

Küresel Salgın Döneminde Kişisel Veriler ve Temas Takip Uygulamaları

Prof. Dr. Mustafa ALKAN

T.C. Gazi Üniversitesi, Ankara, Türkiye, alkan@gazi.edu.tr

Mehmet Ali İNCEEFE

Accert A.Ş., Ankara, Türkiye, mehmetali.inceefe@accert.com.tr

ÖZ

Dünya, hiç beklemediği bir anda küresel bir salgınla karşılaştı. Önce anlamakta, sonra da önlem almada gecikti. En hızlı ve etkin tedbirleri alan Çin, Kore, Singapur gibi ülkeler, teknolojiyen de yararlanarak kısa zamanda salgını yavaşlatarak biraz da olsa eksikliklerini tamamlamayı başardılar.

Başvurulan teknolojik yöntemlerin başında mobil uygulamalar, CCTV ve termal kameralar ile mobil şebekelerden elde edilen konum verileri gelmektedir. Kişisel veriler ve mahremiyet, bir salgın döneminde kişilerin yaşam mücadelesi verirken, toplumsal öncelikler açısından tartışma yaratan konuların başında geldi. Covid-19 virüsünün bulaştığı kişileri ve bu kişilerle bulaşmayı artıracak biçimde temasta bulunan kişilerin belirlenmesi hem bu kişilerin hem de toplumun diğer kesiminin sağlığı açısından çok önemlidir.

Bu çalışmada, salgın ve benzeri dönemlerde kullanılan temas takip çalışmalarını, bu çalışmaların mobil uygulamaya yansımaları ile ülke bazında ve dünya genelinde geliştirilen uygulamalar ve tartışmalar incelenip, kişisel verilerin korunması açısından artı ve eksileri değerlendirilecektir.

Anahtar Kelimeler: Salgın, Pandemi, Temas Takip, Bluetooth, Mobil Uygulama, Konum Verileri, Kişisel Veri Koruma

Personal Data in the Pandemic and Contact Tracing Applications

ABSTRACT

The world has unexpectedly faced a global epidemic. First, it was hard to understand and then late to take an action. Countries such as China, Korea, Singapore, which took the fastest and most effective countermeasures against the pandemic, have successfully managed to complete their deficiencies, by slowing down the epidemic in a short period of time by taking advantages of the technology.

Data from mobile networks, mobile applications, CCTV and thermal cameras are the leading technological incomes in this fight. Personal data and privacy are among the topics that create controversy in terms of social priorities while struggling for life in epidemic.

In this paper, the contact tracking applications used in epidemic and similar periods, reflections of these studies on mobile technologies, applications and arguments on the basis of the country and worldwide are being discussed, and pros and cons of mobile contact tracing applications are being evaluated from the data protection perspective.

Keywords: Pandemic, Contact Tracing, Bluetooth, Mobile Applications, Location Data, Data Protection

GİRİŞ

2019 yılı sonlarında Çin’de belirlendikten sonra hızla yayılan Covid-19 salgını, 1-2 ay içerisinde tüm dünyayı etkilemiş ve yayılma hızındaki olağandışı artış ile bütün ülke ve kurumları çeşitli önlemlere zorlamıştır. Önce okul ve çeşitli iş alanlarında fiziki faaliyetler durduruldu. Daha sonra insan hareketleri sınırlandırılmaya başladı. Covid-19 salgınının neden olduğu kriz, sağlık sistemlerini, yaşam tarzını, ekonomik istikrarı ve bütün değerleri eşi görülmemiş bir zorluk ile karşı karşıya bırakmıştır. [1]

Devletler tarafından ilk başvuru önlemler; geniş sokağa çıkma yasakları, işyerlerinin kapatılması, kamusal alanlar ve kurumlar, enfekte olmuş bireylerin izolasyonu için zorunlu ve gönüllü sosyal mesafe talepleri dâhil karantinalar ve kısıtlamalar olmuştur. Özellikle kişilerin teması ile çok hızlı bir biçimde yayılan bu salgında, enfekte olan kişilerin ve bu kişilerin yakın zamanda temasta olduğu diğer kişilerin belirlenmesi, salgının izlenip kontrol altına alınmasındaki en etkili yöntemlerden birisi olmuştur.

Bu salgınla mücadelede geleneksel önlemlerin yeterli olmadığı görülünce değişik yöntemlere ve teknolojiler başvurulmaya başlandı. Bunların başında, kısıtlamaları ihlal eden kişileri tanımlamak için konum verilerini kullanan bir uygulama yüklemeye teşvik ederek veya zorlayarak, bu kısıtlamalara uyumu izlemek için mobil konum verilerinin kullanımı gelmektedir.

Temas takibi, özünde “*enfekte olmuş bir kişiyle temas etmiş olabilecek kişileri tanımlama sürecidir. Enfekte olmuş biriyle yakın temas halinde olan (10 dakika veya daha uzun bir süre içinde 2 m veya daha yakınında) kişilerin hızla tanımlanarak bulaşmanın engellenmesi*” hedeflenmektedir. [2]

Tüm dünyada olduğu gibi ülkemizde de, salgını yavaşlatmak ve önüne geçip durdurmak için, temas takip uygulamaları ilk hayata geçirilen önlemler arasında hatta başında yer aldı. Konum izleme, temas takibi gibi insanların uzun süredir endişe duydukları gözetim türleri, bir salgında hastalığın yayılmasını izleme ve önlemede kesinlikle fayda sağlayabilir. Bu tür uygulamaların genişletilmesi, normal şartlar altında kabul edilecek ve desteklenecek bir durum olmamakla birlikte, bir salgında daha az sayıda insanın enfekte olmasını ve salgının yayılmasını azaltmak için bu tür kişisel verilerin kullanılması birçok hayatı kurtarmaktadır.

Özellikle konum, sağlık bilgisi ve benzeri kişisel verilerin kullanıldığı bu temas takip uygulamaları bir dizi tartışmayı da beraberinde getirmiştir. Çeşitli veri koruma otoriteleri ve sivil toplum kuruluşları, kişisel verilerin bu salgın sırasında daha etkin yararlanılmasına ilişkin kuralların mahremiyetin korunmasından da taviz verilmeden kullanılması için daha fazla görüş ve değerlendirmeler üretmeye başlamışlardır.

TEMAS TAKİBİ

Dünyadaki birçok insanın mobil cihazlarla internete bağlı olduğu düşünüldüğünde, dijital teknolojilerin ve verilerin salgınla ilgili mücadelede önemli bir rolü vardır. Bu teknolojiler ve veriler, başta ilgili kamu kurum ve kuruluşları olmak üzere, sağlık kuruluşlarının virüsün yayılmasını kontrol altına almak için önemli bir araçtır. Aynı zamanda halkın bilgilendirilmesi, sağlık verilerinin işlenmesi ve temaslı kişilerin izlenmesi açısından büyük öneme sahiptir.

“Avrupa’daki birçok insanın mobil cihazlarla internete bağlı olduğu düşünüldüğünde, dijital teknolojilerin ve verilerin Covid-19 kriziyle mücadelede önemli bir rolü vardır. Bu teknolojiler ve veriler, halkı bilgilendirmek ve ilgili kamu makamlarına virüsün yayılmasını kontrol altına alma çabalarında veya sağlık kuruluşlarının sağlık verileri alışverişinde bulunmalarına yardımcı olmak için önemli bir araç sunabilir.” [3]

Bu kapsamda geleneksel salgın izleme yöntemlerinin yanında özellikle mobil teknolojiler belirgin bir biçimde öne çıkarken, temas takibi için mobil uygulamalar geliştirilmiş, Apple/Google iş birliğinde kişilerin yakın temas ve hareket bilgilerinin izlenebilmesine yönelik arayüz (API) geliştirilmiş ve

özellikle mobil işletmeciler tarafından anonim ve birleştirilmiş kitle hareket bilgileri sağlanmaya başlamıştır.

Birçok ülke, mobil şebekelerden edinilen coğrafi konum verileri ile tren, havayolu veya otoyol verilerini kullanarak insanların hareket biçimlerini anlayıp, bu hareket ile salgının yayılması arasındaki ilişkileri belirleyip, hızlı önlemler almıştır. Özellikle, mobil uygulamaların kullanımlarının zorunlu tutulması salgının kontrol altına alınmasında önemli bir rol oynadı.

Temas Takibinin Amacı

Temas takip uygulamalarının amacını genel olarak aşağıdaki şekilde belirleyebiliriz.

- Devam eden bulaşmayı kesmek ve bir enfeksiyonun yayılmasını azaltmak,
- Enfeksiyon olasılığına karşı temasları uyararak ve önleyici danışmanlık sunmak,
- Zaten enfekte olmuş kişilere tanı, danışmanlık ve tedavi sunmak,
- Enfeksiyon tedavi edilebilirse, ilk olarak enfekte olmuş hastanın yeniden enfeksiyonunu önlemeye yardımcı olmak,
- Belirli bir popülasyondaki bir hastalığın epidemiyolojisi hakkında bilgi edinmek.

Avrupa Hastalık Denetim ve Önleme Merkezi (ECDC) temas takibinin amacını;

Muhtemel veya doğrulanmış Covid-19 vakalarının temaslarının tanımlanmasının ve yönetilmesinin amacı, bulaşmaya müdahale etmek ve ilerideki bulaşmayı kesintiye uğratmak için birincil bilinen vakalardan bulaşışından sonra ortaya çıkabilecek ikincil vakaları hızla tespit etmektir. Bu, şu şekilde gerçekleştirilir:

- *Olası veya doğrulanmış bir Covid-19 vakasının temaslarının hızlı bir şekilde tanımlanması;*
- *Kişilerin kendi kendine karantina, uygun el hijyeni ve solunum görgü kuralları önlemleri ile ilgili bilgilerle ve semptom geliştirmeleri halinde ne yapılması gerektiği konusunda tavsiyelerde bulunarak;*
- *Semptomları olan herkes için zamanında laboratuvar testi.*

Temas takibi, aktif vaka bulma ve test etme ile birlikte ve fiziksel mesafe gibi diğer önlemlerle sinerji içinde devam eden Covid-19 salgınıyla savaşmak için gerekli bir önlem

olarak tanımlanmaktadır.[⁴]

SALGIN VE KİŞİSEL VERİLER

Temas takip uygulamalarının kullanımı kişisel veriler ve mahremiyet açılarından ciddi tereddüt ve endişeleri gündeme getirmiştir;

- Gönüllülük esasına göre yükleme
- Telefon, konum ve diğer kişisel verilerin kullanılmaması
- Kişisel verilerin başka amaçlarla kullanılmaması
- Erişimin kısıtlanması
- Kodların açık olması/yayınlanması
- Salgın sonrası tüm kişisel verilerin silinmesi.

Bu konuda Avrupa Veri Koruma Kurulu (EDBP) 21.Nisan.2020 tarihinde oldukça kapsamlı bir görüş ve rehber hazırlayıp yayınladı. [⁵]

Dünya çapındaki bu endişeleri gidermeye yönelik, toplanan bilgilerin isimleri veya diğer kişisel bilgileri açığa vurmayacağına ve kriz sona erdiğinde silineceğine yönelik ifadeler kullanılmaktadır. 200 akademisyen tarafından yazılan bir mektupta, herhangi bir uygulama geliştirmede güvenlik ve gizlilik, şeffaflık ve dağıtık veri saklama tabanlı uygulamaların kullanılmasını önerilmektedir.

Diğer yandan Fransa kişisel verilerin anonimleştirileceğini, bu uygulamaların geçici olup, salgın süresi sonunda kullanımdan kaldırılacağını, Avustralya ise uygulamanın kaynak kodunun da bağımsız inceleme için yayınlanacağını belirtmişlerdir.

Çeşitli çevrelerce Apple ve Google tarafından geliştirilen çözümün işlevselliğinin özelliklerine uygun olduğundan emin olmak için kodlarının dış denetimine izin verilmesi talep edilmektedir.

Ayrıca, bu işlevselliği işletim sistemlerine uygulayarak daha geniş bir Bluetooth tabanlı temas takip platformu sağlamaktır. Bu çabada gizlilik, şeffaflık ve rıza son derece önemli olup ilgili paydaşlarla istişare ederek geliştirmesi için bu şirketler tarafından yapılacak çalışmaların uzmanların incelemesine açık olacağı belirtilmektedir.

Apple ve Google bu çözüme yönelik olarak, yalnızca hükümet sağlık yetkililerinin uygulama oluşturması, tüm uygulamaların “*Maruziyet Bildirim (Exposure Notification) APT*”sını kullanmadan önce kullanıcı rızası alması ve pozitif test sonuçlarını ve “tanı anahtarlarını” halk sağlığı yetkilileri ile paylaşmadan önce kullanıcıdan ikinci bir rızanın alınması, en az verinin toplanması ve sadece sağlık müdahalesi için kullanılması şartını koşmaktadır. Apple ve Google ayrıca, sağlanacak verilerin hedefli reklamcılık veya polisie amaçlarla kullanımları yasaklamaktadır.

TEMAS TAKİP YÖNTEMLERİ

Kişilerin teması ile çok hızlı bir biçimde yayılan bu salgında, enfekte olan kişilerin ve bu kişilerin yakın zamanda temasta olduğu diğer kişilerin belirlenmesi, salgının izlenip kontrol altına alınmasındaki en etkili yöntemlerden birisidir.

Temas takibi, çok basit görünmekle birlikte oldukça karmaşık ve çok fazla kaynak gerektiren bir süreçtir. Temas takibi ağırlıklı emek yoğun ve manuel bir işlemdir. Temas takibi genel halk için nispeten yeni bir kavram gibi görünse de bu uygulama sağlık yetkilileri tarafından on yıllardır çeşitli bulaşıcı hastalıkları önlemek için, iletim noktalarını özenle belirleyerek ve topluma yayılmasını yavaşlatmak amacıyla kullanılmaktadır.

Ancak Covid-19 virüsünün olağandan farklı ve kolay bulaşıcılığının neden olduğu salgınla mücadelede geleneksel önlemler tek başına yetersiz kalmış ve vaka yönetimi, uyarı otomasyonu ve ağ analitiği gibi teknolojik tabanlı değişik yöntemlere başvurulmuştur.

Vaka temelli bir müdahale yaklaşımı (*verem, kızamık, cinsel yolla bulaşan enfeksiyonlar ve Ebola gibi hastalıklar için rutin olarak kullanılır*), Covid-19 için her toplumda hızlı teşhis testlerinin büyük bir genişlemesini halk sağlığı iş gücünde benzeri görülmemiş bir büyüme ve vaka tanımlama ve temas takibine adanmış yeni teknolojilerin benimsenmesini birleştiren yeni bir ulusal girişim olmadan başarılması imkânsız olacaktır. [6]

Bu kapsamda geleneksel salgın izleme yöntemlerinin yanında özellikle mobil teknolojiler belirgin bir biçimde öne çıkarken, insan tabanlı manuel takip yöntemler yanında 3 temel yöntem benimsendi;

- Mobil işletmecilerin sağladıkları anonim ve birleştirilmiş hareket bilgileri
- Temas takibi için geliştirilen mobil uygulamalar
- Apple/Google iş birliğinde geliştirilen küresel hareket verileri arayüzü.

Gerek dijital gerekse manuel herhangi bir temas takip çalışmasının başarısı yapılacak testlere bağlıdır. Enfeksiyon testlerinin yaygınlığı, kişilerin olası enfeksiyon bildirimlerine göre hareket edip etmediklerini ciddi biçimde etkileyen bir faktördür. Bir test programı, temas bildirimlerine dayalı olarak test yapılmasına olanak sağlamazsa, kullanıcının teste ilgisi azalarak uygulamanın faydasını ve etkinliğini düşürecektir.

Ayrıca,

Her ülkenin yanıtlarını yerel epidemiyolojik duruma ve mevcut kaynaklara göre uyarlaması gerekecektir. Yalnızca düzensiz vakaların gözlemlendiği dönemde temas izleme önlemlerinin titiz bir şekilde uygulanması, daha fazla bulaşmayı azaltabilir ve salgının yayılması üzerinde büyük bir etkiye sahip olabilir. Bununla birlikte, kaynaklar izin veriyorsa, daha yaygın iletimin olduğu coğrafi konumlarda uygulama için de düşünülmelidir. Her vakanın tüm temasları tanımlanıp izlenmese bile, temas takibi, fiziksel mesafe gibi diğer önlemlerle birlikte bulaşmanın azaltılmasına katkıda bulunabilir.

Çin ve Singapur'daki yanıtta ortaya çıkan kanıtlar, etkili temas takibinin semptom başlangıcından izolasyona kadar geçen süreyi azaltmaya yardımcı olduğunu ve devam eden bulaşma olasılığını önemli ölçüde azaltmış olabileceğini göstermiştir. Temas takibi ve karantina, Wuhan ve Güney Kore'de yaygın bulaşma dönemlerinde bir dizi başka önlemlerle birlikte kullanılmıştır. Temas takibi ayrıca Covid-19 epidemiyolojisinin daha iyi anlaşılmasına da katkıda bulunur. [7]

Manuel Temas Takibi

Temas takip sisteminin temelde basit bir çalışma yöntemi vardır. Temas takip sürecinde, tıbbi uzmanlık ve yeterliliği olan kişilerin yanı sıra çoğunluğu klinik olmayan personel kullanılır veya istihdam edilir. Covid-19 için bir kişi pozitif çıktıktan sonra, en yakın hastane veya sağlık kurumu ile temasa geçmesi beklenmektedir. Bu kişinin bir e-posta, kısa mesaj veya telefon ile durumunu bildirmesi gerekir. Temas takip sistemi daha sonra 14 gün boyunca izole edilmeleri gerektiğini söylemek için virüsle temas etme riski olan kişilerle temasa geçecektir. Temas takip programında çalışanlar mümkün olan en erken aşamada enfeksiyon riski olan kişilere ulaşarak, bu riskli kişileri hemen izole etmeye çalışmaktadır. Kişi hasta olsun ya da olmasın bu izolasyon, sağlanmalıdır. [8]

İzlanda'da salgın başladığında program üzerinde çalışan 200 kişi olmasına karşın, toplam 1.700 kişi aramaların nasıl yapılacağı konusunda eğitim almıştır. İngiltere'de temas takip programında tıbbi geçmişi olan yaklaşık 3.000 kişinin yanı sıra 25.000 kişi daha işe alınmıştır. ABD'deki mevcut hastalık takipçilerinin toplam sayısı sadece 2.200 iken, Johns Hopkins Üniversitesi tarafından yayınlanan bir araştırma, ABD'nin temas izlemeye yardımcı olması için en az 100.000 ek halk sağlığı çalışanına ihtiyacı olduğunu ortaya koymuştur.

Başlarda İtalya, İspanya, daha sonra ABD ve İngiltere'deki salgının ulaştığı boyutlar, Covid-19 virüsünün kolay bulaşıcılığının, salgınla mücadelede geleneksel önlemlerin tek başına yetersiz kaldığını ve teknolojik tabanlı değişik yöntemlere başvurulması gerektiğini açıkça göstermektedir.

Bluetooth ile Temas Takibi

Singapur'da, 20 Mart'ta hükümet, insani temas izleme çabalarını desteklemek için Bluetooth tabanlı bir temas izleme uygulaması olan TraceTogether uygulamasını başlattı. Bir kişiyle iletişim kurulduğunda, yaygın enfeksiyon riskini en aza indirmek için hareketlerini ve etkileşimlerini doğru bir şekilde haritalamaları gerekir. Veri günlükleri, telefonlarda “kriptografik olarak oluşturulan geçici kimlikler” kullanılarak şifrelenmiş biçimde saklanır.

Avrupa Komisyonu, 8.Nisan.2020 tarihinde diğer amaçların yanı sıra, temas takibi için mobil uygulamaların kullanımı için Pan-Avrupa koordineli bir yaklaşımın sürdürülmesi yönünde bir öneriyi kabul etti. Ortak yaklaşımla veri minimizasyonu ve ayrıştırma, şifreleme ve dağıtık veri tabanı gibi uygun önlemler de dahil olmak üzere gizlilik ve veri koruma ilkelerinin esas alınması kararlaştırıldı. Bluetooth tabanlı temas takip isteğe bağlı olacaktır. Mobil uygulamaların kullanımının ise veri koruma ve gizlilik üzerindeki etkilerin tartışılması kararlaştırıldı.

Diğer yandan Bluetooth özelliğinin kullanımında bazı hataların yanı sıra iPhone'larda düzgün çalışmasına engel olan birtakım zorluklar da vardır. [9]

Mobil Konum Verileri

Salgının başlangıcında Avrupa Komisyonu, Deutsche Telekom ve Orange gibi büyük mobil işletmecileri saygının önlenmesine destek olmak için anonimleştirilmiş konum verilerini paylaşmaya çağırmıştır. Bu amaçla Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone ve endüstri ticaret organı GSMA'nın yöneticileriyle bir değerlendirme toplantısı yapılmıştır. [10]

Finlandiya'da Telia, şehirler ve bölgeler arasındaki kullanıcı hareketi için anonimleştirilmiş veriler sağladığını açıkladı. İtalya'da mobil operatörler Telecom Italia, Vodafone ve WindTre yetkililere insanların hareketlerini izlemek için toplu veriler sunmaya başladı. Covid-19 dünyanın birçok yerinde hızla yayılmaya devam ederken, bazı hükümetler ve diğer kurumlar mobil şebeke işletmecileri ve diğer şirketler tarafından tutulan veriler veya analizler için talepte bulunmaktadır.

Mobil ağlardan ve diğer internet şirketlerinden gelen veriler ve bilgiler önemli olabilir, çünkü insanların dolaşımı, insandan bulaşan bulaşıcı virüslerin yayılmasına katkıda bulunan kritik faktörlerden biridir. Mobil işletmecilerden elde edilecek veriler dört grupta sınıflandırılmıştır.

- **Meta veriler**

Cep telefonu numarası ve abone bilgileri gibi önemli tanımlayıcıların yerini takma adla değiştirdiği mobil ağlardan arama ayrıntısı kayıtlarını (CDR) içeren trafik verileri.

- **Birleştirilmiş Tanımlanamayan Veriler**

Bireylerin yeniden tanımlanma olasılığını önlemek için tasarlanmış uygun eşiklere (*örneğin, birey sayısı, zaman ve/veya alan ile ilgili*) birleştirilmiş formdaki Meta Verilerdir. Bu, genellikle Meta-Veriden oluşturulan arayan-aranan matrislerini veya kalabalık bilgilerini içerir.

- **Analizler**

Birleştirilmiş Tanımlanamayan Veriler üzerinde gerçekleştirilen analitiklerin ürünü, gösterge tablosu veya görselleştirilmesidir.

- **Mobil İşletmeci Verileri**

Meta Veriler, Birleştirilmiş Tanımlanamayan Veriler ve Analizler için yukarıdaki tanımların herhangi biri veya tümüdür.

Apple/Google Maruziyet Bildirim Sistemi (Exposure Notification System/ENS)

iPhone iOS işletim sistemi üzerinde temas takip uygulaması geliştirmenin en büyük sıkıntısı iOS, arkaplanda sürekli Bluetooth kullanımına izin vermemektedir. Bu konuda Fransız hükümeti de iOS üzerinde çalışacak bir temas takip uygulaması için iOS işletim sisteminde gerekli izinlerin sağlanması konusunda Apple ile görüşmüş ancak, Apple bu özelliği sağlamayı reddetmiştir. [11]

Salgının hızlı yayılması ve yol açtığı büyük can kayıpları üzerine iOS Apple ve Google firmaları iOS ve Android işletim sistemleri üzerinde küresel olarak temas takip uygulamaları için sadece yetkili devlet kurumlarının kullanıma sunacakları bir teknik bir özellik için ortak bir çalışma başlatmışlardır.

Apple/Google Maruziyet Bildirim sistemi, Kişisel Gizlilik Temas Takip Projesi kapsamında geliştirilmiş bir çerçeve ve protokoldür. Maruziyet Bildirimi, Bluetooth teknolojisi ve gizliliği koruyan kriptografinin birleşimine dayanan, dağıtık saklama ve raporlama tabanlı protokoldür.

Apple/Google protokolü, Avrupa DP-3T konsorsiyumu tarafından oluşturulan “*Dağıtık Merkezi Olmayan Gizlilik Korunmalı Temas Takip*” (DP-3T) protokolüne ve Covid Watch tarafından “*Geçici İletişim Numarası*” (TCN) protokolüne benzer, ancak işletim sistemi düzeyinde uygulanır.

Kullanıcı gizliliğini korumak, bu spesifikasyonun tasarımında temel bir gerekliliktir. Protokol, aşağıdaki yollarla gizliliği korur: [12]

- *Maruziyet Bildirimi Bluetooth Özelliği, yakınlık algılaması için konum kullanmaz. Yakınlığı tespit etmek için kesinlikle Bluetooth işaretini kullanır.*
- *Bir kullanıcının "Rolling Proximity Identifier" bilgileri, ortalama olarak her 15 dakikada bir değişir ve bir kişiyle ilişkilendirilmesi için Geçici Maruz Kalma Anahtarına ihtiyaç duyar. Bu davranış, tanımlayıcıları yayınlarken gizlilik kaybı riskini azaltır.*
- *Diğer cihazlardan alınan yakınlık tanımlayıcıları özel olarak cihazda işlenir.*
- *Kullanıcılar, teşhir bildirimine katkıda bulunup bulunmamaya karar verir.*
- *Covid-19 teşhisi konulursa, kullanıcılar Tanılama Anahtarlarını sunucuya paylaşmak için onay vermelidir.*
- *Kullanıcılar, teşhir bildirimine katılımları konusunda şeffaflığa sahiptir.*

TEMAS TAKİP YÖNTEMİNDEKİ GELİŞMELER VE ETKİLERİ

Covid-19 salgınıyla birlikte Covid-19 pozitif kişilerle temas takibi salgının izlenip denetim altına alınabilmesi için geleneksel yöntemlerin yanı sıra teknoloji de bu çabaların hızlı ve etkin bir biçimde başarıya ulaşmasında önemli bir rol oynayabilir.

Mobil cihazlar, pozitif bir Covid-19 teşhisi bildiren bir kişiyle geçen 14 gün içerisinde kimlerin temasta olduğunu (1,5-2 metreden yakın mesafede 10 dakikadan uzun bir süre) belirlemeye yardımcı olacak ve salgın yayılımı modelleme çabalarını destekleyecek verileri sağlayan bir sistem oluşturmak için otomatik ve ölçeklenebilir bir şekilde kullanılabilir. Bu amaçla akıllı telefonlardaki "bluetooth" sinyallerinin kullanılması esas alınırken, bu tür yakınlık izleme sistemleri için önerilen altyapılar gizlilik ve güvenlik özelliklerine göre de büyük farklılıklar göstermektedir. Veri toplama modeli, anonimleştirme yaklaşımı ve veri minimizasyonu tasarımları açısından ülkeler ve gruplar arasında farklı yaklaşımlar ortaya çıkmaktadır. Bu amaçla geliştirilecek mobil uygulamaların ve temas takip veri tabanlarının daha etkin hale getirilebilmesi için temelde iki yöntem tartışılmaktadır: merkezi ve dağıtık (merkezi olmayan) modeller. [13] (Şekil-1)

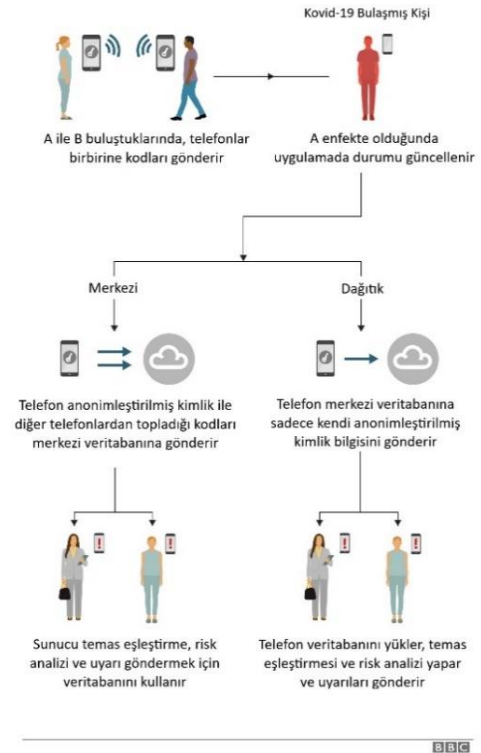
Merkezi Modeller

Kullanıcılara atanan kısa süreli tanımlayıcılar oluşturarak, temas takibinin izlenmesini hedefler. Tanımlayıcıların ve iletişim grafiklerinin oluşturulması, genellikle bir hükümet ya da başka bir güvenilir kuruluş tarafından kontrol edildiği varsayılan bir sunucuda yapılır.

Bu model, sunucuyu yöneten kuruluşun, örneğin, emniyet teşkilatı, sınır kontrolü veya istihbarat kurumlarının talebi üzerine, insanlara bulaşma durumu dışında sunucunun verilerini ve yeteneklerini kötüye kullanmayacağını varsayar. Bu koruma, potansiyel olarak bir "veri yakalama" modeline dönüştürülebilen merkezi sunucunun korunmasına dayanır.

Dağıtık Modeller

Kişilere ait hassas veriler mümkün olduğunca kullanıcı cihazlarında tutulacak şekilde tasarlanmıştır. Bu yaklaşımda bir merkezi sunucunun olmasına karşın hassas veriler için merkezi sunucuya güvenilmez. Kişilerin temasına ait veriler sadece kendi cihazlarında saklanır ve öngörülen sürenin sonunda herhangi bir pozitiflik söz konusu değilse ilgili bütün veriler cihazdan silinir.



Şekil-1. Temas Takip Uygulama Yöntemleri

Her iki modelde de kişisel verilerin korunmasına yönelik kaygı ve endişelerin yanı sıra kurulum ve işletme maliyetleri ve uygulama süresinde kullanıcı cihazı ile altyapı arasındaki günlük onlarca megabyte seviyelerine çıkacak veri yoğunluğu gibi konular da bu sistemlerin seçiminde önemli etkenlerdir.

Merkezi sistem ciddi tartışmalara yol açmıştır. Birçok kurum, kuruluş, STK ve akademik dünyadan kişisel verilerin güvenliğine yönelik çeşitli eleştiriler gelmiştir.

"Üçüncü yol" olarak ne merkezi ne de dağıtık yaklaşımların yeterli düzeyde gizlilik koruması sunmadığı iddiasıyla, özellikle ConTra Corona, Epione ve Pronto-C2 gibi farklı çözümlerin araştırılması gerektiği savunulmaktadır. [14]

Prensipte mobil temas takip uygulamaları cihazlardaki "Bluetooth" özelliğinin kullanımına dayanmaktadır. Bu yöntem, coğrafi konum sistemlerine (*Global Positioning System GPS*) göre hem yakınlık mesafesi olarak daha doğru veriler üretmektedir, hem de mahremiyet açısından daha güvenli çözüm üretmektedir.

Bu konu ile ilgili dünyadaki uygulamalara bakıldığında, Çin "Bluetooth" ve "GPS" teknolojilerine dayalı bir merkezi temas takip sistemleri kullanırken, Avrupa ülkeleri ve Avrupa Komisyonu kişisel verilerin güvenliği açısından coğrafi konum sistemlerinin kullanımına sıcak bakmayıp, "Bluetooth" temelli dağıtık temas takip sistemlerinin kullanılmasını önermiştir. [15]

Apple'ın iOS sisteminin arkaplanda sürekli çalışacak "Bluetooth" özelliğine izin vermemesi, bağımsız olarak geliştirilecek mobil uygulamaların önündeki en büyük engellerden birisi olmuştur. Ancak, Apple/Google şirketleri temas takibinde kullanılmak üzere bir uygulama arayüzü (API) geliştirmek için iş birliğine gitmişler ve bu amaçla işletim sisteminde bazı temel değişiklikler yapmışlardır.

Akademisyenler, güvenlik uzmanları, araştırmacılar ve endüstri tarafından birkaç alternatif temas takip sistemi önerilip geliştirilmiştir. [16] Bu dağıtık yöntemlerin başlıcaları aşağıdaki gibidir;

- DP3T protokolü
- Apple/Google Maruziyet Bildirim Sistemi
- PACT-Est protokolü
- PACT-Ouest protokolü
- TCN protokolü
- ROBERT protokolü.

Bunların yanı sıra merkezi veritabanı ve sunuculara dayalı olan Pan-Avrupa Gizlilik Koruma Temas Takip protokolü önerilmiştir (PEPP-PT). Bu konuda geliştirilen temel protokoller aşağıda özetlenmiştir.

Pan-Avrupa Gizlilik Koruma Temas Takibi (PEPP-PT)

PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), İsviçre'de kâr amacı gütmeyen bir kuruluştur. PEPP-PT, salgınlara karşı Avrupa gizlilik ve veri koruma yasaları ve ilkelerine bağlı bir çözüm sağlamak için oluşturulmuştur. PEPP-PT teknik mekanizmaları ve standartları, ulusal ölçekte salgına müdahalelerin hızını ve gerçek zamanlı kapasitesini en üst düzeye çıkarmak için dijital teknolojinin olanaklarından yararlanarak gizliliği tamamen korumayı hedeflemektedir. Bu teknolojileri tüm ülkelerde, bulaşıcı hastalıkların önlenmesinde yöneticilerine ve geliştiricilere olabildiğince hızlı ve sorunsuz bir şekilde sunmayı amaçlamaktadır.

PEPP-PT Covid-19 salgını bağlamında geliştirilen "*Tam Yığın Açık Protokolüdür*" (*Full-Stack Open Protocol*). Protokol, "*Dağıtık Gizlilik Koruma Temas Takip*" (DP-3T) protokolü gibi, enfekte olmuş bir kişinin temasta bulunduğu kişileri keşfetmek ve kaydetmek için Bluetooth özelliğini kullanır. Bununla birlikte, DP-3T'nin aksine, kişi günlüklerini işlemek ve hastaları enfekte bir hastayla olası temas

konusunda bireysel olarak bilgilendirmek için merkezi bir veritabanı ve raporlama sunucusu kullanır. Bu yaklaşımların mahremiyeti tehlikeye attığı ileri sürülmektedir. [17]

Helmholtz Alman Araştırma Merkezleri Derneği (CISPA), École Polytechnique Fédérale de Lausanne, ETH Zürih ve KU Leuven ve Bilimsel Değişim Enstitüsü, PePP-PT tasarımı etrafında bir “şeffaflık ve açık bir yönetim eksikliği ile veri koruma kaygılarını” gerekçe göstererek PePP/PT girişiminden çekildi. Benzer biçimde 26 ülkeden 300’ün üzerinde güvenlik ve gizlilik akademisyeni 20.Nisan.2020 tarihinde, PEPP-PT tarafından benimsenen yaklaşımı eleştiren ve “kişiler hakkında müdahaleci bilgilerin yeniden yapılandırılmasına izin veren çözümlerin daha fazla tartışılmadan reddedilmesi gerektiğini” belirten bir açık mektup yayınlamıştır. [18]

ROBust ve Gizlilik Koruma Temas Takip Protokolü (ROBERT)

ROBERT, PEPP-PT için bir protokol önerisidir. ROBERT, bir grup gizlilik ve güvenlik araştırmacıları olan Inria (*PRIVATICS ekibi tarafından yönetilen ortak çaba*) ve Fraunhofer AISEC arasındaki iş birliği ile geliştirilmektedir.

Dağıtık Gizlilik Korunmalı Temas Takibi (DP-3T)

DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*), “kişisel gizliliğe saygı duyan COVID-19 salgını için temas takibine açık bir teknik çözüm oluşturmak üzere güçlerini birleştiren Avrupa genelinden araştırmacıların bir işbirliği” çerçevesinde “güvenli, dağıtık (merkezi olmayan), gizliliği koruyan bir yakınlık izleme sistemini belgeler. Amacı, enfekte bir kişiyle temas halinde olan kişileri tanımlama sürecini basitleştirmek ve hızlandırmak, böylece SARS-CoV-2 virüsünün yayılmasını yavaşlatmaya yardımcı olacak teknolojik bir temel sağlamaktır. Sistem, bireyler ve topluluklar için gizlilik ve güvenlik risklerini en aza indirmeyi ve en üst düzeyde veri korumasını garanti etmeyi amaçlamaktadır.” [19]

DP-3T, gizliliği koruyan temas takip sistemlerini analiz ederek, tasarlamakta ve geliştirmektedir. Bu kapsamda “başkalarının da kullanması için açık kaynak olarak sunulan İsviçre uygulamasının ilk sürümünü de” oluşturmuştur.

DP-3T, Dağıtık Gizlilik Koruma Temas Takip protokolü, Apple ve Google’ın kendi kişi izleme modelini temel aldığı protokoldür.

DÜNYA ÖRNEKLERİ

Salgının küresel boyutta ve çok hızlı yayılması başlangıçta başta toplum olmak üzere, devletler ve teknoloji şirketlerinde büyük şaşkınlık ve paniğe yol açtı. İnsan hayatı doğal olarak öne çıkarken, özellikle AB olmak üzere gelişmiş ülkelerde temel hak ve özgürlükler konusunda kaygıları giderecek düzenlemeler yapılmaya başlandı. Aradan geçen 6-7 aylık dönemde gerek temas takip uygulamalarına yönelik teknolojik tartışmaların gerekse temel hak ve özgürlüklere yönelik düzenlemelerin ilk sonuçları elde edilmeye başlandı.

Bu çalışmanın odağını oluşturan temas takip uygulamaları, insan kaynakları ağırlıklı olarak bulaşma haritası çıkartarak, salgının yayılmasını önlemeyi hedefleyen geleneksel yaklaşıma teknolojik destek sağlayarak, gerekli verilerin gerek çok geniş ölçekte toplanmasında gerekse de bu toplanan verilerin çok daha hızlı işlenmesine yardımcı olması hedeflenen uygulamalardır.

Dünyadaki temas takip uygulamalarında bazı ülkeler merkezi yapıyı, bazı ülkeler de dağıtık yapıyı tercih etmişlerdir. Başlangıçta merkezi yapıyı tercih eden bazı ülkeler ise süreç içerisinde dağıtık yapıya geçmişlerdir.

Araştırmalara göre, tüm temas takip uygulamalarının %50'sinden fazlası kullanıcıların verilerini ne kadar süreyle saklayacaklarını belirtmiyor. Veri saklama ve imha prosedürlerini özetleyen açık gizlilik politikalarının eksikliği veri koruma ve mahremiyet endişelerini önemli ölçüde artırmaktadır.

Bu konuyla ilgili dünya örnekleri aşağıda yer almaktadır.

Çin

Çin hükümeti Alipay ve WeChat ile birlikte, vatandaşların Covid-19 olan kişilerle temas halinde olup olmadıklarını kontrol etmelerini sağlayan bir uygulama kurdu. 200'den fazla Çin şehrinde kullanılmaktadır.

Zorunlu bir uygulama olup, konum ve rehber bilgilerini toplar. Bir kullanıcının konumu ve kısmen devlet anketiyle bilgilendirilen tıbbi ve seyahat geçmişi gibi bilgilere dayanmaktadır. [20]

Singapur

Singapur temas takip uygulamalarını ilk geliştiren ve uygulamaya sokan ülkelerden biridir. TraceTogether adlı geliştirdiği bir uygulamayı kullanmaktadır. OpenTrace adlı açık kaynaklı bir referans uygulamasıyla geliştirilen BlueTrace adlı dijital bir kişi izleme protokolü kullanmaktadır.

Bu uygulama aracılığıyla bireyler, denetimli giriş/çıkış noktalarında (1) bir QR kodunu taramak için SingPass Mobil uygulamasını kullanarak veya "SafeEntry Check-in" işlevini kullanarak yakındaki konumların bir listesinden seçim yaparak (2) bir kimliğe sahip olan SafeEntry'den personel tarafından taranan bir barkodlu kart (*örneğin NRIC, Passion card, öğrenci pasosu ve çalışma izni*) veya (3) bir mekânda görüntülenen bir QR kodunun tarayıp kişinin kişisel bilgilerinin sunarak giriş/çıkış yaparlar.

İzlanda

İzlanda Rakning C-19 rota izleme, kullanıcı arayüzü ve ulusal Covid-19 web sayfası Upplýsingar um Covid-19 á landslandi'den gelen içeriğe sahip Android ve iOS için bir GPS kayıt uygulamasını geliştirdi.

Pozitif vakalarda, konum verileri daha geleneksel temas izlemeyi desteklemek için kullanılmaktadır. Mayıs 2020 itibarıyla, İzlandalıların %38'i tarafından indirilen uygulama, dünyadaki temas takip uygulamaları arasında en yaygın kullanım oranına sahiptir. Konum verileri, cep telefonu numarası ve gerekirse sosyal güvenlik numarası toplanmakta ve uygulama kullanıcının telefonundan kaldırıldığında kullanıcının telefonunda hiçbir konum verisi saklanmamaktadır. [21]

Almanya

Almanya başlangıçta Alman sağlık kuruluşu Robert Koch Enstitüsü'nün de aralarında bulunduğu kuruluşlar tarafından geliştirilen PEPP-PT protokolünü destekledi. [22] Buna göre kullanıcıların cep telefonlarından veri toplayarak merkezi bir veritabanında saklayacak bir uygulama geliştirdi. Ancak iOS işletim sistemindeki kısıtlar ve Apple firmasının bu konudaki yaklaşımı nedeniyle geri adım atmıştır.

Almanya Haziran.2020 ayında, Apple/Google platformunda dağıtık (*merkezi olmayan*) modelde bir temas takip uygulamasını hayata geçirdi. [23] Nüfusun %20'ye yakın bir bölümü bu yeni uygulamayı indirerek kullanmaya başlamıştır.

İngiltere

İngiltere, ilk olarak kişileri tespit etmek için akıllı telefonlarda Bluetooth bağlantısını kullanacak temas takip uygulaması için, Singapur'da geliştirilen TraceTogether uygulamasından yararlanmıştır. Ancak kısa sürede Bluetooth kullanmanın, özellikle uygulamanın her zaman telefonda açık tutulmasından dolayı pilin hızlı tükenmesi ve iOS sisteminin arkaplanda Bluetooth özelliğinin çalışması ile ilgili sıkıntılar yaşanmaya başlamıştır.

İngiltere, Oxford bilim adamlarının sağlık hizmetinin virüs salgınlarını düzgün bir şekilde izleyebilmesi için hayati olduğunu düşündüğü merkezi bir modele dayalı olarak geliştirdiği uygulamadan vazgeçip,

Haziran.2020 ortalarında Apple/Google tarafından sağlanan daha gizlilik odaklı teknolojiye dayalı bir modele geçmiştir. [24]

Fransa

Haziran.2020 ayında, Fransız hükümeti StopCovid isimli temas takip uygulamasını yayınladı, ancak 1,9 milyon kişinin indirdiği uygulama ile sadece 14 bildirim gönderildi. 22.Ekim.2020 tarihinde StopCovid uygulaması güncellenerek "TousAntiCovid" (*Herkes Covid'e Karşı*) olarak yeniden adlandırılmıştır.

Fransa, bir grup araştırmacı ve özel şirket tarafından geliştirilen ve merkezi bir mimari üzerinde çalışan temas takip uygulaması ROBERT protokolünü kullanmaktadır. Sunucu kişilere kalıcı bir kimlik (*takma ad*) atar ve telefona bu kalıcı kimlikten türetilen geçici kimliklerin bir listesini gönderir.

Avustralya

Avustralya, Singapur tarafından geliştirilen BlueTrace protokolüne dayalı olarak geliştirilen COVIDSafe uygulamasını 26.Nisan.2020 tarihinde yayınlamak üzere kullanmaya başlamıştır. Hükümet, toplanan kayıt bilgileri ve Bluetooth temas verilerine yalnızca devlet sağlık görevlilerinin erişebileceğini vurgulasa da verilerin bir merkezde toplanıyor olması ciddi eleştirilere neden olmaktadır. [25]

Avustralya Sağlık Bakanlığı, insanların mahremiyetini korumak ve uygulamadan elde edilen bilgilere erişimi kısıtlamak için Biyogüvenlik Yasası kapsamında bir Karar yayınladı. Eyalet ve Bölge sağlık yetkililerinin bilgilere yalnızca temas takibi için, ancak kullanıcının açık rızasıyla erişebilecektir.

Avustralya Hükümeti 8.Mayıs.2020 tarihinde GitHub sitesinde barındırılan, COVIDSafe Uygulaması kaynak kodunu genel denetim için yayınladı.

COVIDSafe ile toplanacak kişisel verilerin depolanması için Avustralya hükümetinin, Amazon Web Services (AWS) ile bir sözleşme imzalaması, özellikle ABD hükümetinin 2018 tarihli Bulut Yasası ile sınır ötesi verilere de olası erişimi ciddi endişelere yol açmıştır.

"Avustralya Sağlık Bakanı COVID-19 salgınının bittiğini açıkladığında, kullanıcılardan uygulamayı telefonlarından silmeleri istenecektir. Bu, bir kişinin telefonundaki tüm uygulama bilgilerini silecektir. Ulusal COVIDSafe Veri Deposundaki bilgiler de pandeminin sonunda imha edilecektir." [26]

İsviçre

DP-3T protokolünü kullanan ve Apple/Google Bluetooth arayüzünün (API) en üstünde bulunan SwissCovid adlı bir uygulamadır. Uygulama "Mozilla Public License 2.0" ile lisanslanmıştır.

İsrail

İsrail Sağlık Bakanlığı 22.Mart.2020 tarihinde iOS ve Android temas takip uygulaması olan "HaMagen"i başlattı. Hamagen, kullanıcının standart konum API'lerini kullanarak nerede olduğunu izler ve yollarının önceki 14 gün içinde geçip geçmediğini kontrol etmek için Covid-19 teşhisi konan kişilerin bilinen hareketleriyle karşılaştırır. Hamagen uygulaması, konumlar ve saatler hakkındaki bilgilerin kullanıcının cihazında çapraz referanslandığı ve bulut veritabanına aktarılmadığı ilk önce gizlilik ilkesi yaklaşımı ile tasarlanmıştır.

İsrail Sağlık Bakanlığı tarafından paylaşılacak olan virüsle teşhis edilen biriyle temasa geçtiklerinde ortaya çıkar. Konum geçmişi yalnızca kullanıcının cihazında depolandığı ve e-posta veya cep telefonu ile kullanıcı kimliği toplanılmadığı belirtilmektedir.

Bu örneklerin dışında birçok ülke tarafından da temas takip uygulamaları geliştirilmiştir. Örneğin;

- Güney Kore, kredi kartı işlemlerini, CCTV görüntülerini ve cep telefonu konumlarını izledi.
- Avusturya, dağıtık (*merkezi olmayan*) bir uygulama sunan ilk ülke oldu. Kızıl Haç tarafından işletilen kullanıcılar, eşleşmeler gerçekleştiğinde manuel olarak kontrol etme seçeneğine sahiptir.

- Norveç her beş kişiden sadece birini aktif olarak kişi izleme uygulamasını kullanmaktadır. Kullanıcı verilerinin merkezi bir veritabanında depolanması gizlilikle ilgili endişeleri gündeme getirmiştir.

Temmuz.2020 itibarı ile temas takip uygulamalarının akıllı telefon kullanıcıları tarafından indirilme oranları aşağıdaki gibidir. [27]

Katar	%91,8
İzlanda	%38,0
Singapur	%37,0
İsrail.....	%22,3
Avustralya	%21,6
İsviçre	%17,6
Türkiye	%17,3
Almanya	%17,3
Hindistan	%12,5
Yeni Zelanda	%10,7
İtalya.....	%7,2

Bu veriler göstermektedir ki, teknolojik uygulamalar salgınla mücadelede etkin ve faydalı olabilirler ancak insan emeğinin yerine geçememektedir. Temas takip uygulamalarının çok daha kapsamlı bir sağlık hizmeti müdahalesinin parçası olması gerekmektedir. Bu, salgınla mücadelede yaygın testleri ve yeterli sağlık hizmetlerine erişimi içerir. Yayımlanmış 15 çalışmanın yeni bir sistematik incelemesi, teknolojinin etkili olabilmesi için hala manuel temas takibi, sosyal mesafe ve kitle testi gerektirdiğini göstermektedir.

TÜRKİYE'DEKİ GELİŞMELER

Türkiye, Covid-19 salgını ile diğer ülkelere göre biraz daha geç karşılaştı. Bu, gerek topluma gerek kamu kurumlarına gerekse de iletişim altyapı ve hizmet sağlayıcılarına bazı hazırlıklar için biraz da olsa zaman sağlamıştır. Ancak, eğitimden iş hayatına büyük ölçekli izolasyon sürecinde evden online çalışmaların artması ve eğitimin uzaktan yapılmaya başlaması sonucu, veri ve ses iletişimde ciddi artışlara yol açmıştır.

KVKK 27.03.2020 ve 9.Nisan.2020 tarihlerinde Covid-19 salgınına yönelik 2 duyuru yapmıştır.

KVKK bu duyurularında, salgın döneminde kişisel verilerin işlenmesine yönelik temel birtakım konularda açıklamalarla birlikte bazı uyarı ve önerilerde bulunmuştur.

Kişisel Verileri Koruma Kurumu

KVKK, Covid-19 salgını ile ilgili ilk duyurusunu 27.03.2020 tarihinde yapmıştır. Bu duyuruda; [28]

Covid-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler

- *Tüm Dünya ve Ülkemizi etkileyen Covid-19 virüsü salgını var*
- *Bu salgının yayılmasını engellemek ve etkilerini hafifletmek için özel nitelikli kişisel veriler de (sağlıkla ilgili veriler vb.) dâhil olmak üzere pek çok kişisel verinin (TC kimlik no, ad, adres, işyeri, seyahat bilgileri gibi) işlenmesi kaçınılmazdır.*
- *Veri sorumluları ve veri işleyenlerin, söz konusu faaliyetleri Kanun hükümlerine uygun yürütülmesinin sağlaması ve veri güvenliğine yönelik gerekli idari ve teknik tedbirlerin alması gerekir.*
- *Bu nedenle kişisel verilerin hukuka uygun olarak işlenmesi ve bu konuda alınan herhangi bir önlemin hukukun genel ilkelerine uygun olması, bu çerçevede kişilerin temel hak ve özgürlükleri açısından geri döndürülemez zararların ortaya çıkmaması önemlidir.*
- *Covid-19 virüsüne karşı alınan önlemler kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri gerekli, amaçla bağlantılı, sınırlı ve ölçülü olmalıdır.*
- *Bu konuda alınan kararlar, Sağlık Bakanlığı başta olmak üzere halk sağlığı kuruluşlarının veya diğer ilgili kurum ve kuruluşların rehberliği ve /veya talimatları çerçevesinde olmalıdır.*

Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler

- 6698 sayılı Kanunda kişisel verilerin işlenmesinde sayılan genel (temel) ilkeler hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalıdır.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmez.
- İşlenmesini gerektiren sebeplerin ortadan kalkması halinde ise söz konusu kişisel veriler silinmeli, yok edilmeli veya anonim hale getirilmelidir.

Kanuna Uygunluk

- Özellikle sağlık verilerinin işlenmesi açısından çalışanın rızasını alma yoluna gidilmesi tercih edilebileceği gibi, salgının yayılma hızı düşünülürse, çalışan kendi rızası ile de hastalık bildirimini yapabilecektir.
- Açık rıza dışındaki şartlar dâhilinde ise, sağlık verilerinin iş yeri hekimleri tarafından işlenmesi söz konusu olacaktır.
- Bu süreçte doğaldır ki her işlenen veri özel nitelikli kişisel veri de olmayabilir (Örneğin kişilerin son olarak seyahat ettikleri ülke bilgisi gibi).
- Bu durumlarda da Kanunun 5 inci maddesinde kişisel veri işleme şartlarının dikkate alınması gerekecektir.
- Bu çerçevede, mevcut durum kamu güvenliğini ve kamu düzenini tehdit ettiğinden kişisel verilerin Sağlık Bakanlığı ve yukarıdaki madde kapsamına giren kamu kurum ve kuruluşları tarafından işlenmesinin önünde de bir engel bulunmamaktadır.

Aydınlatma Yükümlülüğü (Şeffaflık)

- Kişisel verileri işleyen veri sorumluları, kişisel verilerin toplanma amacı ve ne kadar süreyle saklanacağı hususu da dâhil olmak üzere, uyguladıkları önlemler konusunda şeffaf olmalıdır.
- Bireylere kişisel verilerinin işlenmesi hakkında kısa, kolay erişilebilir, anlaşılır, açık ve sade bir dil kullanılması suretiyle bilgi sağlamalıdır.

Gizlilik

- Covid-19 virüsünün yayılmasını önleme bağlamında, veri sorumlusu ve veri işleyenler tarafından başta sağlık verisi olmak üzere herhangi bir veri işleme faaliyetinde, kişisel verilerin güvenliğini sağlayacak gerekli idari ve teknik tedbirler alınmalıdır.
- Etkilenen kişilerin verileri açık ve zorunlu bir gerekçe olmaksızın herhangi bir üçüncü tarafa ifşa edilmemelidir.
- Sosyal medya hesapları ve benzeri mecralarda sağlık verileri başta olmak üzere kişisel veriler ile ilgili hukuka aykırı olarak yapılacak paylaşımların aynı zamanda TCK 136 ncı maddesi kapsamında suç teşkil edebilecektir.

Veri Minimizasyonu

- Covid-19 virüsünün yayılmasını önleme amacına yönelik gerçekleştirilen veri işleme faaliyetleri de amaçla bağlantılı ve sınırlı ölçüde gerçekleştirilmeli, gereğinden fazla kişisel veri işlenmesinden kaçınılmalıdır.
- Hedeflenen amaca ulaşmak için imkân dâhilindeki en müdahaleci olmayan yolun tercih edilmesi gerekmektedir.

9.Nisan.2020 tarihinde Covid-19 virüsü salgını ile mücadele kapsamında kişisel verilerin işlenmesi ve kişilerin hareketlerinin izlenmesi konularında bir Kamuoyu Duyurusu yayınlamıştır. Bu duyuruda; [29]

- Çeşitli ülkelerde koronavirüsün yayılımını önlemek amacıyla;
 - Mobil uygulamalar vb. yöntemlerle; bu hastalığı taşıyan veya taşıma riski bulunan kişilerle temasa geçenlerin tespit edilmesi, virüsün yayılma haritası çıkartılarak tedavi ve karantina uygulanması, karantinaya alınanların kontrolü, sokağa çıkma yasağının uygulanması,
 - Kalabalık yerlerin tespiti gibi amaçlarla ilgili kişilerin sağlık, konum ve iletişim bilgileri gibi kişisel verileri işlenmektedir.
- Böyle durumlarda kişisel verilerin güvenliğinin gözetilmesi gerektiği de tartışmalıdır.
- Konum verisinin ilgili kişi ile ilişkilendirilerek kullanılmasının gerekli olduğu durumlarda;

- 6698 sayılı Kanununun 28 inci maddesinin (1) numaralı fıkrasının (ç) bendinde, kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde Kanun hükümlerinin uygulanmayacağı düzenlenmiştir.
- Salgın hastalık teşhisi konmuş kişilerin bulaşıcılığının sürdüğü dönemde izolasyonlarının temin edilmesi ve
- Genel nüfusun konum verilerinin işlenmesi suretiyle kalabalık alanların tespit edilmesi bu kapsamda değerlendirilmektedir.
- Diğer taraftan kişilerin konum verilerinin sağlık durumlarıyla ilişkilendirilmek suretiyle işlenmesi sürecinde söz konusu verilerin üçüncü kişilerce ele geçirilmesi halinde ilgili kişiler bakımından ciddi zararlar ortaya çıkabilir.
- İlgili kurum ve kuruluşlar kişisel verilerin güvenliğini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri almalıdır.
- Bu verilerin işlenmesini gerektiren sebepler ortadan kalktığında söz konusu kişisel veriler silinmeli veya yok edilmelidir.

T.C. Sağlık Bakanlığı

Türkiye’de Bakanlık tarafından “Hayat Eve Sığar” başlıklı bir temas takip programı geliştirilmiştir. Bu uygulama dünya örnekleriyle karşılaştırıldığında tipik merkezi veri tabanı ve sunucu sistemine dayalı bir yapıya sahiptir.

Bu uygulama tarafından “Kimlik verisi: TC Kimlik Numarası, baba adı ve doğum tarihi” “İletişim verisi GSM numaralarını girmeniz veya kişi listesinden.” “Konum verisi” “Sağlık verisi” “Meslek verisi” telefon numarası, konum bilgisi ve aile/yakın bilgisi istenmektedir. Ayrıca SMS ile doğrulama yapılmaktadır. [30]

Toplanan verilerin paylaşımı ile ilgili, Aydınlatma Metninde; “İzolasyon altında bulunmanız gereken bölgeyi terk etmeniz halinde bu uygulama ile elde edilen kimlik, iletişim ve konum verileriniz, kamu sağlığının korunması ve salgının yayılmasını önleme amaçlarıyla İçişleri Bakanlığı ve kolluk kuvvetleri ile paylaşılacağı” bilgisi yer almaktadır. Ancak, veriyi saklama süresi ile ilgili bir açıklama yer almamaktadır.

Temel olarak temas takip uygulaması olarak başlatılan proje gelinen noktada, kapsamı oldukça genişletilmiş; maske talebi, güncel istatistikleri, salgın yoğunluk haritası, HES kodu, yakın kişilerin bilgileri gibi ek özelliklerinin yanı sıra Alo182 ile Sağlık Bakanlığı ve e-Nabız web sitelerine erişim hizmetleri de eklenmiştir.

KVKK, 27.03.2020 tarihinde yaptığı duyuruda “Covid-19 virüsüne karşı alınan önlemler kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri **gerekli, amaçla bağlantılı, sınırlı ve ölçülü** olması gerektiğini ve bu konuda alınan kararlar, **Sağlık Bakanlığı başta olmak üzere halk sağlığı kuruluşlarının** veya diğer ilgili kurum ve kuruluşların rehberliği ve / veya talimatları çerçevesinde uygulanması” gerektiğini belirtip, “amaç ve ne kadar süreyle saklanacağı hususu da dâhil olmak üzere, **uyguladıkları önlemler konusunda şeffaf olunması**” ve “amaçla bağlantılı ve sınırlı ölçüde gerçekleştirilmesi, **gereğinden fazla kişisel veri işlenmesinden kaçınılması**” ve “**imkân dâhilindeki en müdahaleci olmayan yolun tercih edilmesi**” konularını açık bir biçimde ifade etmiştir.

Bu açıklamaları, KVKK’nın bu süreçlerde ve bu süreçlerin denetiminde daha aktif rol alacağı biçiminde değerlendirmek mümkündür.

Ancak, “Hayat Eve Sığar” uygulaması gündeme geldiğinde, 9.Nisan.2020 tarihindeki düzenlemesiyle bu tür uygulamaların kapsam bakımından Kanununun 28. Maddesinin 1(ç) fıkrası hükmü çerçevesinde değerlendirilerek tümüyle KVKK dışında tutmuştur. Halbuki Kanununun 6. maddenin 3. fıkrası, “*kamu sağlığının korunması, koruyucu hekimlik*” kapsamında işlenecek sağlık verileri ile ilgili olarak sadece “*rıza aranmaksızın işlenmesi*”ne izin verirken, diğer yükümlülükleri ortadan kaldırmamaktadır. “Hayat Eve Sığar” temas takip uygulamasına, özellikle AB örneklerinin aksine salgının yayılmasına ve

izlenmesine yönelik olmayan işlevler de eklenerek kapsamı çok genişletilmiş, daha sonra da KVKK tarafından Kanununun 28. Maddesinin 1(ç) fıkrasıyla kanunun kapsamı dışına çıkartılmıştır.

Benzer biçimde, mobil işletmeciler tarafından salgın önleme amacıyla paylaşılacak verilerin de (*genel nüfusun konum verilerinin ilgili kişi ile ilişkilendirilerek kullanılması suretiyle kalabalık alanların tespit edilmesi*) aynı biçimde KVKK kapsamı dışında değerlendirileceğini belirtmiştir.

Ancak, mobil işletmecilerin gerek “*metaveri, anonimleştirilmiş ve birleştirilmiş hareket verilerini*” gerekse de “*kalabalık alanların tespit edilmesi için ilgili kişi ile ilişkilendirilerek kullanılacak genel nüfusun konum verilerini*” paylaşım paylaşmadığı konusunda herhangi bir bildirim yapılmamıştır.

SONUÇ

Temas takip uygulamalarının, dünyada salgının takibi yayılması ve önlenmesinde önemli bir rol oynaması beklenmesine rağmen bu uygulamaların sınırlı bir etkisi oldu. Oxford Üniversitesi araştırmacıları, temas takip uygulamalarının etkili olabilmesi için bir ülke nüfusunun %60'ının temas takip uygulamasını indirip kullanması gerektiğini söyledi.

Temas takip uygulamalarının başarısı, yaygın kullanıma dayalıdır. Bu da güven ile mümkündür. İzlanda'nın temas uygulaması, nüfusun %38'i tarafından indirilerek dünyadaki en yüksek kişi başına indirme oranına ulaşmıştır. Temas takip uygulamalarının, geliştirilmesinde öncü olarak görülen Singapur'da yaklaşık 2,1 milyon kez indirildiği görüldü. Bu, ülke nüfusunun yaklaşık %37'sine karşılık gelir ki hala önerilen %60 eşliğinin çok altındadır. Ancak bu kadar etkileyici kullanma oranının bile epidemiyologlarca anlamlı bir fark yaratmak için gerekli olduğu belirtilen en az %60-75 kullanım oranına yaklaşmadığı görülmektedir. Ayrıca, İzlanda'nın deneyimi de bu tezleri desteklemektedir.

Ancak bilim adamlarınca yapılan modeller, kişilerin %75'inin bir temas takip uygulamasını kullanması durumunda ölümlerin %78 ve enfeksiyonların %81 oranına kadar azaltılmasına yardımcı olabileceğini, diğer yandan %15' oranındaki bir yüklemeye bile ölümlerde %11,8 oranında, enfeksiyonda ise %15 oranında azalma anlamına gelebileceğini göstermektedir.

Temas takip uygulamalarının kullanımı kişisel veriler ve mahremiyet açılarından ciddi tereddüt ve endişeleri gündeme getirmiştir. Bugüne dek elde edilen sonuçlar, söz konusu tereddüt ve endişelerin giderilmeden temas takip uygulamalarının beklenen sonuçları sağlayamayacağı ve sonuçta başarılı olamayacağı göstermektedir.

Ülkemizde Hayat Eve Sığar uygulamasının akıllı telefon kullananların %17,6'sı tarafından indirildiği belirtilmektedir. Dolayısıyla toplumda tam olarak karşılık bulamamış olması HES uygulamasının hedeflenen başarıya ulaşılmasının önündeki en büyük engellerden biri gibi görülmektedir.

Toplu insan hareketliliğinin izlenmesinin salgının yayılma biçimine yönelik izleme, inceleme ve tahminler için kullanımında genel ilke “*metaveriler ile anonimleştirilmiş ve birleştirilmiş tanımlanamayan konum verilerinin*” kullanılmasıdır. Teknik olarak, anonimleştirilen tüm veriler gibi konum verileri de veri koruma düzenlemeleri kapsamı dışına çıkar ve özellikle toplu hareketlerin belirlenmesi için kullanılan birleştirme işlemi de tek tek bireylere ulaşılmasını engellemektedir.

Bu nedenle, tüm dünyada olduğu gibi ülkemizde de bu endişeleri gidermeye yönelik, uygulamaların toplanan bilgilerin isimleri veya diğer kişisel bilgileri açığa çıkarmaması gerekmektedir. Gönüllülük esasına göre kullanılması, toplanacak verilere erişimin kısıtlı olması ve kimlerin eriştiğinin bilinmesi önemlidir. Bu verilerin başka amaçlarla kullanılmaması, kaynak kodlarının bağımsız incelemeye açık olması ve salgın sona erdiğinde bu amaçla toplanan tüm verinin silineceğine yönelik güvence sağlanması gerekmektedir.

Bu konudaki en iyi güvence şeffaflıktır. Şeffaflığın en iyi uygulaması ise, toplanıp işlenen verilerin neler olduğu, nasıl ve kimler tarafından erişilip işlendiği konularında yapılan işlemlerin açık ve denetlenebilir olmasıdır.

KAYNAKÇA:

- [1] European Commission , C(2020) 2296 final, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data
- [2] <https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>
- [3] European Commission , C(2020) 2296 final, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data
- [4] European Centre for Disease Prevention and Control, TECHNICAL REPORT Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update 8 April 2020
- [5] EDBP Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020
- [6] https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf
- [7] European Centre for Disease Prevention and Control, TECHNICAL REPORT Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update 8 April 2020
- [8] <https://www.wired.co.uk/article/nhs-covid-19-tracking-app-contact-tracing>
- [9] Basford, Sarah, 'CovidSafe still has bugs, according to experts', Gizmodo, 25 May 2020
<gizmodo.com.au/2020/05/covidsafe-bugs-ios-android-tracking-privacy/>
- [10] <https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/>
- [11] <https://www.cnet.com/news/apples-bluetooth-policy-is-blocking-contact-tracing-app-france-says/>
- [12] https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf
- [13] <https://www.bbc.com/news/technology-52650576>
- [14] <https://eprint.iacr.org/2020/493>
- [15] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670
- [16] Ces syst`emes ne permettent pas d'identifier des « clusters » puisqu'ils n'utilisent aucune information de géolocalisation
- [17] https://en.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing#cite_note-:2-17
- [18] https://en.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing
- [19] <https://github.com/DP-3T/documents>
- [20] <https://privacy.org.nz/assets/2020-05-12-OPC-Comparison-of-COVID-19-Apps-colours.pdf>
- [21] <https://privacy.org.nz/assets/2020-05-12-OPC-Comparison-of-COVID-19-Apps-colours.pdf>
- [22] <https://www.computerweekly.com/news/252484779/Data-privacy-fears-emerge-as-German-contact-tracing-app-downloaded-65m-times-in-first-day>
- [23] <https://www.coronawarn.app/en/>
- [24] <https://www.bbc.com/news/technology-53114251>
- [25] <https://privacy.org.nz/assets/2020-05-12-OPC-Comparison-of-COVID-19-Apps-colours.pdf>
- [26] <https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#about-the-app>
- [27] <https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/>
- [28] <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler>
- [29] <https://kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2->
- [30] https://hesapp.saglik.gov.tr/hayat_eve_sigar_aydinlatma.pdf