyla verileştirmesi, akıllara Foucault'un biyopolitika kavramını getirmektedir. Bu kavramı Foucault şu cümlelerle açıklamaktadır: "Biyopolitika kavramı, 18. yüzyıldan başlayarak bir nüfus oluşturan birtakım yaşayan canlıların süreçlerine özgü karakteristik fenomenler aracılığıyla (sağlık, hijyen, doğum oranı, yaşam beklentisi, ırk gibi) iktidar uygulamalarından kaynaklı sorunları rasyonalize etmektir" (Foucault vd. 2008: 317). Modern devletin "bedeni" sağlığına kavuşturma iştiyakı, bedenin "gücünün eksilmesinin, çalışma süresinin azalmasının, enerjisinin düşüşünün, üretimdeki eksik kadar bunun mal olabileceği tedavilerin de yol açtığı ekonomik maliyetlerin" önüne geçmek adına ortaya çıkar (Foucault, 2011: 249). Foucault, 17 ve 18. yüzyıllarda bedene yoğunlaşan disiplin edici gücün tür-olarak-insan üzerinde düzenleştirici bir güce dönüşerek gözetim, hiyerarşi, dokümantasyon ve raporlar aracılığıyla hâkimiyeti altındaki iş gücünü kontrol etmesine dikkat çekmektedir (2003:242). Bu düzenleştirici güç, nüfusu odak noktasına alarak bir homeostazi kurmayı hedeflemektedir (2011: 252). Nüfus bir dengeye ulaşmalı ve denge çizgisinden uzaklaşanlar tekrardan o çizgiye denklenmelidir. Modern devletin "yaşatma ve ölüme bırakma"

iktidarıyla ölüm, doğum hızlarını kontrol etme isteğinin en önemli izdüşümü, sağlık alanındaki gelişmelerde görülmektedir (Foucault vd. 2003 : 245). Bu gelişmeler, bedenleri sağlıklı tutarak onları yaşatmak ve iş gücünden faydalanmak adına yapılan disiplin edici güçlerdir.

Tür olarak insanın disipline edilmesinde, istatistik ve nüfus bilim gibi alanlar ön plana çıkmaktadır (2011: 249) ve bu düzenleştirici süreç belli bir oranda gözetimi gerekli kılmaktadır. Zira istatistik ve demografi, konu üzerine veri toplanmadan sürdürülebilir alanlar değildir. Bu da günümüz terimlerince, öznenin verileştirilmesinin (quantified self) bir disiplin aracı olduğunu göstermektedir (Ajana, 2017).

Biyopolitika kavramı dikkate alındığında, iktidarların Kovid-19 salgınında öznelerin çeşitli yasaklamalar ve maske kurallarıyla sağlıklarına, teknolojik gelişmeleri kullanarak takip uygulamalarıyla sosyal mesafelerine bu denli dikkat etmeleri ve özen göstermeleri garip karşılanmayacaktır. Zira güç, disiplin edici ve düzenleştirici olarak kullanılır (2011: 254), disiplin edemediği yerde özneyi cezalandırır. İktidarın bu disiplin edici gücü, hemen göze çarpmayan, rasyonel gözüken mekanizmalarda (sigorta, güvenlik araçları, şehir planlaması vs.) görülürken, kriz anlarında bu biyopolitika, üstü kapalılığını kaybeder ve açıkça beden üzerine disipline ediciliğini gösterir (Marwick, 2012). Nitekim Kovid-19 salgını da bir kriz durumu olarak kabul edildiği durumda, salgın sürecinde biyopolitikanın yaşam üzerindeki etkisinin daha belirgin olduğunu görmek mümkün olacaktır.

Günümüzde devlet bazlı Kovid-19 takip uygulamalarında göze çarpan bu disiplin edicilik ve gözetim, Foucault'un bahsettiği gibi normal zamanlarda gözlerden ırak olan biyopolitikasının yüzeye çıktığı anlardan biri olarak görülebilir. Kişi takip uygulamalarında temaslı veya pozitif olarak işaretlendiğinde hareketinin kısıtlanacağının farkında olduğundan kendini korumaya özen gösterecektir, nitekim bu özen, uygulamaların disiplin edici tarafını gözler önüne sermektedir. Bu özenin salgın açısından gerekliliğinin ötesinde farklı bir açıdan bakıldığında, uygulamaların topladığı lokasyon verisinin kişinin gideceği yerleri seçerken titiz olmasına sebep olması da mümkündür. Zira lokasyon verisi, birey üzerinde bir gözetim oluşturulabilmesi uygun bir platform oluşturmaktadır. Normal zamanlarda gözle görülemeyen biyopolitikanın yüzeye çıktığında, bireyde gözetim altında hissetmekten kaynaklanabilecek devlete karşı bir güvensizlik oluşturduğu, bu güvensizliğin aynı zamanda dijital Kovid-19 uygulamalarının topladığı verilerin oluşturduğu mahremiyet tartışmaları üzerinden de açığa çıktığı görülmektedir.

Kovid-19 temas takip uygulamalarında verinin kime ait olacağı tartışması, tasarlanan uygulamaların bazılarında lokasyon verisinin de toplanması ve toplanan

bu verilerin nasıl kullanılacağı konusundaki belirsizlik, uygulamalara olan genel güvensizliğin sebepleri olarak sayılabilir. Kovid-19 temas takip uygulamalarına güvenmemek, şayet Nguyen'in makalesinde bahsettiği veri okuryazarlığına sahipsek, yerinde olacaktır (2020). Zira Nguyen, toplumun verileştirmeyi kritik edebilecek, fayda ve zararlarını fark edip önlem alabilecek bir oranda veri okuryazarlığına acil bir şekilde sahip olması gerektiğinden bahseder (Nguyen, 2020). Fakat bireylerin birçok özel şirketin (Althusser'in İdeoloji ve Devletin İdeolojik Aygıtları kitabında bahsedilen consent kavramı ile) onların kendi rızasıyla topladığı verilerinin günümüze kadar farkında olmamış ve önlem almamış olduğu düşünüldüğünde, Kovid-19 takip uygulamalarının topluma sunduğu mahremiyet vs. toplum sağlığı gibi kısıtlı bir tercihte gizliliği tercih etmesinin yersiz olacağı tartışılabilir.

Özel şirketlerin topladığı verinin devletin topladığından daha az tehlikeli görünmesi, tehlikeli olmadığına işaret olmayabilir. Zira özel şirketlerin temel misyonu kâr maksimizasyonudur. Bireyleri verileştirme de bu şirketlerin bireylerin yönelimlerini keşfeden algoritmalar yoluyla reklamlarını geliştirmelerini sağlayan önemli bir kâr artırma yoludur. İnsanın bir veriye indirgenerek verileştirilmesi ve bu verinin ise başka bir şey pazarlamak için metalaştırılmasını tartıştığımız günümüzde, politik ekonomiyi Marksist bir bakış açısıyla kritik eden sosyologlar, verinin bir sermaye hâline geldiğinden ve bu verinin elde edilmesinin ise gözetim ekonomisi ile gerçekleştiğinden bahsetmektedirler (Couldry & Mejias, 2019; Fuchs, 2011; Hughes & Southern, 2019). Fuchs, bu gözetim ekonomisini anlatırken Google'ın bir panoptikon gibi inşa olarak insanları gözetlediğini ve onların bilgilerini metalaştırma yoluyla çalıştığını söyler. Google, hayatın birçok alanında bireyleri ve onların internet üzerinde yaptıkları tercihleri gözeterek insanlar hakkında veriler toplar. Sonra bu verileri metalaştırma stratejileri belirler. Bu anlamda, Google insanların kendi rızalarıyla verilerini ücretsiz olarak vermelerini sağlayarak onları daima sömürmektedir.

Couldry & Mejias ile Fuchs, özel şirketlere veri üreten bireyin ücreti ödenmeyen bir iş gücü olduğunu söylemektedir (Couldry & Mejias, 2019; Fuchs, 2011). Bireylerin bu veri üretimini kendi rızalarıyla yapıyor oluşları ve verileştirmeye rıza göstermeleri akıllara Althusser'in "kültürel hegemonya" kavramını getirmektedir. Zira bu bağlamda, bireyler şirketlerin kâr yapmaları için ücretsiz çalışan fakat şirketlerin kendilerinin faydaları için çalıştıklarına inanan işçiler gibidir. Bu sömürü döngüsünü durdurmanın en önemli yolunun da bireylerin bilinçlenmeleri olacağı söylenebilir.

Bu bağlamda, 18. yüzyıl sonundan bu yana sermaye olarak iş gücü, yerini 21. yüzyılda veriye bırakmıştır denilebilir. Bu sermayeleştirme iddiası sonrası verinin

kime ait olduğu sorusu ortaya çıkmaktadır. Erken kapitalizmde iş gücü işçiye aittir, sözü ne kadar sorgulanabilir ise bugün veri bireye aittir, demek de aynı ölçüde sorgulanabilir. Bu konuda sahipsiz toprağın (no man's land) sömürülmeye açık bir toprak olduğu vurgusunu yapan Julie Cohen, verinin kimseye ait olmadığı iddiasının veriyi sömürülmeye açık hâle getirdiğinden bahseder (Cohen, 2018) ve bu sömürülme de veri kolonyalizmi mefhumu altında kavramsallaşmaktadır. Couldry ve Mejias, veri kolonyalizmi hakkında şunları söylemektedirler: "Sürekli takip edilebilen yaşam, nereden bakılırsa bakılsın, mülksüzleştirilmiş bir yaşamdır. Bu mülksüzleştirmeyi kabul etmemek, veri sömürgeciliğine karşı direnişin başlangıcıdır" (Couldry & Mejias, 2019:8).

Sonuç olarak, normal hayatta şirketlere gösterdiğimiz tam güveni sorgulamadan devlete güvensiz bir tutum göstermek makul olmayacaktır denilebilir. Zira ne devlet ne de özel şirketler ortak iyi için çalışırlar ve bu durumda vatandaşların/müşterilerin bilinçli ve eleştirel bir tavırla karşılarına gelen teklifleri değerlendirmesi yerinde olacaktır. Bireysel tutarlılığı korumak adına, 'normal' hayatta sorgulamadan izin verilen özel şirket "hüküm ve koşullarını" dikkate alarak, biyopolitikanın yüzeye çıkıp belirginleştiği vakitlerde de devlete bireyi verileştirmesi hususunda izin verip vermemenin gözden geçirilmesi gerekmektedir.

4. Sonuç

Bu makale, merkezî (centralised) ve dağıtık (decentralised) sistemlerin yapısını, işlevlerini ve limitasyonlarını ele almakla beraber, bu sistemleri üreten aktörlere karşı oluşabilecek güvensizlik konularını da tartıştı. Merkezî (centralised) sistemlerin risk takip sürecini hızlı işletebilmesi açısından, Kovid-19 tanısı koymayı ve filyasyon uygulamasını kolaylaştırıcı bir etkiye sahip olmasının yanında veriyi bir güç olarak ele alırsak gücü dağıtmak yerine, tek bir aktörde toplaması tehlikesi üzerine konuşmak da önem arz ediyor. Fakat bu noktada, gücün tekelleşmesinin zararının mutlaklığı tartışılabilir. Zira Bauman ve Lyon "Akışkan Gözetim" kitabında böyle bir iddianın neden kaçınılası olduğunu şu cümlelerle anlatırlar: "Günlük hayatlarımızla ilgili bilgiler bizi gözetleyen kurumlar için şeffaflaştıkça onların kendi faaliyetlerini anlamak daha da zorlaşıyor… Gelgelelim, burada bir komplonun varlığı şöyle dursun, kasıt bile olmayabilir. Yeni gözetimin saydam olmayışı kısmen onun teknik karakteriyle ve organizasyonlar içinde ve arasındaki karmaşık veri akışıyla ilgilidir. Kısmense, ulusal güvenliği veya ticari rekabeti çevreleyen gizlilikle" (2020:24).

Fakat dikkat edilmelidir ki ister veri olarak ister ekonomik hedeflerle olsun, gücün tekelleşmeye bir eğilimi vardır. Gözetim araçlarının çoğunu elinde bulunduran

aktör, kısa sürede hepsine sahip olabilir. Tüm bunlardan hareketle dağıtık (decentralised) sistemlerin mahremiyeti koruma adına daha çok tercih edilebilir olduklarını söylemek gerekmektedir.

Dağıtık (decentralised) modellerde birinci kısımda bahsedilen limitasyonlarının ötesinde, gücün dağıtılmış ve bir aktörde toplanmıyor olması, kullanıcıya mahremiyetinin korunacağına dair güven verebilmektedir. Günümüzde dağıtık (decentralised) modelin kullanıldığı en büyük örnek, Google ve Apple gibi iki teknoloji şirketinin ortak olarak tasarladıkları "Maruz Kalma Arayüzü"dür. Bu iki şirketin, sistemi bir arayüz olarak tasarlamaları ve devlet uygulamalarına belli şartlar getirerek devleti de Kovid-19 salgınına teknolojik önlemler kapsamına almaları, makalenin ikinci kısmında sunulan ortak iyiyi hedefledikleri izlenimini veriyor. Bu sistem için dağıtık (decentralised) verinin Google ve Apple ile paylaşılmıyor olması bu veri ile bir reklam optimizasyonu yapılamayacağını da göstermiş oluyor ve bu da Google ve Apple'ın ikinci kısımda bahsedilen özsel özel şirket maslahatından bu mesele özelinde vazgeçtiğini gösterebilir. Kâr maksimizasyonu hedefi bulundurmayan, devletlerin virüsle mücadelelerinin yerini almaya değil de destek olmaya çalışan ve veriyi bireysel cihazlarda biriktiren bu sistem kullanıcıların mahremiyeti için birçok avantaj sağlamakta ve kullanıcıyı ortak iyinin hedeflendiğine dair birçok noktada ikna edebilmektedir.

Bu avantajların dışında dikkate alınması gereken bir diğer mesele ise bu API'nın dünyada gelmiş geçmiş en büyük blok zincirlerden birini teşkil ediyor olmasıdır. Bu açıdan, Kovid-19 salgını, dünya nüfusunun büyük bir kısmının tek bir API ile kontrol edilebilirliğini gösterecek bir deney ortamı olarak görülebilir. Bu nedenle, "Maruz Kalma Arayüzü", bu şirketlerin kitlesel gözetim vizyonunun kanıtlanması açısından muazzam bir öneme sahiptir. Kovid-19 salgınının, bu şirketlerin gelecek planları için ortak iyiyi hedeflemek kılıfıyla dünyayı tek bir API'da birleştirmeyi denemek adına uygun bir test ortamı sağlamış olduğu iddia edilmesi gayet mümkündür. Kısacası, kullanıcıların mahremiyetini önemsemesi ve reklam optimizasyonu gibi kâr getirecek bir uygulamayı reddetmesi bu API sunucularının salt ortak iyiyi hedefledikleri için yeterli bir gerekçe sunmamaktadır.

Başka bir açıdan, bu özel şirketlerin tasarlanan diğer filyasyon uygulamalarına nazaran kullanıcının mahremiyetini önemsiyor olmasını ortak iyiyi hedefledikleri hakkında bir hüküm çıkarmadan önce, bu mahremiyeti neden önemsedikleri sorusunu da akıllarda bulundurmak gerekir. Zira bireylerin dijital alanda mahremiyetlerini korumak için hassasiyetleri artmasaydı acaba bu şirketler filyasyon uygulamasını tasarlarken bireyin mahremiyetine dikkat ederler miydi? Bu soru, muhatabını Nguyen'in Kovid-19 salgını döneminde hızla artan verileşmeye karşı-

lık, veri okuryazarlığının acilen yaygınlaştırılması gerektiğini ifade ettiği yazısına yönlendirmektedir (Nguyen, 2020).

Sonuç olarak Google ve Apple API, mahremiyet konusunda salt devletin veya salt şirketin oluşturabileceği bir kriz yönetiminden daha büyük bir güveni kazanabilme konusunda önemli bir adım atmıştır. Fakat bu API sistemini salt ortak iyiyi hedef alarak mı tasarlamıştır sorusu akıllarda takılı kalmıştır ve kalmalıdır.

Teşekkür

Makalenin gelişiminde destekleri için Uğur Özdemir, Hiba Irmak, Abdullah Çiftçi ve Furkan Tektaş'a teşekkür ederiz. Ayrıca Sıla Sena Çelebi'ye makalenin editörlüğünü de yaptığı için teşekkür ederiz.

Kaynakça

Agamben, Giorgio; Benvenuto, S. (2020). Coronavirus and philosophers. European Journal of Psychoanalysis.
https://www.journal-psychoanalysis.eu/coronavirus-and-philosophers/

Ajana, B. (2017). Digital health and the biopolitics of the Quantified Self. DIGITAL HEALTH, 3, 2055207616689509. https://doi.org/10.1177/2055207616689509

Apple and Google partner on COVID-19 contact tracing technology. (t.y.). Apple Newsroom. Geliş tarihi 19 Ocak 2021, gönderen https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Bauman, Z. (2007). Liquid Times: Living in an Age of Uncertainty. Polity.

Bian, S., Zhou, B., & Lukowicz, P. (2020). Social Distance Monitor with a Wearable Magnetic Field Proximity Sensor. Sensors, 20(18), 5101. https://doi.org/10.3390/s20185101

Busvine, D., & Rinke, A. (2020, April 22). Switzerland, Austria align with 'Gapple' on corona contact tracing. Reuters.
https://www.reuters.com/article/health-coronavirus-europe-tech-idUSL3N2CA36L Ciucci, M., & Gouardères, F. (2020). National COVID-19 contact tracing apps (BRIEFING
PE 652.711; ITRE in Focus, p. 9). Policy Department for Economic, Scientific and Quality of Life Policies. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_BRI(20 20)652711

Cohen, J. E. (2018). The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy. Philosophy & Technology, 31(2), 213–233. https://doi.org/10.1007/s13347-017-0258-2

Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. Television & New Media, 20(4), 336–349. https://doi.org/10.1177/1527476418796632

Cristi, Renato. (2020). Pandemics and Philosophy. European Journal of Psychoanalysis. https://www.journal-psychoanalysis.eu/pandemics-and-philosophy/

Demirtaş, T., & Tekiner, H. (2020). Filiation: A Historical Term the COVID-19 Outbreak Recalled in Turkey. https://doi.org/10.14744/etd.2020.54782

Downey, A. (2020, April 29). NHSX differs with Apple and Google over contact-tracing app.
https://www.digitalhealth.net/2020/04/nhsx-differs-with-apple-and-google-over-contact-tracing-app/

Foucault, M., Davidson, A. I., & Burchell, G. (2008). The Birth of Biopolitics: Lectures at the Collège de France, 1978-1979. Palgrave Macmillan UK.

Foucault, Michel. (1995). Discipline and Punish: The Birth of the Prison. Vintage Books.

Foucault, Michel, Bertani, M., Fontana, A., Ewald, F., & Macey, D. (2003). Society must be defended: Lectures at the Collège de France, 1975-76 (1st ed). Picador.

Foucault, Michel. (2011). Toplumu Savunmak Gerekir. Yapı Kredi Yayınları.

Fuchs, C. (2011). A Contribution to the Critique of the Political Economy of Google. Fast Capitalism, 8(1).

Han, B.-C. (2017). In the Swarm: Digital Prospects. MIT Press.

Hughes, C., & Southern, A. (2019). The world of work and the crisis of capitalism: Marx and the Fourth Industrial Revolution: Journal of Classical Sociology. https://doi.org/10.1177/1468795X18810577

Iacoboni, J. (2020, Mayıs 1). Is it Safe? The Immuni App: Digital Surveillance during the Coronavirus Pandemic. Byline Times.
https://bylinetimes.com/2020/05/01/is-it-safe-the-immuni-app-digital-surveillance-during-the-coronavirus-pandemic/

Kelion, L. (2020, Nisan 27). NHS rejects Apple-Google coronavirus app plan. BBC News. https://www.bbc.com/news/technology-52441428

Kelion, L. (2020, Nisan 21). Coronavirus: Apple and France in stand-off over contact-tracing app—BBC News. https://www.bbc.com/news/technology-52366129

Marwick, A. (2012). The Public Domain: Surveillance in Everyday Life. Surveillance & Society, 9(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Mobile OS market share 2019. (t.y.). Statista. Geliş tarihi 19 Ocak 2021, gönderen https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

Nguyen, D. (2020). Mediatisation and datafication in the global COVID-19 pandemic: On the urgency of data literacy. Media International Australia, 1329878X20947563. https://doi.org/10.1177/1329878X20947563

O'Brien, C. (2020, Nisan 29). HSE Covid-19 tracing app data will be stored on individual devices. The Irish Times.
https://www.irishtimes.com/business/technology/hse-covid-19-tracing-app-data-will-be-stored-on-individual-devices-1.4240304

Rinke, D., & Busvine, A. (2020, Nisan 26). Germany flips to Apple-Google approach on smartphone contact tracing. Reuters.
https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J

Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. Ethics and Information Technology, 1–13. https://doi.org/10.1007/s10676-020-09547-x

Stanley, J., & Callas, J. (t.y.). Tracking Apps are Unlikely to Help Stop COVID-19. American Civil Liberties Union. Geliş tarihi 19 Ocak 2021, gönderen https://www.aclu.org/news/privacy-technology/tracking-apps-are-unlikely-to-help-stop-covid-19/

Vincent, J. (2020, May 5). Without Apple and Google, the UK's contact-tracing app is in trouble. The Verge. https://www.theverge.com/2020/5/5/21248288/uk-covid-19-contact-tracing-app-bluetooth-restrictions-apple-google

Yang, D., Yurtsever, E., Renganathan, V., Redmill, K. A., & Özgüner, Ü. (2020). A
Vision-based Social Distancing and Critical Density Detection System for COVID-19.
ArXiv:2007.03578 [Cs, Eess]. http://arxiv.org/abs/2007.03578

York, S. W. and J. C. (2020, June 17). Almanya'nın Corona-Warn-App Uygulaması: Sık Sorulan Sorular (Ahmet Alphan Sabancı, Trans.). Electronic Frontier Foundation. https://www.eff.org/tr/deeplinks/2020/06/germanys-corona-warn-app-frequently-aske d-questions