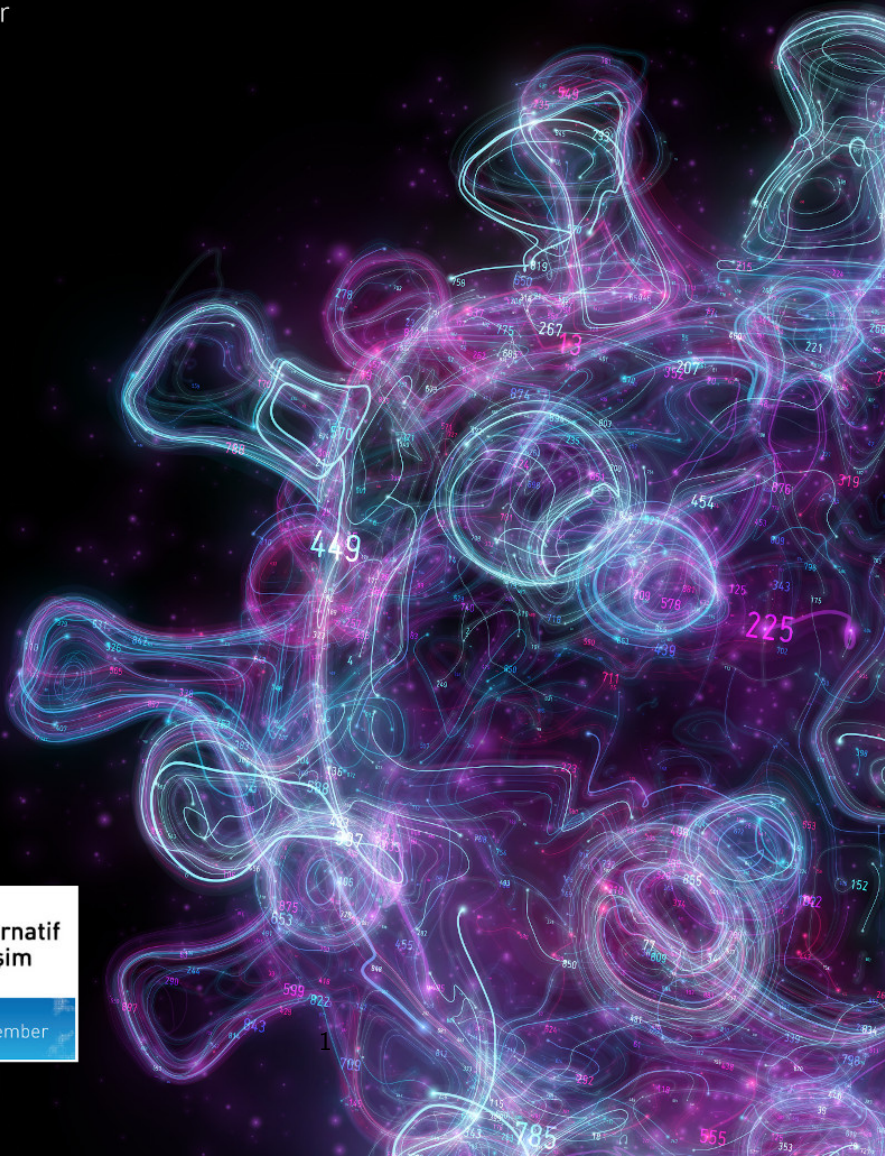
COVID-19 SÜRECİNDE TEMAS TAKİP UYGULAMALARI

ve KİŞİSEL VERİLERİN KORUNMASI

*Faruk Çayır



alternatif bilişim

EDRi member

alternatif bilişim

COVID-19 Sürecinde

Temas Takip Uygulamaları ve Kişisel Verilerin Korunması

Faruk Çayır

Mayıs 2020

ISBN 978 - 605 - 80007 - 1 - 1

Yazar: Faruk Çayır
Editör: Mutlu Binark
LaTeX yerleşimi: Ali Rıza Keleş
Kapak tasarımı: Cemgazi Yoldaş
Kapak görseli: freepik.com

Alternatif Bilişim Derneği,
Dikmen Caddesi No:220-B/8 Çankaya/Ankara +90 312 230 1560 bilgi@alternatifbilisim.org
http://www.alternatifbilisim.org

Önsöz

COVID-19 sürecinde küresel ölçekte pandemi takip uygulamalarının halk sağlığının korunması ve toplum güvenliği adına yaşama geçirilmesine tanıklık ettik. Otoriter devletlerden liberal Batı demokrasilerine değin, pandemi takip uygulamalarını yaşama geçirmeyen ülke sayısı son derece az. Akıllı telefon uygulamalarından, elektronik bilekliklere ve CCTV ile entegre QR kod taramalarına değin bir çok uygulama dolaşımda. Hükümetler, merkezi veya gayri merkezi veri toplama ve depolama arasında seçimler yaptılar. Bu seçimlerin siyasi, toplumsal ve ekonomik sonuçları olacağı aşikar. Türkiye'de de *Hayat Eve Sığar* adıyla bir uygulama Sağlık Bakanlığı tarafından akıllı telefon kullanıcılarına sunuldu. Burada önemli olan bu olağanüstü durumda kişisel verilerin mahremiyetinin halk sağlığı adına geçici olarak sınırlandırılmasının yeni normalin bir parçası haline gelip gelmeyeceği sorunu.

Bu izleme çalışmasında Derneğimiz üyesi avukat Faruk Çayır, dünyadaki uygulamaları derledi, kişisel verilerin korunması temelinde bu uygulamaları inceledi. Hayat Eve Sığar uygulaması üzerine yoğunlaşarak, uygulamanın hangi verileri topladığını, hangi taraflarla paylaştığını ve kişisel verilerin korunması bağlamında mevcut sorunlarını tartıştı. Bu izleme çalışması, Derneğimizin bilişim teknolojileri ve uygulamalarının yaşama geçirilmesinde tüm paydaşların katılımının etkili bir şekilde katılımın sağlanması, bilgiye erişimde şeffaflığın temini konusundaki toplumsal ve siyasal rolünün somut bir çıktısı olduğunu düşünmekteyim.

Mutlu Binark
18 Mayıs 2020

COVID-19 SÜRECİNDE TEMAS TAKİP UYGULAMALARI VE KİŞİSEL VERİLERİN KORUNMASI

2020 yılının ilk ayında COVID-19 virüsünün önce Çin'de ardından tüm dünya ülkelerinde hızla yayılmaya başlaması, epideminin pandemiye dönüşmesiyle dünyadaki çoğu hükümet virüsün yayılmasını yavaşlatmak ve halk sağlığını korumak amacıyla bir dizi dijital izleme, gözetim ve sansür önlemlerini yaşama geçirdi. Bunlardan bazıları daha önce görülmemiş bir şekilde gerekli ve yeterli inceleme yapılmaksızın acele verilmiş idari kararlar ile yapılırken, bazıları da yasama organları tarafından uygulamaya konuldu.

Görünen o ki önümüzdeki haftalar ve aylar boyunca dijital izleme ve gözetim uygulamaları yurttaşların dijital haklarını tehdit etmeye devam edecek. COVID-19'un yayılmasını kontrol etmeye yardımcı olacağı belirtilen aşırı ve orantısız teknolojik uygulamalar, hükümetler ile teknoloji şirketlerinin kişisel verilere erişimlerini giderek artıracak. Kişisel veriler toplumsal alanı güvenlikleştirme uygulamalarının doğal bir parçası haline gelecek.

COVID-19 sürecinde, virüsten etkilenen bireyleri izlemek, fiziksel mesafenin etkinliğini daha iyi anlamak veya temas edilenlere göre etkilenebilecek kişilere uyarı göndermek için büyük teknoloji şirketleri tarafından tutulan konum verilerinin kullanılmasına küresel olarak ilgi artmaktadır. Bireylerin hastalık tanısı konulmuş ve bilinen vakalara yakınlıklarını ölçmek büyük önem kazanmıştır. Bu nedenle dünyanın dört bir yanındaki hükümetler, virüsün yayılımının bulunmasına yardımcı olmak için mobil konum verilerinin kullanılıp kullanılmayacağını ve nasıl kullanılacağını düşünmeye başlamıştır.

Ocak ayından bu yana tüm dünyada mevcut olan kişi izleme uygulamalarının sayısında keskin bir artış olmuştur. Bu uygulamaların, bireyleri ve temas ettikleri diğer bireyleri izlemek için konum verilerini kullanarak virüsün yayılmasını engellemeye yardımcı olmak için tasar-

landığı iddia edilmiştir. Bu uygulamaları geliştirenlerin niyetleri iyi olsa da, uygulamalar hem etkinlik hem de önemli derece gizlilik endişelerini beraberinde getirmektedir. Birçok çalışmanın gösterdiği gibi, anonimleştirilmiş bazı veri setleri bile yeniden tanımlanma riski altındadır.[1] Ayrıca, açık gizlilik politikalarının bulunmaması ve merkezi veri depolamasının kullanılması, verilerin kötüye kullanıma karşı savunmasız olma olasılığını artıracaktır.

[1] https://cpg.doc.ic.ac.uk/blog/fighting-covid-19/

I. KONUM VERİLERİ HAKKINDA[2]

Konum verileri, bir cihazın temel işlevlerinin parçası olarak cep telefonu operatörleri ve işletim sistemi üreticileri; kullanıcılara çeşitli özellikler sağlayan mobil uygulama üreticileri; aktif olarak bir ağa bağlı olmasalar bile izlenmelerine olanak tanıyan ve tanımlayıcı bilgiler yayan akıllı eşya veya oyuncak -nesnelerin İnterneti (IoT) cihazları- üreticileri tarafından kayıt altına alınmaktadır. Devletler tarafından çeşitli vasıtalar ile bireylerin konum verilerine yasal olarak yetki verilmiş kurum ve kuruluşlarca gerek yasal gerekse yasal olmayan yöntemler ile erişilebilmektedir.[3] Ancak pandemi süreci kurum ve kuruluşların bu acil ve olağanüstü durumu bahane ederek ve fırsat bilerek hiçbir engel ile karşılaşmaksızın ve herhangi bir açıklama yapmaksızın, konum verilerini süresiz saklama ve kullanma yetkisine dönüşebilir.

Hassas konum verileri veya "mobil veriler", cihazların ve kişilerin zaman içinde iç ve dış mekanlarda nasıl hareket ettikleri hakkında bilgiler içerir. Bir cihazın en basit bağlanabilirlik özelliği veya cihazlarda kablosuz içerik gönderme ve alma yeteneği, bu cihazların bulunduğu yer hakkında bilgi içermektedir. Örneğin, kablosuz servis sağlayıcıları, cihazları yerel baz istasyonları ve ağlar üzerinden sağladıkları için cihazların nerede bulunduğunu bilirler. Daha genel bir düzeyde, bir IP adresi (İnternet trafiği göndermek ve almak için cihazlar tarafından serbestçe ve açıkça paylaşılan bir tanımlayıcı) bir kişinin şehrini ve ülkesini bilmek için genellikle yeterlidir.

Çoğu zaman konum verileri denildiğinde, GPS (Global Positioning System, Küresel Konumlandırma Sistemi) düşünülür. Ancak GPS, cihazların konumunu belirlemek için kullanılan yollardan birisidir. GPS, işletim sistemleri, telefon operatörleri, mobil uygulamalar ve ağa bağlı diğer cihazlar tarafından çoğunlukla da diğer yöntemlerle birlikte kullanılır.

[2] Bu bölüm https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/ web sitesindeki bilgilerden alıntılanarak kısaltılmış ve derlenmiştir.

[3] Türkiye'de Elektronik Haberleşme Kanununun 51. Maddesine göre trafik ve konum verileri telefon operatörleri tarafından işlenebilmektedir.

GPS, dünya üzerinde herhangi engelsiz bir görüş hattında, dört veya daha fazla uydusu ile her türlü hava koşulunda yer ve zaman bilgileri sağlayan uzay tabanlı uydu navigasyon sistemidir.[4] Akıllı telefonlar ve diğer cihazlar, herhangi bir telefon veya internet alımından bağımsız olarak GPS üzerinden konumu algılayabilir.

Baz istasyonları kullanıcılara ağ erişimi sağlarlar. Herbir istasyon eşsiz bir numaraya sahiptir. Cep telefonları kendisine yakın bu istasyonlardan birine bağlanır. Bu aynı zamanda mobil operatörlerin konumumuzu yaklaşık olarak bilebilmesi anlamına gelir. Ayrıca HTS kayıtları olarak bilinen Historical Traffic Search, kişilerin telefonlarıyla gerçekleştirdikleri görüşmelerin arayan, aranan; arama zamanı, arama süresi, arama yeri ve sinyal alınan baz istasyonları gibi bilgileri kapsar.

Wi-Fi ağlarına bağlanma durumundaysa, mobil cihazlar, yakındaki Wi-Fi ağlarını tarayarak konumlarını belirleyebilirler. Yakındaki ağlar veya "erişim noktaları", örneğin komşuların Wi-Fi'ları veya kafe ve mağazalarda bulunan Wi-Fi'yi içerebilir. Konumları bilinen kablosuz ağ yönlendiricilerinin (router) benzersiz tanımlayıcılarıdan (MAC adresleri ve SSID) oluşan büyük veritabanları mevcuttur. Bu ağlardan birine bağlanan cihazın konumu büyük bir kesinlikle belirlenebilir.

Bluetooh özelliğini kullanan birçok uygulama, tek yönlü Bluetooth sinyalleri yayan küçük radyo vericilere sahip "donanımlara" (beacons) olan yakınlıklarını algılamak için tasarlanmıştır. Bu donanımlar oldukça ucuz ve hemen heryere veya herşeye kolayca iliştirilebilirler. Örneğin bir mağaza kapısına veya mağaza raflarındaki bir ürüne kurulablilir. Kullanıcının Bluetooth'a erişim izni verdiği bir uygulama cihazın konumunu çıkarabilir, mağazanın önünden geçmekte olduğunuzu veya ürünle ilgilendiğinizi anlayabilir, yakınlığa dayalı uyarılar veya başka içerikler gönderebilir. Bu cihazın konumumun oldukça hassas bir şekilde belirlenebilmesi anlamına gelir.

Her bir konum verisi elde etme yöntemi farklı bir hassasiyet seviyesi gerektirir ve farklı amaçlar için kullanılabilir. Birçok hükümet ve devlet kurumu, nüfus düzeyindeki eğilimleri ve hareketleri gözlemlemek için "anonim" veya "anonim ve toplu" konum verilerine erişmekle ilgilenmektedir. Bazı durumlarda verileri anonim hale getirmek mümkün olsa da, her bir kesin konum verisi ve veri kümesini gerçekten "anonim" hale

[4] https://tr.wikipedia.org/wiki/GPS

getirmek çok zordur. İsimler yerine benzersiz tanımlayıcılar kullanılsa bile, çoğu insanın davranışları, örneğin evlerinin konumundan (cihazın açık olup olmadığı, saat kaçta açıldığı v.b. bilgiler) kolayca izlenebilir. Her ne kadar konum verileri açısından benzersiz kimlik tanımlayıcı işaretler kullanılsa bile; konum verisi ile bir kaç bilgi yan yana geldiğinde kişi ya da grupların kimliği açığa çıkarılabilir.[5]

Bu konuda yapılan bir araştırmaya göre, basitçe anonimleştirilmiş bir veri kümesi, ad, ev adresi, telefon numarası veya diğer belirgin tanımlayıcıları içermez. Ancak, bireyin kalıpları yeterince benzersizse, verileri bir bireye geri bağlamak için dış bilgiler kullanılabilir.[6] Örneğin, benzersiz kimlik tanımlayıcı ile anonim hale dönüştürüldüğü varsayılan bir tıbbi veri tabanına ulaşabilecek kötü niyetli bir kişi, farklı bir kişinin sağlık kaydını bulmak için, konum verileri ve halka açık bir seçmen kaydı listesi ile tıbbi veri tabanı birleştirerek istediği kişiyi başarıyla tanımlanabilir hale dönüştürebilir.

Verileri anonimleştirmeye ilişkin bu tarz zorlukların üstesinden gelmek çok zordur ancak politika belirleyiciler aşırı ödün vermemeye çok dikkat etmeli ve konum verileri kümelerini özel ve hassas veri olarak ele almalıdır.[7] Konum verilerine kimin erişebileceği ve hangi amaçlarla kullanılabileceğini öngörerek ve veri kaydının sınırlı kalmasını sağlayarak; konum verileri hakkında idari, teknik ve yasal denetimlerin arttırılması gerekmektedir.

[5] https://www.nature.com/articles/srep01376

[6] https://dl.acm.org/doi/abs/10.1145/2030613.2030630

[7] https://www.nature.com/articles/sdata2018286

II. COVID-19 SÜRECİNDE DÜNYADA KULLANIMA AÇILAN TEMAS TAKİP PROGRAMLARI VE ALINAN ÖNLEMLER

Privacy International tarafından devletlerin gözetim ve izolasyon takip uygulamalarına ilişkin bir dizi haber takip edilip derlenmiştir. Derleme takipçilerin bildirimlerine göre teyit edilerek güncellenmekte- dir.[8]

GDPRHub, tüm dünyada yeni koronavirüsle savaşmak için kişisel verileri kullanan projelerin bir listesini toplamaktadır. Liste, merkezi olmayan kişi izleme uygulamaları ve çerçeveleri gibi kategorilere ayrılmıştır. Listede merkezi temas izleme sistemleri, kilit uygulamalar, öz değerlendirme uygulamaları, harita projeleri ve istatistiksel analizler de içermektedir.[9]

Çalışmanın bu kısmında bazı devlet uygulamaları ile ilgili kısa örnekler ve bilgiler yer almaktadır:

Birleşik Krallık

İngiltere Ulusal Sağlık Hizmetleri'nin (NHS) dijital kolu olan NHSX Oxford Üniversitesi'nden bir ekip ile COVID-19'un yayılmasını izlemek için bir iletişim izleme uygulaması geliştirmiştir.[10] Uygulama bireyin kaydolması esasına göre çalışacak ve insanları bölgelerindeki yeni vakalara karşı uyaracaktır. *The Guardian*'ın haberine göre, İngiltere'deki en büyük telefon operatörü şirketleri hükümetle telefon konumu ve kullanım verilerinin, evde kalmanın etkinliğini ölçmek için kullanıp kullanamayacağıyla ilişkili olarak görüşmelerde bulunmuştur.[11] İngiltere'deki O2 gibi diğer operatörler ise, hükümetin virüsün yayılması için modeller oluşturmasına yardımcı olduklarını ancak kullanıcı verilerini teslim etmediklerini belirtmiştir.

[8] https://privacyinternational.org/examples/tracking-global-response-covid-19

[9] https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

[10] https://www.digitalhealth.net/2020/03/nhsx-coronavirus-contact-tracking-app/

[11] https://www.theguardian.com/world/2020/mar/19/plan-phone-location-data-assist-uk-coronavirus-effort

Almanya

Der Tagesspiegel'in haberine göre, Alman mobil operatörü Deutsche Telekom, 17 Mart'ta, kullanıcılarının anonimleştirilmiş konum verilerini hastalık kontrolü ve önlenmesinden sorumlu bir araştırma enstitüsü ve devlet kurumu olan Robert-Koch Enstitüsü'ne iletti.[12] Almanya'nın temas izleme için merkezi Pan-Avrupa Gizlilik Koruma Proximity İzleme (PEPP-PT) standardını kabul edeceğini duyurduktan üç gün sonra, Sağlık Bakanı Jens Spahn bunun yerine Apple, Google ve diğer Avrupa ülkeleri tarafından desteklenen merkezi olmayan yaklaşımı kullanacaklarını duyurmuştur.[13]

Polonya

Polonya, 19 Mart'ta yurttaşların evde kalmasını sağlamak için, GPS konumu, zaman damgalı fotoğraflar ve yüz tanıma sistemlerini kullanan bir Ev Karantina uygulamasını başlattı. Uygulama, rutin olarak kullanıcılardan GPS konumlarıyla eşleşmesi gereken konumlarını paylaşmalarını istemektedir. Ayrıca, hükümetten mesaj aldıktan sonra 20 dakika içinde bölgede bir fotoğraf çekmeleri ve bir "görevi" tamamlamaları talep edilmektedir. Bu yapılmazsa, yetkililer tarafından kişiye karşı önlem alınabilir.

Bu uygulama aynı zamanda kullanıcıların karantinaya adım atmasına izin verilmeden önce yetkililer tarafından onaylanması gereken yemek, market ve psikolojik yardım taleplerini göndermelerine izin vermektedir. Uygulama sırasında açılan hesap aynı zamanda COVID-19 ile ilgili bilgilere ve karantinaya alınan kişileri denetleyen servislere doğrudan temasa geçecektir. Bu hesap, karantina süresi daha erken bitmediği sürece, etkinleştirme tarihinden itibaren 14 gün geçerli olacaktır. Devre dışı bırakıldıktan sonra bile, kişisel veriler 6 yıl boyunca saklanacaktır.

Kullanıcı uygulama aracılığıyla herhangi bir yeni belirtiyi veya yer değişikliğini yetkililere bilgilendirmekle yükümlüdür. Bilgiler polis merkezi ve Sağlık Bilgi Sistemleri Merkezi ile paylaşılmaktadır.[14]

[12] https://www.tagesspiegel.de/wissen/wie-breitet-sich-das-coronavirus-aus-rki-bekommt-handydaten-von-deutscher-telekom/25655144.html

[13] https://en24.news/e/2020/04/corona-app-jens-spahn-is-said-to-have-opted-for-controversial-pepp-pt-model.html

[14] https://www.gov.pl/web/cyfryzacja/pokonajmy-razem-koronawirusa--poznaj-protego-safe

Amerika Birleşik Devletleri

The Washington Post, Google, Facebook ve diğer büyük teknoloji firmalarının COVID-19'un yayılmasıyla mücadelede insanların konum verilerini kullanmak için ABD hükümetiyle görüşmelerde bulunduğunu bildirdi.[15] Şirketler, ABD'nin farklı bölgeleri arasındaki iletim şansını tahmin etmek için toplu ve anonimleştirilmiş verileri hükümetle paylaşacaklar. Önlemler, insanların fiziksel mesafe gibi devlet tarafından yürürlüğe konulan sınırlama önlemlerine uyup uymadığını kontrol etmek için de kullanılmaktadır.

İsrail

17 Mart'ta İsrail hükümeti, İsrail iç güvenlik kurumu Shin Bet'e COVID-19 olduğundan şüphelenilen veya onaylanan kişilerin cep telefonlarını izlemek için acil durum yetkisi vermeyi onayladı. 22 Mart tarihinde İsrail Sağlık Bakanlığı, enfekte kişileri ve temas çevresini saptamak için, İsrail'de terörle mücadele amacıyla geliştirilen Hamagen ("kalkan") uygulamasını kullanmaya başladı.[16] Uygulama İOS veya Android cihazlara yüklendikten sonra, uygulamanın hareketlerini izlediği ve elde edilen verileri enfekte kişilerin bulunduğu tüm yerleri listeleyen Sağlık Bakanlığı verileriyle karşılaştırdığı bildirildi.

İran

İran, kullanıcılardan hastalık belirtilerini ve coğrafi konumlarını isteyen ve en yakın test merkezlerini tavsiye eden bir uygulama geliştirdi. Ancak aslında uygulama kullanıcıların konumlarını izlemeye devam etmekte ve kullanıcıların oturma, yürüme v.b. fiziksel aktivitelerini kayıtlamaktadır. Bu iddialar siber güvenlik şirketi Avast tarafından desteklenmiştir.[17]

Hong Kong

Hong Kong zorunlu 14 günlük karantina uyulması sağlamak için 19 Mart'ta adaya gelen tüm yolcular üzerinde elektronik bileklikler takarak

[15] https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/

[16] https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus/

[17] https://blog.avast.com/iranian-coronavirus-app-collecting-sensitive-information-avast

uygulamaya başladı. Uygulamanın kişilerin karantinaya alınacakları yaşam alanının koordinatlarını izleyebilmesi için, kullanıcılardan evlerinin köşelerine yürümeleri ve ev alanını bildirmeleri istenmektedir. Bileklik kırılırsa veya akıllı telefon yaşam alanından çıkarılırsa Sağlık Bakanlığı ve polise bir bildirim gönderilir.[18]

Güney Kore

Science Magazine, Mart ayının ilk haftasında, İçişleri Bakanlığı'nın karantinaya alınanları takip etmek ve hastalık belirtileriyle ilgili veri toplamak için bir uygulama başlattığını bildirdi.[19] *Straits Times* haberine göre, temas takibi için Kore Hastalık Kontrol ve Önleme Merkezleri hastalarla görüşüyor ve kapalı devre kamera görüntüleri (CCTV) görüntüleri, kredi kartı kayıtları ile cep telefonu GPS verilerini kullanarak yerlerini doğruluyor.[20] Ayrıca, karantinada kendilerini izole etmeleri gerekenlere de konum verilerini aktaran bir bileklik takılmaktadır.[21] Bu konum izleme bileklik lerini takmayı kabul etmeyenlerin, karantina sırasında evlerinde değil, devlet tesislerinde kalmaları gerektiğini belirtmiştir. Bluetooth teknolojisi tabanlı bileklik, karantinadaki kişiler için bir mobil uygulamaya bağlanarak çalışmaktadır. Bileklik takanlar, akıllı telefonlarındandan 20 metreden fazla uzaklaştığında bir alarm tetiklenir ve bu alarm yetkilileri uyarır. Evlerinin sınırlarını terk eden veya belediye çalışanları ile telefon görüşmesi yapmayanlar karantina kurallarını ihlal etmiş sayılırlar. Bu gelişme sonucunda, yetkililer ve polis memurları kullanıcıyı takip etmek için harekete geçirilir.

Tayland

Tayland Ulusal Yayın ve Telekomünikasyon Komisyonu (NBTC), Çin, Makao, Hong Kong, Güney Kore, İtalya ve İran gibi yüksek riskli ülkelerden seyahat eden her Taylandlı ve yabancıya ücretsiz bir SIM kart vermektedir.[22] Bu SIM kart, AOT (Tayland Havaalanları) Havaalanları uygulaması ile birlikte kullanılarak, kullanıcıların 14 gün boyunca karantinada kalıp kalmadıkları takip edilecektir. Yetkilerin açıklamalarına

[18] https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html

[19] https://www.sciencemag.org/news/2020/03/coronavirus-cases-have-dropped-sharply-south-korea-whats-secret-its-success

[20] https://www.straitstimes.com/asia/east-asia/how-china-s-korea-and-taiwan-are-using-tech-to-curb-outbreak https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109

[21] https://yenimedya.wordpress.com/2020/04/24/guney-korede-karantinayi-ihlal-edenler-27-nisandan-itibaren-bileklik-takacak/

[22] https://www.nationthailand.com/news/30384226

göre uygulama 14 günün sonunda izlemeyi durduracak ve verileri silecektir. Kişiler SIM'i almayı veya AOT Airports uygulamasını indirmeyi reddederse, ülkeye girmelerine izin verilmemektedir.

Çin Halk Cumhuriyeti

Çin, kullanıcıların seyahat geçmişlerine ve kendilerine göre her kişiye renk kodları (kırmızı, sarı veya yeşil) atamak için Alipay veya WeChat aracılığıyla kaydolabilecekleri bir uygulama (Sağlık Kodu) ile ülke çapında bir sistem kullanmaktadır.[23] Rapor edilen sağlık durumuna göre atanan kodlar, bir kişinin özgürlüğünün sınırlanıp sınırlanmayacağını ve ne ölçüde kısıtlanacağını belirler. Sonrasındaysa uygulama aracılığıyla polisle konum verileri paylaşılır. Örneğin, *yeşil kod*, sahibinin kısıtlamasız hareket etmesini sağlar. *Sarı kodu* olan birinden yedi gün boyunca evde kalması istenebilir. *Kırmızı*, iki haftalık bir karantina anlamına gelmektedir.[24]

Singapur

21 Mart'ta Singapur hükümeti, enfekte kişinin takibinde yardımcı olacak bir uygulama olan TraceTogether uygulamasını yayınladı.[25] Uygulama, kişi ile yakındaki diğer telefonları tanımak için Bluetooth teknolojisi kullanmaktadır. Daha sonra zaman damgaları da dahil olmak üzere bu kişilere yakın olup olmadığınız takip edilmektedir. İhtiyaç ortaya çıkarsa, bu bilgiler daha sonra iki kullanıcı arasındaki karşılaşmanın yakınlığına ve süresine bağlı olarak yakın kişileri tanımlamak için kullanılabilir.[26] Bir kişiye virüs teşhisi konulursa, Sağlık Bakanlığı'nın yakın temasları tanımlamak için uygulamadaki verilere erişmesine kullanıcı izin verebilir. Veriler telefonun kendisinde 21 gün boyunca saklanır ve kişi, "yakın kişi" olarak tanımlanmadığı sürece verilere erişilmez. Bluetooth üzerinden iki telefon arasındaki iletişim için telefon numaraları anonimleştirilir.

Ayrıca Singapur'da hükümet, her bir pozitif COVID-19 vakası hak-

[23] https://yenimedya.wordpress.com/2020/03/02/buyuk-veri-cinin-korona-virus-savasinda-kamuoyunu-yesiller-sarilar-ve-kirmizilar-olarak-nasil-boluyor/

[24] https://www.cgdev.org/blog/covid-19-information-problems-and-digital-surveillance
https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay

[25] https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

[26] https://www.medianama.com/2020/03/223-surveillance-coronavirus/

kında ayrıntılı bilgi sağlayan çevrimiçi bir kontrol paneli tutmaktadır.[27] Örneğin vaka 199, 26 Şubat ile 2 Mart tarihleri arasında Malezya'ya seyahat eden ve diğer birçok COVID-19 vakasına bağlı bir camiye katılmış olan 37 yaşındaki bir erkeğe atıfta bulunmaktadır. Web sitesi aynı zamanda bu kişinin yaşadığı sokağın adını da vermektedir ve GrabFood şirketi için yemek dağıtım elemanı olarak çalıştığını ve Singapur'daki (adlandırılmış) bir camiyi ziyaret ettiğini not etmektedir.[28]

[27] https://co.vid19.sg/singapore/

[28] https://co.vid19.sg/singapore/cases/singapore-case-199-37-year-old-male-singapore-citizen

III. ULUSLARARASI KURULUŞLARIN PANDEMİ TAKİP UYGULAMALARINDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN AÇIKLAMALARI

BM özel raportörleri devletlerin insan haklarını bastırmak için acil durum önlemlerini kötüye kullanmamaları konusundaki açıklama yaparak, "Mevcut sağlık krizinin ciddiyetini kabul etsek ve önemli tehditlere karşılık uluslararası hukuk tarafından acil durum yetkilerinin kullanılmasına izin verildiğini kabul etsek de, devletlere, koronavirüse yönelik acil durum müdahalelerinin orantılı, gerekli ve ayrımcı olmayan olması gerektiğini acilen hatırlatıyoruz." [29] demiştir.

BM/DESA (Ekonomik ve Sosyal İşler Dairesi Başkanlığı) hükümetleri sağlık krizi hakkında şeffaf davranarak bilgi paylaşmaya çağırarak; kamuoyu dahil olmak üzere çeşitli paydaşları salgının yönetimine dahil etmek; kamu-özel sektör ortaklıkları için uygun gizlilik önlemleri ile paydaş ortaklıkları ve yenilikçi dijital teknolojilerin uygulanmasını hızlandırmaya yönelik açıklama yayınladı.[30]

Avrupa Komisyonu'nun Temas İzleme Uygulamaları Hakkında Tavsiye metni ile pandemi takip uygulamalarının kullanımı için koordineli bir yaklaşım önererek, anonim ve toplu mobil konum verileri yoluyla virüsün yayılmasını tahmin etmek ve modellemek için; temel ilkelere saygı ve bireylerin damgalanmaması, en az müdahaleci ama etkili araçların tercih edilmesi, teknik güvencelerin ortaya konulması, siber güvenlik önlemlerinin alınması, pandemi kontrolü sona erdiğinde alınan bu önlemlerin sona erdirilmesi, yakınlık verilerine dayanan anonim analiz ve uyarı sistemlerinin tercih edilmesi ve uygulamaların gizlilik ayarlarıyla ilgili şeffaflık sağlanması yönünde bir tavsiyelerde bulunmuştur.[31]

[29] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

[30] https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/

[31] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

Avrupa Komisyonu sağlık verilerinin kullanımına ilişkin *eHealth Network* metni yayınlayarak, AB'nin COVID-19 ile mücadelesinde izlemeyi destekleyen mobil uygulamalarda şu hususlara dikkat edilmesi önerilmiştir: Kişi izleme ve uyarı rolünün değerlendirilmesi, mevcut girişimlerin envanteri ve ulusal ölçekte kişi takibi için temel gerekliliklerin detaylandırılması, uygulamaların gönüllü, ulusal sağlık otoritesi tarafından onaylı, kişisel verilerin güvenli bir şekilde şifrelenmesi ve gerekli olmadığı anda kaldırılması gerektiği.[32]

Avrupa Komisyonu'nun *Veri Koruma ile İlişkili COVID-19 Salgınına Karşı Mücadeleyi Destekleyen Uygulamalar Rehberi* uygulamaların AB gizliliği ve veri koruma mevzuatına, özellikle GDPR[33] (Avrupa Birliği Genel Veri Koruma Tüzüğü) ve eGizlilik Direktifine uyumu sağlamak için yerine getirmesi gereken özellikleri ve gereksinimleri belirtir.[34]

Avrupa Birliği Avrupa Veri Koruma Kurulu (EDPB)'nun COVID-19 Pandemisine Karşı Mücadeleyi Destekleyen Uygulamalara İlişkin Kılavuz Taslağı yayınlayarak; Avrupa Birliği'ne dahil devletlerin veri koruma otoritelerini danışmaya davet etmiş ve hesap verebilir bir şekilde uygulamalar geliştirmesini, tasarımsal ve varsayılan özellik olarak gizliliği temel alan, açık kaynak kodlu, kriz bittikten ve herhangi bir veri silindikten veya anonimleştirildikten sonra sistemin acil durumlarda dahi kullanılmaması, gönüllü, güvenli ve birlikte çalışabilir olmaları da dahil olmak üzere kişi izleme uygulamaları için belirli önlemlerin teşvik edilmesi gerektiğini belirtmiştir. Devletlerin bu tür uygulamalar için yasal bir dayanak oluşturan ulusal yasaları yürürlüğe koymalarını, bireysel kullanıcıların konum takibinin gerekli olmadığı, sağlık yetkilileri ve bilim insanlarının bu uygulamaların temel fonksiyonel gereksinimlerini tanımlamak için sıkı bir zorunluluk testi geliştirmeleri gereğinin altı çizilmiştir. Merkezi olmayan uygulamaların daha fazla kullanılması gerektiğinin, minimum veri kaydına paralel olarak ve kişilerin sağlık otoriteleri tarafından test sonrası temaslarının tam otomatik olmayan yollarla sınırlandırılmasının, verilerin geri kullanılmaması ve zamanında silinmesinin, alınan önlemler ile uygulamayı kullananların temas kişilerinin yeniden tanımlanmasını önlenmesi gerektiğinin altını çizdi.[35]

Avrupa Veri Koruma Kurulu'nun (EDPB) COVID-19 Salgını Bağ-

[32] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[33] https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/

[34] https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf

[35] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

lamında Kişisel Verilerin İşlenmesi Hakkında Bildiri metni ise konum verilerinin kullanımı, istihdam, temel ilkeler ve işlemenin yasallığı hakkında kapsamlı bir kitapçıktır.[36]

AB Temel Haklar Ajansı'nın AB'deki Coronavirus Salgınında Temel Haklara İlişkin Bülteninin 4. Bölümünde işverenler ve medya kurumlarının veri koruma yetkilileri tarafından pandemi sırasında gizlilik ve veri koruma haklarının nasıl sağlanacağına ilişkin bilgiler verilmekte, özellikle veri işleme ana hatlarıyla açıklanmaktadır.[37]

Avrupa Komisyonu Başkanı Ursula von der Leyen ve Avrupa Konseyi Başkanı Charles Michel, 15 Nisan'da COVID-19 sınırlama önlemlerini kaldırmaya yönelik ortak bir Avrupa Yol Haritası imzaladı.[38] Ortak deklerasyona göre, veri gizliliğine saygı gösteren mobil uygulamaların kullanımı ile kişi takip ve uyarı uygulaması için bir çerçeve oluşturmak amaçlanmıştır. Enfeksiyon zincirlerini kesintiye uğratmaya ve daha fazla bulaşma riskini azaltmaya yardımcı olabildikleri için, pandemi takip uygulamaları 'artan test kapasiteleri de dahil olmak üzere diğer önlemleri tamamladıkları sürece üye devletlerin oluşturduğu stratejilerde önemli bir unsur olmalıdır. Mobil uygulamaların gönüllü olmaları ve ulusal sağlık otoritelerinin sistem tasarımına dahil edilmesi önerilmektedir. Önerilen güvenceler, verilerin anonimleştirilmesi ve toplanması, kullanıcıların izlenmesi ve yönetişim korumaları gibi bir dizi teknik güvencelerin bir karışımıdır. COVID-19 krizi sona erdiğinde şeffaf ve sona erme süresi belirli olan uygulama ile kaydedilen verilerin silinmesi ve uygulamaların devre dışı bırakılması gereklidir. Belgeye göre, bu uygulamalara duyulan güven ve gizlilik ve veri korumaya saygıları, başarıları ve etkililikleri için çok önemlidir.

EDRI'nin (Avrupa Dijital Haklar Örgütü) yapmış olduğu açıklamaya göre, "Devletler pandemi ile mücadelede dijital gözetim teknolojilerini kullanırken insan haklarına saygı göstermelidir. Üzerinde anlaşmaya varılmamış dijital gözetim gücündeki bir artış cep telefonu konum verilerine erişim elde etmek, gizliliği, ifade özgürlüğünü ve örgütlenme özgürlüğü haklarını ihlal edebilecek ve kamu makamlarına olan güveni azaltabilecek şekilde tehdit edebileceği gibi herhangi bir halk sağlığı müdahalesinin etkinliğini de baltalayabilir. Bu önlemler aynı zamanda ayrımcılık riski taşır ve zaten ötekileştirilmiş topluluklara orantısız bir

[36] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[37] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-1_en.pdf

[38] https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

şekilde zarar verebilir."[39]

Access Now, COVID-19 kişi izleme uygulamalarının kullanımında gizlilik ve halk sağlığı için yapılması ve yapılmaması gerekenlere dair bir dizi öneri hazırlamıştır.[40]

CCC (Chaos Computer Club) tarafından yapılan açıklama ile kişi izleme uygulamalarına ilişkin asgari 10 gereksinim sıralanmış ve "Prensip olarak, bir "Corona Uygulaması" kavramı, toplanabilecek temas ve sağlık verileri nedeniyle büyük bir risk içerir. Aynı zamanda son yıllarda kripto ve gizlilik toplulukları tarafından geliştirilen "tasarım gereği gizlilik" ilkelerine bağlı kalınarak, bu teknolojilerin yardımıyla, bir gizlilik felaketi yaratmadan pandemi takip uygulamalarının potansiyelini ortaya çıkarmak da mümkündür. Sadece bu nedenle, mahremiyeti ihlal eden ve hatta tehlikeye atan tüm kavramlar kesinlikle reddedilmesi gerektiği" belirtilmiştir.[41]

Privacy International tarafından farklı ülkeler tarafından uygulanan COVID-19 uygulamalarına ilişkin bir bilgilendirme listesi hazırlanmaya başlanmıştır.[42] Privacy International tarafından yapılan açıklamaya göre, "Bu tür uygulamaların başlangıç noktası yalnızca sağlığa yardımcı olmaktır. Uygulamalar pandemiye mücadelede halk sağlığını korumanın küçük bir parçasıdır. Herhangi bir önlem insana öncelik vermeli ve verileri en aza indirmelidir. İnsanların, verilerinin ve cihazlarının güvenli olduğuna emin olmaları ve bu küresel salgının sonunda verilerin yok edilmesi gereklidir."[43]

Avrupa Özgür Yazılım Vakfı'nın (FSFE) açıklamasına göre, "Özgür Yazılımlar, eksiksiz bir veri korumasını ve uyumlu bir kullanımı doğrulamak için yeterli şeffaflık sunar, böylece güvenli bir sistem kurulabilir. Güvenli bir ortamda küresel kod geliştirme işbirliğini mümkün kılan yalnızca Özgür Yazılım'lardır. Herhangi bir sahipli çözüm kaçınılmaz olarak sayısız izole edilmiş veri sızıntısına yol açacak ve böylece enerji ve zaman israfına neden olacaktır. Özgür Yazılım lisansları evrensel bir işbirliğinin yanı sıra herhangi bir yetki alanında yazılım kodlarının paylaşılmasına izin verir."[44]

[39] https://alternatifbilisim.org/stklardan-covid-19-ile-mucadele-dijital-hak-ve-ozgurluklere-saygi-cagrisi/

[40] https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/

[41] https://www.ccc.de/en/updates/2020/contact-tracing-requirements

[42] https://www.privacyinternational.org/examples/apps-and-covid-19

[43] https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps

[44] https://fsfe.org/news/2020/news-20200402-02.en.html

Electronic Frontier Foundation (EFF) tarafından yapılan açıklamaya göre, "EFF uzun zamandır hükümetlerin ve şirketlerin konum verileri, sağlık verileri ve kişisel ilişkilerimizin dijital gözetimine karşı ve büyük veri sistemlerinin hayatımızı açık kitaplara dönüştürmesine karşı mücadele ediyor. Bu tür veri işleme genellikle gizliliğimizi ihlal eder, özgür konuşmamızı ve ilişkilendirmemizi engeller ve azınlıklara farklı yükler getirir. Halk sağlığı yetkilileri COVID-19'u içermek için çalışırken büyük verilerin bir miktar kullanımı garanti edilebilir. Ancak, halk sağlığı uzmanları tarafından belirlendiği üzere tıbbi olarak gerekli olmalıdır; kişisel verilerin işlenmesi gerçek yeni ihtiyaçlar ile orantılı olmalıdır. İnsanlar uyrukları veya diğer demografik faktörler nedeniyle incelenmemelidir ve herhangi bir yeni hükümet yetkisinin, hastalık bulunduğunda sona ermesi gerekir."[45]

COVID-19 ile ilgili gizlilik ve veri koruma kaynaklarına ilişkin daha fazla bilgi için:

Future of Privacy Forum tarafından hazırlanan ve düzenli olarak güncellenmeye çalışan kaynak deposuna bu adresten ulaşabilirsiniz: https://sites.google.com/fpf.org/covid-19-privacy-resources

EDRI (Avrupa Dijital Haklar Örgütü) tarafından hazırlanan COVID-19 Sürecinde Dijital Haklara İlişkin Belge Havuzuna bu adresten ulaşabilirsiniz: https://edri.org/covid-19-digital-rights-document-pool/

[45] https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

IV. TÜRKİYE'DE COVID-19 SÜRECİNDE *HAYAT EVE SIĞAR* UYGULAMASI VE KİŞİSEL VERİLERİN KORUNMASI

6698 sayılı Kişisel Verilerin Korunması Kanununun 5.inci maddesinde kişisel verilerin işlenme şartları, 6.ncı maddesinde ise sağlık verilerinin dahil olduğu özel nitelikli kişisel verilerin işlenme şartları belirlenmiştir. Kanunun 6.ncı maddesinde özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenemeyeceği belirtilmekle birlikte sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği düzenlenmiştir.

Ayrıca Kanunun 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.

Dolayısıyla Kişisel Verilerin Korunması Kanunu kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis ve tedavi, kamu güvenliği, kamu düzeni gerekçeleri ile yetkili kurum ve kuruluşlar tarafından sağlık verileri gibi özel nitelikli kişisel verilerin ilgilinin açık rızası aranmaksızın, Sağlık Bakanlığı'nca işlenmesini mümkün kılmaktadır.

Kişisel Verilerin Korunması Kurumu tarafından da pandemi sürecinde kişisel verilerin korunmasına ilişkin çeşitli tarihlerde aşağıdaki açıklamalar yapılmıştır:

- 27/03/2020 tarihli açıklamaya göre, "Bu istisnai zamanlarda dahi veri sorumluları ve veri işleyenlerin, ilgili kişilerin kişisel verilerinin güvenliğini sağlamaları gerekmektedir. 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. Bu minvalde özellikle COVID-19 virüsüne karşı alınan önlemler kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri gerekli, amaçla bağlantılı, sınırlı ve ölçülü olmalıdır."[46]

- 07/04/2020 tarihli açıklamaya göre, "Uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin işlendiği görülmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanununun 5.inci maddesinde kişisel verilerin işlenme şartları, 6.ncı maddesinde ise biyometrik verilerin dâhil olduğu özel nitelikli kişisel verilerin işlenme şartları belirlenmiştir. Bu noktada, kişisel verilerin Kanunun 5.inci ve/veya 6.ncı maddesinde belirtilen şartlara uygun olarak işlenmesi gerekmektedir."[47]

- 09/04/2020 tarihli açıklamaya göre, "Kişilerin konum verilerinin sağlık durumlarıyla ilişkilendirilmek suretiyle işlenmesi sürecinde söz konusu verilerin üçüncü kişilerce ele geçirilmesi halinde ilgili kişiler bakımından ciddi zararlar ortaya çıkabileceği dikkate alınarak, ilgili kurum ve kuruluşların kişisel verilerin güvenliğini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri almaları ve bu verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde söz konusu kişisel verilerin silinmesi veya yok edilmesi unutulmamalıdır."[48]

[46] https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-

[47] https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu

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

HAYAT EVE SIĞAR UYGULAMASI

Sağlık Bakanlığı COVID-19 pandemisi nedeniyle üç farklı uygulamayı yaşama geçirdi. Bu uygulamalardan Korona Virüs Kontrolü Uygulaması (19 Mart 2020) ve Pandemi İzolasyon Takip Projesi (09 Nisan 2020) uygulamaları, Hayat Eve Sığar (18 Nisan 2020) uygulaması adı altında birleştirildi. Hayat Eve Sığar uygulaması Sağlık Bakanlığı'nın, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve GSM operatörleri (Türkcell, Türk Telekom, Vodafone) işbirliğiyle yaşama geçirdiği bir uygulamadır. Cep telefonu abonelerinin konum verilerine göre bulundukları konumu değiştirip, değiştirmedikleri izlenmektedir.

Uygulama ile Sağlık Bakanlığı, Mernis (Merkezi Nüfus Sistemi) bilgileri, E-Nabız sistemleri ile veri alış-verişi yapmaktadır.

Uygulama;

- COVID-19 testi pozitif ve tanı konulan kişileri,
- Tanı konulanlarla yakın temas/teması olanlar kişileri,
- Yaş gruplarına göre (65 yaş üstü, 20 yaş altı) sokağa çıkma yasağı getirilen kişileri

kapsamaktadır.

Uygulama;

- Evde izolasyon altında bulunması gereken kişilerin, evlerini terk ettiğinde kısa mesaj servisi aracılığıyla uyarılması,
- Bu kişilerle anında iletişime geçilerek, izolasyon bulunmaları gereken yere dönmelerinin istenmesi,
- Yapılan uyarıya uymayan ve ihlale devam edenlerin durumlarının ilgili emniyet birimleriyle paylaşılarak gerekli idari önlem ve yaptırımların uygulanması,
- Yol kontrolü yapan emniyet ekiplerinin, kişinin bilgilerini sorgulayarak izolasyon ihlali yapıp yapmadığını öğrenebilmesi

şeklinde gerçekleşmektedir.

Uygulama içeriğinde;

- Anket; Bugün kendinizi nasıl hissediyorsunuz?
- Harita üzerinde hastane, eczane, market zincirleri, metro ve duraklar gibi temel ihtiyaç noktalarına kolayca ulaşma,
- Yoğunluk; Salgının yoğun olduğu riskli bölgelerine yaklaşıldığında uyarı verilerek haritada anlık olarak yaklaşılmaması gereken alanların görülmesi,
- Ailem; aile bölümüne yakınlar eklenerek, kişinin onay vermesi durumunda konum bilgileri ve bulundukları bölgelere göre risk durumlarının görülüp takip edilebilmesi,
- Bilgilendirme

bölümleri bulunmaktadır.

Uygulamanın aydınlatma metninde aşağıdaki açıklamalara yer verilmiştir:[49]

Veri Sorumlusunun Kimliği: Bu uygulamada işlenen kişisel verileriniz Bakımından veri sorumlusu T.C. Sağlık Bakanlığıdır.

Kişisel Verilerin İşlenme Amaçları: Bu uygulamada aşağıda yer alan kişisel verileriniz, pandemi ile mücadele süresiyle sınırlı olmak üzere şu amaçlarla işlenmektedir, bilgisi yer almaktadır.

Kimlik verisi: TC Kimlik Numarası, baba adı ve doğum tarihi bilgileriniz, kimliğinizin doğrulanması amacıyla işlenmektedir. Bu verileri girmeksizin de uygulamayı bazı kısıtlamalarla kullanabilmektesiniz. Eğer TC kimlik Numarasını girmek istemezseniz, COVID-19 riskinizin hesaplanabilmesi için yaşınızı girmeniz gerekmektedir.

İletişim verisi: Uygulamayı ilk yüklediğinizde SMS ile gönderilecek olan kodu girmek ve telefonunuzu doğrulamak amacıyla GSM numaranız işlenmektedir. Her bir GSM numarası ile uygulamaya yalnızca bir kez kayıt olunabilmekte; aynı GSM numarası ile birden fazla kişinin uygulamayı kullanma imkanı bulunmamaktadır. Ayrıca, uygulamanın "Aile" sekmesinde takip etmek istediğiniz sevdiklerinize davetiye göndermek için, onların GSM numaralarını girmeniz veya kişi listesinden seçmeniz gerekmektedir.

[49] https://hesapp.saglik.gov.tr/hayat_eve_sigar_aydinlatma.pdf

Konum verisi: Konum bilginiz, harita üzerinde konumuzun gösterilmesi, bulunduğunuz bölgede COVID-19 pozitif ve risk yoğunluğunun harita üzerinden gösterilmesi, izolasyon altında bulunduğunuz lokasyonun belirlenmesi, bu lokasyonu terk etmeniz durumunda tarafınıza bildirim gönderilmesi ve ilgili makamlara bilgi verilmesi amaçlarıyla işlenmektedir.

Sağlık verisi: Sağlık bilgileriniz, COVID-19 riskinizin belirlenmesi amacıyla işlenmektedir. Yöneltilen sorulara vereceğiniz yanıtlara gören yakın sağlık tesisini ziyaretiniz istenebilecek veya periyodik aralıklarla hastalık belirtileriniz hakkında tarafınıza devam sorular yöneltilecektir.

Meslek verisi: Sağlık çalışanı olup olmadığınız ve eğer sağlık çalışanıysanız hastalarla temasınızı olup olmadığı bilgisi, hastalık riski seviyesini belirlemek amacıyla işlenmektedir.

Kişisel Verilerin Aktarımı: 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 paylaşılmaktadır.

HAYAT EVE SIĞAR UYGULAMASININ KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN İNCELENMESİ VE ÖNERİLER

Pandemi takip uygulamaları toplanabilecek konum verileri ve sağlık verileri nedeniyle büyük bir risk içermektedir. Tek başına konum verilerinin dahi 3 ya da daha fazla veri ile bütünleştirildiğinde bireylerin ya da toplulukların kimliğinin açığa çıkarılabileceği unutulmamalıdır. Ancak bazı asgari teknolojiler ve ilkeler göz önüne alınarak bir gizlilik ya da kişisel veri sızıntısı felaketine yol açmadan temas takip uygulamalarının geliştirilmesi de mümkündür. Bu anlamda teknik olarak önerilen ve uluslararası bazı metinlerden belirtilen ilkelerden aşağıda bahsedeceğiz. Bu ilkeler ve öneriler gerek Avrupa Komisyonu tarafından yayınlanan Sağlık Verilerinin Kullanımına İlişkin eHealth Network Metni, Avrupa Birliği Avrupa Veri Koruma Kurulu (EDPB)'nun COVID-19 Pandemisine Karşı Mücadeleyi Destekleyen Uygulamalara İlişkin Kılavuz Taslağı gibi resmi metinlerde, gerekse EFF (Electronik Frontier Foundation), EDRI (Avrupa Dijital Haklar Örgütü), CCC (Chaos Computer Club) gibi sivil toplum kuruluşlarının metinlerinde yer almıştır.

1. Anlam ve amaç

İrtibat ve konum izleme uygulamalarının kullanımındaki temel ön kabul, temas izlemenin enfeksiyon sayısını önemli ölçüde ve belirgin bir şekilde azaltmaya yardımcı olabileceği argümanıdır. Bu değerlendirmenin geçerliliği bilimsel verilerle desteklenmiş bilgilere dayanmalı ve halk sağlığı uzmanlarının sorumluluğu altında olmalıdır. Uygulama üzerinden kişi izlemenin yararlı olmadığı veya uygulamanın amacını yerine getirmediği ortaya çıkması durumunda uygulamanın kullanımı sona ermelidir. Uygulama ve toplanan tüm veriler yalnızca enfeksiyon zincirleriyle savaşmak için kullanılmalıdır. Uygulamaların amaç dışında diğer her türlü kullanımı teknik olarak önlenmeli ve yasal olarak yasaklanmalıdır.

2. Gönüllülük ve onay

Hem kişisel özgürlükler hem de etkili halk sağlığı müdahalesi nedeniyle, kullanıcılar virüsle ilgili konum izleme için oluşturulan bir uygulama gibi gözetim sistemlerine katılıp katılmamaya karar verme ve onay verme yetkisine sahip olmalıdır. Bu onay uygulamaların kullanılması için ön şart olmamalı; gönüllü, spesifik olmalı ve detaylı bilgilendirilme içermeli, herhangi bir zamanda geri alınabilir olmalıdır. Ayrıca bu uygulamalarda kullanıcı hakkında toplanmış verilerin yine kullanıcı tarafında depolanması mümkün olup, kullanıcının rızası ve onayı ile kurumlarla paylaşılması gereklidir. Hastalığın yayılımı ve hızı ile ilgili olarak uygulamanın önemli bir yer tutması, uygulamanın zorla kullandırılması ile değil, mahremiyete saygı duyan güvenilir bir teknoloji kullanılarak ve gönüllü olarak kullanılması ile mümkündür.

3. Şeffaflık

İrtibat ve konum izleme uygulamalarının, düzenli olarak kullanıcıların uygulamadaki etkinlikleri hakkında kullanıcıları bilgilendirmesi gereklidir. Uygulamalar sağlam güvenlik programları ile şifrelenmeli, üçüncü taraf denetimleri ve sızma testlerini içermelidir. Devletler ve hükümetler, uygulamaya ilişkin politikalarını ve eğitim materyallerini yayınlamalı ve aynı zamanda her bir temas izleme programının kullanımı ile ilgili istatistikleri ve diğer bilgileri mümkün olan en ayrıntılı şekilde düzenli olarak yayınlamalıdır.

Uygulamalar teknik güvenlik açısından, teknoloji ve gizlilik konusunda bilgili, bu alanda çalışan odalar ve sivil toplum örgütleri ile bağımsız denetçiler tarafından test edilmiş ve belgelendirilmiş olmalıdır.

Her bir programın etkinliği ve kötüye kullanımı konusunda bağımsız uzmanlar tarafından yapılan denetim sonuçlarını düzenli olarak yürütmeli ve yayınlamalıdır.

Devletler, ne tür idari, teknik ve hukuki önlemler aldıkları konusunda şeffaf olmalıdır. Kişisel bilgileri toplanan kişilerin, gizlilik çıkarlarını göz önünde bulundurarak, programlar vasıtasıyla hakkında toplanan verilere ilişkin taleplerine hükümetler tarafından tam olarak cevap verilmeli, bu konudaki şikayetler ile ilgili etkili bir başvuru hakkı tanınmalıdır. Kişiler gerektiğinde bu uygulamalarda işlenen kişisel verileri ile ilgili mahkemeye başvurma hakkına sahip olmalıdır. Aynı zamanda veri koruma otoriteleri tarafından onaylanmış güvenlik prosedürleri uygulanmalıdır.

4. Önyargı ve ayrımcılığa maruz kalmama

İrtibat ve konum izleme uygulamaları kişilerin sağlık, cinsiyet, yaş, dil, din, ırk, etnik köken, milliyet, göçmenlik statüsü veya engellilik gibi hassas verileri ile bütünleştirilebilir olmamalıdır. Pandemi sırasında veya sonrasında, bilimsel çalışmalar için olsa dahi kasıtlı olarak veya farklı bir şekilde kategorilere dayalı ayrımlar ve etiketlemeler yapılmamalıdır. Hükümetlerin halk sağlığı bilgilerine erişimi olduğundan, bu verileri sosyal güvenlik yasaları, çalışma yaşamına ilişkin yasalar, ceza yasası veya göçmenlik yasalarının uygulanması gibi başka amaçlarla kullanmamalıdır.

5. Veri minimizasyonu

İrtibat ve konum izleme uygulamaları halk sağlığı sorununu çözmek için gereken kişisel bilgileri mümkün olan en az miktarda toplamalı, saklamalı ve kullanmalıdır. Yalnızca uygulama amacı (virüs etkileşimi) ile ilgili ve gerekli olan minimum veri ve meta veriler saklanmalıdır. Bu nedenle de, kullanıcıların virüs ile temasa etmesine özgü olmayan herhangi bir verinin merkezi olarak toplanmaması gerekir.

Konum verilerinin başka herhangi bir veri ile eşleştirilmesine gerek bulunmamaktadır. Konum bilgileri, sağlık bilgileri gibi ek veriler telefonlara yerel olarak kaydedilirse, kullanıcılar bu verileri üçüncü taraflara iletmek veya hatta yayınlamak zorunda bırakılmamalıdır. Ayrıca konum verileri ve sağlık verileri, kimlik numaraları gibi hassas veriler telefonda yerel olarak güvenli bir şekilde şifrelenmelidir. Gerçek temas takibi amacının ötesine geçen, bilimsel araştırma amaçları için yapılan gönüllü veri toplanması açısından da uygulamanın ara yüzünde açıkça

ve ayrı bir onay alınmalı ve kullanıcılar tarafından herhangi bir zamanda iptal edilebilir olmalıdır.

6. Kullanım süresi ve kaydedilen verilerin kullanımının sınırlanması

İrtibat ve konum izleme uygulamalarında pandemi ve izolasyon amacı için toplanan verilerin toplanma süresi kesin ve net bir şekilde belirtilmeli, bu süre sonunda toplanan veriler tamamen silinmelidir. Kullanıcılar herhangi bir zamanda, kişisel verilerinin silinmesini talep etme hakkına sahip olmalıdır. Halk sağlığı bağlamının ve süresinin dışında, verilerin kullanılmayacağına ilişkin temas takip sistemleri hakkında ek yasal önlemler alınmalıdır.

7.Kullanıcı verilerini kaydeden merkezi sistemlerin kullanılması

Tüm verileri kaydeden ve her şeyi bilen merkezi sunucular olmadan, anonim bir kişi takibi, teknik olarak mümkündür. Kullanıcı gizliliğinin merkezi altyapı operatörünün güvenilirliğine ve yeterliliğine bağımlı olması teknik olarak gerekli değildir. Merkezi sistemler tarafından vaat edilen güvenlik önlemleri ve sistemin güvenilirliği kullanıcılar tarafından etkili bir şekilde doğrulanamaz. Bu durum diğer yandan yazılım mimarisi açısından etik sorunlara da yol açar. Etik bir uygulama geliştirme, kullanıcı verilerinin mümkün olduğu kadar yine kullanıcı da kalmasını ve dışarıya en az verinin çıkacağı şekilde bir mimariye sahip olmasını gerektirir. Bu nedenle uygulamalar ve sistemler, şifreleme, anonimleştirme, kaynak kodun doğrulanabilirliği yoluyla kullanıcı verilerinin güvenliğini ve gizliliğini garanti edecek şekilde tasarlanmalıdır.

Google, Apple gibi şirketler de dahil olmak üzere hiçbir merkezi otoriteye güvenilmemelidir. Temas takip ve irtibat uygulamalarının şeffaflığı ve geliştirilebilirliği açısından Özgür Yazılım (Free Software) olması gereklidir. Özgür Yazılımlar, eksiksiz bir veri koruması ve uyumlu bir kullanımı doğrulamak için yeterli şeffaflık sunar, böylece güvenli bir sistem kurulabilir. Güvenli bir ortamda küresel kod geliştirme işbirliği Özgür Yazılım vasıtasıyla mümkün kılınabilir. Herhangi bir şirket ya da merkezi otorite tarafından sunulan çözüm önerileri kaçınılmaz olarak sayısız veri sızıntısına yol açacaktır. Özgür Yazılım lisansları evrensel bir işbirliğinin yanı sıra herhangi bir yetki alanında yazılım kodlarının paylaşılmasına da izin verir.[50] Böylelikle bir ülkede geliştirilen çözümler

[50] https://fsfe.org/news/2020/news-20200402-02.en.html

başka bir ülkede yeniden kullanılabilir, benimsenebilir olacak ve kollektif bir yapı ortaya çıkacaktır.

8. Gizlilik ilkesine göre tasarım

Bu uygulamalar sadece gizlilik ilkesine dayandıklarında, inandırıcı düzeyde sosyal kabul elde edilebilir. Kriptografi ve anonimleştirme teknolojileri gibi doğrulanabilir teknik önlemler ile kullanıcının gizliliği sağlanmalıdır. Yazılımın geliştirilmesi aşamasında etik bir ilke olarak **gizlilik ilkesine göre tasarım** benimsenmelidir. Bu ilkeye bağlı olarak kullanıcılar, pandemi takip uygulamalarında kendi verileriyle ilgili herhangi bir kişi ya da kuruma güvenmemelidir.

9. Anonimlik

Uygulamalarda kablosuz teknoloji (örn. Bluetooth veya GPS) yoluyla oluşturulan temas izleme kimlikleri, üçüncü kişiler tarafından izlenememeli ve sık sık değiştirilmelidir. Bu nedenle konum verilerine eşlik eden telefon numaraları, kullanılan IP adresleri, cihaz kimlikleri vb. gibi iletişim verileriyle kullanıcı kimliklerini bağlamak veya bu verilerle birlikte kullanıcı kimliği türetmek uygun değildir. Kullanıcı kontrollü bir özel anahtara sahip olmadan kimliklerin yorumlanamayacağı ve bağlanamayacağı şekilde geçici kullanıcı kimliği oluşturmanın tasarımı mümkündür. Bu nedenle, geçici kullanıcı kimlikleri doğrudan veya dolaylı olarak kullanıcıları tanımlayıcı bilgilerden türetilmemelidir.

Ayrıca kullanıcılar için her ne kadar benzersiz kullanıcı kimlikleri oluşturulduğu belirtilse de bu durum tam olarak ve her zaman anonimliğin sağlandığı anlamına gelmez. Anonimlik kavramı, verilerinizin hiçbir zaman bir kişi ile ilişkilendirilecek şekilde geri döndürülememesi anlamına gelmektedir. Uygulama ve sistemler tarafından atanmış olan kullanıcı kimlikleri ile diğer veriler eşleştiğinde, veriler takma adlı veri haline dönüşür, yani tam anlamıyla anonim hale gelmez. Herhangi bir kişisel veri toplamadan veya kullanıcı kimliği türetmeden de temas takip uygulaması kullanmak mümkündür. Bu nedenle de merkezi sistemler tarafından kullanıcılar için kimlikler türetmek uygun değildir.

HAYAT EVE SIĞAR UYGULAMASINA ASGARİ GİZLİLİK İLKELERİ VE TEKNOLOJİLERİ AÇISINDAN BAKIŞ

Sağlık Bakanlığı tarafından, COVID-19 pandemisi nedeniyle 18 Nisan 2020'de hayata geçirilen *Hayat Eve Sığar* uygulaması 10 milyondan fazla kişi tarafından yüklenmiştir.

Hayat Eve Sığar Uygulaması; Bluetooth, GPS ve GSM operatörlerinden (Turkcell, Türk Telekom, Vodafone) alınan baz istasyonu bilgilerini kullanmaktadır. Bu uygulama ile T.C. Kimlik Numarası, baba adı ve doğum tarihi bilgileri, konum verileri, Mernis adres bilgileri, sağlık verileri, telefon numarası bilgileri işlenmektedir. Bu uygulama yüklendiğinde telefonu vasıtasıyla iletişim (baz istasyonu) verileri, rehberde kayıtlı kişiler, kamera, fotoğraf ve video, konum, yaklaşık konum (ağ tabanlı), kesin konum bilgileri (GPS ve Ağ Tabanlı), kablosuz bağlantı bilgileri, tam ağ erişimi bilgileri, Bluetooth cihazlarla eşleşme ve Bluetooth ayarları, ağ bağlantıları, Google hizmet yapılandırması bilgilerine erişebilir.

Kişisel veriler Sağlık Bakanlığı tarafından işlenmekte olup, veri sorumlusu Sağlık Bakanlığı'dır. Ayrıca İçişleri Bakanlığı ve Emniyet Kuvvetleri ile de veriler paylaşılmakta olup, veri paylaşımı yapılan tüm bu kurumlar da aynı zamanda veri sorumlusudur. Dolayısıyla verilerin toplanması ve eşleştirilmesinde merkezi sistem benimsenmiş, hatta birden fazla merkezi veri tabanı ile veri alışverişi yapılmasına izin verilmiştir. Uygulama aracılığıyla veri minimizasyonuna aykırı olarak ve halk sağlığı amacıyla alakalı olmayan birçok kişisel veri toplanmakta ve işlenmektedir.

Kullanıcıların uygulamadaki etkinlikleri hakkında kullanıcılara bilgilendirme yapılmadığı gibi, uygulamanın kullanımına ilişkin politikalar yayınlanmamıştır. Uygulamanın etkililiği ve kötüye kullanımı konusunda bağımsız uzmanlar tarafından herhangi bir denetim yapılmamış, bu hususa ilişkin bir rapor yayınlanmamıştır. Uygulamaya ilişkin ne tür idari, teknik ve hukuki önlemler alındığı, sızma testlerinin yapılıp yapılmadığı bilinmediğinden şeffaflık söz konusu değildir.

Kullanımının COVID-19 testi pozitif ve tanı konulan kişiler ve tanı konulanlarla yakın teması olanlar kişiler açısından zorunlu olduğu Sağlık Bakanlığı tarafından açıklanmıştır. Ayrıca teşhis ve tanı konulmayan kişiler tarafından uygulamanın Google Play ve ya Apple App Store mağazalarından indirilmesi mümkündür. Uygulamanın kurulum aşamasında

ilk istenilen telefon numarası verisinin Sağlık Bakanlığı ile paylaşılmasını takiben uygulama telefon operatörü bilgilerinize ulaşacağından ad, soyad, adres ve diğer abonelik bilgilerine siz onay vermemiş olsanız dahi erişecektir. Dolayısıyla uygulama etik olarak tasarım gereği gizlilik ilkesine uygun olmadığı gibi, kullanıcıların üçüncü kişiler tarafından belirlenebilirliği açısından her kullanıcıya anonim veya geçici bir kimlik türetip türetmediğinin tespiti mümkün değildir.

Uygulama Sağlık Bakanlığı tarafından geliştirildiğinden uygulamanın şeffaflığı, denetlenebilirliği, geliştirilmesi, açıklarının tespiti ve bu açıkların kapatılmasına ilişkin bağımsız geliştiriciler ve diğer kurumlar tarafından denetlenmesi mümkün gözükmemektedir.

Kullanıma sunulmadan önce hangi bilimsel verilere ve gerekçelere dayandığı açıkça ortaya konulmamış ancak yalnızca uygulamanın işlenen kişisel verilerin temel kullanım amacı açıklanmıştır. Uygulama, Türkiye'nin üyesi olduğu Avrupa Komisyonu tarafından yayınlanan *eHealth-Covıd-19 İle Mücadeleyi Desteklemek İçin Uygulamalarda Veri Koruma Kılavuzu*'na uygun değildir. Yeterli, açık bir bilgilendirme ve onay metni bulunmamaktadır. Yine veri koruma kılavuzunda bu tür uygulamaların ülkelerin yetkili veri koruma otoritelerinin denetiminden geçirilmesi ve bu veri koruma otoritelerinin denetimine tabi olması gerektiğini vurgulamaktadır. Uygulamanın gerekli ve yeterli kontrollerden geçirilip geçirilmediği, özellik hassas veri olan sağlık verilerinin ve diğer kişisel verilerin korunması açısından Kişisel Verilerin Korunması Kurulu gibi bu konuda yetkili kurumun denetimin geçirilip, geçirilmediği konusunda herhangi bir bilgi ve açıklama bulunmamaktadır.

V. SONUÇ

Akıllı telefonlara sahip milyarlarca insanın genellikle bu cihazlarda işletim sistemleri ve çeşitli uygulamalar kullandığını düşünürsek, insanlara ulaşmak ve cihazlarından kapsamlı veriler çekmek mümkündür. Kaldı ki, akıllı telefonların donanımları (Chip, işlemci ve antenler), işletim sistemleri (genellikle Apple ve Android), uygulama mağazaları (Apple App Store ve Google Play), platformlar (analiz şirketleri ve sosyal medya şirketleri) ve uygulamalar tarafından ticari sömürünün bir parçası olarak devam eden sürekli bir izleme ve gözetim hali hazırda uygulanmaktadır.

Facebook, Google, Apple v.b. büyük teknoloji şirketleri ve analiz şirketleri yıllardır çok ayrıntılı ve toplu olarak konum verilerini biriktirmektedir. Platformlar için tüm veriler ticari değer taşımakta ve platform ekonomisinin temel kaynağını üretmekte ve değeri yaratmaktadır. Devletlerin istedikleri takdirde Google ve Apple'dan, WeChat'den konum verilerini elde etmeleri de mümkündür. Ancak anlık veri takibi yapılabilecek, teknik olarak desteklenen "pandemi takip" uygulamaları hızlı ve etkili çözüm üretmek amacıyla COVID-19 virüsünün yayılmasını önlemeye yönelik bir araç olarak düşünülmektedir. Bu uygulamaların enfeksiyon zincirlerinin hızlı izlenmesi ve virüs etkileşiminin kesilmesine olanak sağlayacağı düşünülmektedir.

Genel olarak bu uygulamalar enfekte olmuş kişilerin ve temas ettiği kişilerin daha hızlı uyarılmasına, böylece kendilerini daha hızlı karantinaya alabilmelerine olanak sağlayabilir ve enfeksiyonun daha fazla yayılmasını önleyebilir. Ancak bu durumda dahi herhangi bir korona temas izleme uygulaması, ne kendimizi ne de temas ettiğimiz kişileri korumaya yönelik değildir. Önemle belirtmek gerekir ki, bu uygulamaların kullanılması COVID-19 pandemisinin sona ermesini yahut halk sağlığı krizine kesin çözüm üretilmesini sağlamayacaktır. Bu uygulamalar hükümetler tarafından gerekli sosyal güvenlik önlemleri alınmadan ve yeterli sağlık olanakları sağlanmadan, yurttaşların işlerini kaybetme gibi ekonomik kaygılar ortadan kaldırılmadan; kişilerin evde kalmalarını, so-

kağa çıkmamalarını, yakın temastan kaçınmalarını veya hastalığın sona erdirilmesini sağlamaz. Dolayısıyla asıl bu sosyal ve ekonomik önlemler alınmadan yalnızca teknolojik çözümler ve uygulamalar vasıtası ile halk sağlığı krizine çözüm üretilebilmesi mümkün değildir.

Bu anlamda teknolojik önlemler ve pandemi takip uygulamaları açısından hükümetler tarafından belirtilen önlemlere ve vaatlere güvenmek yeterli değildir. Temas izleme uygulamaları hükümetlerin büyük bir gözetim yetkisine sahip olmasını sağlayacağı gibi; kişilerin sağlık, cinsiyet, yaş, dil, din, ırk, etnik köken, milliyet, göçmenlik statüsü veya engellilik gibi hassas verileri işlendiğinden toplumda ciddi ve bir önyargı ve ayrımcılık yaratılması riski içerir. Uluslararası sözleşmeler ve Anayasa ile tanınan temel hak ve hürriyetlere ilişkin güvenceler halk sağlığı gerekçe gösterilerek bertaraf edilmemeli; özel hayatın gizliliği, kişisel verilerin korunması ve ifade özgürlüğü gibi hakların kullanımın engellenmesine ilişkin geniş kapsamlı istisnalar ve gözetimi derinleştirecek teknolojik uygulamalar kullanılmamalıdır.

2016 yılında Sağlık Bakanlığı'nın 33 hastanesine yapılan siber saldırı sonucu bir milyona yakın hasta verisinin çalınmış, bu saldırılar sonucunda kişilerin yalnızca sağlık bilgileri değil, diğer kişisel bilgileri de üçüncü kişiler tarafından elde edilmiştir. 2018 yılında sonuçlanan bir dava sonucu sağlık verileri de dahil olmak üzere birçok kişisel verinin Sosyal Güvenlik Kurumu tarafından üçüncü bir şirkete ihale ile satıldığı ortaya çıkmıştır. Yine 2019 yılı yerel seçimlerinde kişilerin sağlık verilerinin politik amaçlarla kullanılmasına Sağlık Bakanlığı'nın sessiz kalması, Türkiye'de Sağlık Bakanlığı ve diğer kurumların şeffaf ve güvenilir bir şekilde kişisel verileri depolayamadığını ortaya koymaktadır.

Bu olumsuz örnekleri de göz önüne alırsak, Hayat Eve Sığar uygulamasının bir an önce, şeffaf ve denetlenebilir şekilde, Türkiye'nin de taraf olduğu uluslararası sözleşmelerdeki kuruluşlarını tavsiyeleri doğrultusunda tanzim edilmesi gereklidir.

EK 1: Sivil Toplum Açıklaması

https://alternatifbilisim.org/stklardan-covid-19-ile-mucadele-dijital-hak-ve-ozgurluklere-saygi-cagrisi/

Derneğimizin de aralarında bulunduğu hak ve özgürlük temelinde çalışan çok sayıda örgüt, devletlere ve şirketlere koronavirüse karşı mücadelede dijital gözetim teknolojilerini kullanırken insan haklarına saygı gösterme çağrısı yaptı. Açıklamayı Ankara Üniversitesi İletişim Fakültesi Araştırma Görevlisi Hasan H. Kayış derneğimiz için çevirdi.

Devletler pandemi ile mücadelede dijital gözetim teknolojilerini kullanırken insan haklarına saygı göstermelidir

COVID-19 salgını, dünya çapında hükümetler tarafından büyük ölçekli ve koordineli müdahale gerektiren küresel bir halk sağlığı acil durumudur. Bununla birlikte, Devletlerin virüsü kontrol altına alma çabaları, büyük ölçüde genişletilmiş dijital gözetim sistemlerine başvuran yeni bir çağın başlangıcı için kullanılmamalıdır.

Biz, aşağıda imzası bulunan kuruluşlar, hükümetlerden pandemi ile mücadelede bireyleri ve nüfusları izlemek ve görüntülemek için dijital teknolojilerin kullanılmasının kesinlikle insan haklarına uygun bir şekilde yapılmasını sağlayacak şekilde liderlik göstermesini istiyoruz.

Teknoloji bu çaba sırasında halk sağlığı mesajlarını yaymak ve sağlık hizmetlerine erişimi artırmak gibi önemli bir rol oynayabilir ve oynamalıdır. Bununla birlikte, üzerinde anlaşmaya varılmamış dijital gözetim gücündeki bir artış cep telefonu konum verilerine erişim elde etmek, gizliliği, ifade özgürlüğünü ve örgütlenme özgürlüğü haklarını ihlal edebilecek ve kamu makamlarına olan güveni azaltabilecek şekilde tehdit edebileceği gibi herhangi bir halk sağlığı müdahalesinin etkinliğini de baltalayabilir. Bu önlemler aynı zamanda ayrımcılık riski taşır ve zaten ötekileştirilmiş topluluklara orantısız bir şekilde zarar verebilir.

Bunlar olağanüstü zamanlar ama insan hakları hukuku hala geçerli. Gerçekten de insan hakları çerçevesi, bireylerin ve daha geniş toplum-

ların korunması için farklı hakların dikkatle dengelenmesini sağlamak üzere tasarlanmıştır. Devletler, bir halk sağlığı kriziyle mücadele adına gizlilik ve ifade özgürlüğü gibi hakları göz ardı edemezler. Aksine, insan haklarının korunması halk sağlığını da teşvik eder. Artık hükümet ler her zamankinden daha fazla, bu haklara getirilen kısıtlamaların köklü insan hakları güvencelerine uygun olmasını sağlamalıdır.

Bu kriz ortak insaniyetimizi gösterme fırsatı sunuyor. İnsan hakları standartları ve hukukun üstünlüğü ile tutarlı olarak bu salgınla mücadele etmek için olağanüstü çaba gösterebiliriz. Hükümetlerin şimdi pandemiyle yüzleşmek için verdikleri kararlar gelecekte dünyanın nasıl görüneceğini şekillendirecek.

Aşağıdaki hükümler yerine getirilmediği sürece tüm hükümetleri COVID-19 salgınına artan dijital gözetim ile yanıt vermemeye çağırıyoruz:

1. Pandemiyi ele almak için alınan gözetim tedbirleri yasal, gerekli ve orantılı olmalıdır. Söz konusu tedbirler yasalar tarafından sağlanmalı ve uygun halk sağlığı yetkilileri tarafından belirlenen meşru halk sağlığı hedefleri tarafından gerekçelendirilmeli ve bu ihtiyaçlarla orantılı olmalıdır. Hükümetler aldıkları önlemler konusunda, dikkatle incelenebilmeleri ve uygunsa daha sonra değiştirilebilmeleri, geri çekilmeleri veya tersine çevrilmeleri için şeffaf olmalıdır. COVID-19 salgınının ayrım gözetmeyen kitle gözetimi için bir bahane olarak hizmet etmesine izin veremeyiz.

2. Hükümetler izleme ve gözetim güçlerini genişletirse, bu yetkiler zamana bağlı olmalı ve sadece mevcut salgını ele almak için gerektiği kadar devam etmelidir. COVID-19 salgınının süresiz gözetim için bir mazeret olmasına izin veremeyiz.

3. Devletler, sağlık verileri de dâhil olmak üzere kişisel verilerin daha fazla toplanması, saklanması ve bir araya getirilmesinin yalnızca COVID-19 pandemisine yanıt vermek amacıyla kullanılmasını sağlamalıdır. Pandemiğe yanıt vermek için toplanan, saklanan ve bir araya getirilen veriler kapsamla sınırlı, pandemiye göre zamana bağlı olmalı ve ticari veya başka herhangi bir amaçla kullanılmamalıdır. COVID-19 salgınının bireyin mahremiyet hakkını ihlal etmek için bir mazeret olmasına izin veremeyiz.

4. Hükümetler, toplanan kişisel verileri toplama, iletim, işleme ve depolamada kullanılan tüm cihazların, uygulamaların, ağların veya

hizmetlerin yeterli güvenliğinin sağlanması da dâhil olmak üzere, insanların verilerini korumak için her türlü çabayı göstermelidir. Verilerin anonim olduğu iddiaları kanıtlara dayanmalı ve nasıl anonimleştirildiği konusunda yeterli bilgi ile desteklenmelidir. İnsanların dijital güvenliğinden ödün verilmesine gerekçe olarak "salgına yanıt verme" girişimlerine izin veremeyiz.

5. Büyük veri ve yapay zeka sistemleri de dahil olmak üzere COVID-19'a müdahale ederken dijital gözetim teknolojilerinin her türlü kullanımı, bu araçların ırksal azınlıklara, yoksulluk içinde yaşayan kişilere, ihtiyaçlar ve yaşanmış gerçeklikleri büyük veri kümelerinde gizlenebilen veya yanlış temsil edilebilen diğer marjinal nüfuslara karşı ayrımcılığı ve diğer hak ihlallerini kolaylaştırma riskini ele almalıdır. COVID-19 salgınının toplumdaki farklı gruplar arasındaki insan haklarından yararlanma boşluğunu daha da artırmasına izin veremeyiz.

6. Hükümetler diğer kamu veya özel sektör kuruluşları ile veri paylaşım anlaşmaları yaparlarsa, bunu yasalara dayandırılmalı, bu anlaşmaların gizlilik ve insan hakları üzerindeki etkilerini değerlendirmek için gerekli bilgileri yazılı olarak, varsayılan hükümler, kamu gözetimi ve diğer güvenlik önlemleri ile kamuya açıklaması gerekmektedir. Hükümetler COVID-19 ile mücadele çabalarına katılan işletmelerin insan haklarına saygı duyduğundan emin olmak ve herhangi bir müdahalenin diğer ticari ve ticari çıkarlardan korunmasını sağlamak için gerekli özeni göstermelidir. COVID-19 salgınının, hükümetlerin üçüncü taraflarla topladığı ve paylaştığı bilgiler için insanları karanlıkta bırakacak bir mazeret olmasına izin veremeyiz.

7. Herhangi bir müdahale, hesap verilebilir önlemleri ve kötüye kullanıma karşı korumayı içermelidir. COVID-19 ile ilgili artan gözetim çabaları, güvenlik veya istihbarat teşkilatları alanına girmemeli ve uygun bağımsız organlar tarafından etkin gözetim altında tutulmalıdır. Ayrıca bireylere veri toplamak, bir araya getirmek, saklamak ve kullanmak için COVID-19 ile ilgili önlemleri bilme ve bunlara karşı çıkma fırsatı verilmelidir. Gözetime tabi tutulan bireylerin etkili hukuk yollarına erişimi olmalıdır.

8. Veri toplama çabalarını içeren COVID-19 ile ilgili müdahaleler, ilgili paydaşların, özellikle halk sağlığı sektöründeki uzmanların

ve marjinal nüfus gruplarının özgür, aktif ve anlamlı katılımı için araçlar içermelidir.

İmzalayanlar:

- 7amleh – Arab Center for Social Media Advancement
- Access Now
- African Declaration on Internet Rights and Freedoms Coalition
- AI Now
- Algorithm Watch
- Alternatif Bilisim
- Amnesty International
- ApTI
- ARTICLE 19
- Asociación para una Ciudadanía Participativa, ACI Participa
- Association for Progressive Communications (APC)
- ASUTIC, Senegal
- Athan – Freedom of Expression Activist Organization
- Australian Privacy Foundation
- Barracón Digital
- Big Brother Watch
- Bits of Freedom
- Center for Advancement of Rights and Democracy (CARD)
- Center for Digital Democracy
- Center for Economic Justice

- Centro De Estudios Constitucionales y de Derechos Humanos de Rosario
- Chaos Computer Club – CCC
- Citizen D / Državljan D
- CIVICUS
- Civil Liberties Union for Europe
- CódigoSur
- Coding Rights
- Coletivo Brasil de Comunicação Social
- Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
- Comité por la Libre Expresión (C-Libre)
- Committee to Protect Journalists
- Consumer Action
- Consumer Federation of America
- Cooperativa Tierra Común
- Creative Commons Uruguay
- D3 – Defesa dos Direitos Digitais
- Data Privacy Brasil
- Democratic Transition and Human Rights Support Center "DAAM"
- Derechos Digitales
- Digital Rights Lawyers Initiative (DRLI)
- Digital Rights Watch
- Digital Security Lab Ukraine
- Digitalcourage

- EPIC
- epicenter.works
- European Digital Rights – EDRi
- Fitug
- Foundation for Information Policy Research
- Foundation for Media Alternatives
- Fundación Acceso (Centroamérica)
- Fundación Ciudadanía y Desarrollo, Ecuador
- Fundación Datos Protegidos
- Fundación Internet Bolivia
- Fundación Taigüey, República Dominicana
- Fundación Vía Libre
- Hermes Center
- Hiperderecho
- Homo Digitalis
- Human Rights Watch
- Hungarian Civil Liberties Union
- ImpACT International for Human Rights Policies
- Index on Censorship
- Initiative für Netzfreiheit
- Innovation for Change – Middle East and North Africa
- International Commission of Jurists
- International Service for Human Rights (ISHR)
- Intervozes – Coletivo Brasil de Comunicação Social

- Ipandetec
- IPPF
- Irish Council for Civil Liberties (ICCL)
- IT-Political Association of Denmark
- Iuridicum Remedium z.s. (IURE)
- Karisma
- La Quadrature du Net
- Liberia Information Technology Student Union
- Liberty
- Luchadoras
- Majal.org
- Masaar "Community for Technology and Law"
- Media Rights Agenda (Nigeria)
- MENA Rights Group
- Metamorphosis Foundation
- New America's Open Technology Institute
- Observacom
- Open Data Institute
- Open Rights Group
- OpenMedia
- OutRight Action International
- Pangea
- Panoptykon Foundation
- Paradigm Initiative (PIN)

- PEN International
- Privacy International
- Public Citizen
- Public Knowledge
- R3D: Red en Defensa de los Derechos Digitales
- RedesAyuda
- SHARE Foundation
- Skyline International for Human Rights
- Sursiendo
- Swedish Consumers' Association
- Tahrir Institute for Middle East Policy (TIMEP)
- Tech Inquiry
- TechHerNG
- TEDIC
- The Bachchao Project
- Unwanted Witness, Uganda
- Usuarios Digitales
- WITNESS
- World Wide Web Foundation