
# COVID-19 SALGINI GÖZETİM TOPLUMUNU MEŞRULAŞTIRACAK MI?

TREND ANALİZİ NİSAN 2020

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

## 1. GİRİŞ

Birleşmiş Milletler Genel Kurulunun 16 Aralık 1966 tarihli Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17'nci maddesinde şöyle ifade edilmektedir: "Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez[1]."

Madde son derece açık. Ancak günümüzde sürekli yanımızda taşıdığımız akıllı cep telefonlarındaki onlarca uygulamadan yerküreye binlerce kilometre mesafedeki uydulara, neredeyse her sokak başında bulunan kapalı devre güvenlik kameralarından bize bir ürün ya da hizmet sunan bir şirkete kadar pek çok taraf yüz milyonlarca birey hakkında veri toplayabilmekte, bu verileri işleyebilmekte ve pek çok durumda elde ettiği verileri kâr amacı güden firmalara pazarlayabilmektedir. Yıllardır süregelen bu veri karmaşası, 2019 yılı sonunda Çin'in Wuhan kentinde ortaya çıkan ve dünya çapında yüzbinlerce insanı etkisi altına alan COVID-19 salgını ile kamuoyu gündemini daha fazla meşgul etmeye başlamıştır. Salgının bir anda dünyaya yayılmasıyla Çin'de polis memurlarının kalabalık halde yürüyen insanlara baktığında o kişilerin vücut ısılarının dijital kasklarının ekranına yansıdığı ya da İsrail hükümetinin istihbarat teşkilatına cep telefonu sahibi vatandaşlarının konumlarını anlık olarak belirleme yetkisi vermesi gibi haber ve görüntüler sosyal medyada yaygınlaşmıştır. Salgını kontrol altında tutmak isteyen hükümetler eskisinden çok daha fazla veri toplamaya ve bu verileri salgının önüne geçmek için daha yoğun ve farklı şekillerde kullanmaya çalışırken, salgın korkusu yaşayan insanların ise bu tip yeni uygulamalara eskiye nazaran daha az tepki göstermesi, bu girişimlerin normalleşip salgından sonra da kalıcı hale gelmesi endişelerini beslemektedir. Bildiğimiz dünyanın birkaç gün içinde başkalaşması ve devletlerin dijitalleşme ve teknolojinin imkânlarını daha güçlü şekilde hayata geçirmeye başlaması yaşadığımız günleri adeta George Orwell'in *1984* romanından çıkma sahnelere dönüştürmektedir.

COVID-19 salgınında yaşanan kaotik atmosfer insanları, salgının sonuçlanması için "ne gerekirse yapılması" düşüncesine sevk etmiştir. Örneğin, San Francisco'da yaşayan web geliştiricisi ve veri güvenliği aktivisti Maciej Cegłowski dahi, yayımladığı blog yazısında, salgının önüne geçilmesinin son derece zor olduğunu ve bu süreçte gözetim sistemleriyle toplanan verilerin, sağlık amacıyla da kullanılması gerektiğini dile getirmiştir. Bu sayede yetkililerin salgının etkisinin daha ciddi boyutlarda olduğu noktaları tespit edebileceğini, bunlara yönelik deneyler yapabileceğini, insanların çevreleri hakkında bilgi alabileceğini ve tüm veriler sayesinde bu tip çalışmaların mümkün olan en düşük bütçeyle yapılabileceğini savunan Cegłowski, yine de bu verilere erişimin sadece sağlık yetkilileri ve hükümetle sınırlı olması ve salgın akabinde sonlandırılması gerektiğinin altını çizmektedir[2].

Bugün Çin başta olmak üzere dünyanın dört bir yanında pek çok hükümet, bu salgının önüne geçmek için sözkonusu gözetim ağını genişletme ve bu ağ yoluyla elde edilen verileri pek çok farklı şekilde kullanma kararı almış; bu kapsamda virüsten etkilenmiş, etkilenmesi muhtemel olan ya da olmayan yüz milyonlarca kişinin dijital verilerini toplamaya ve işlemeye başlamıştır. Peki salgın korkusu kişisel verilerin korunması konusunda birtakım esneklikler doğurup, kamuoyu tepkisi "verilerin kamuoyu sağlığını korumak amacıyla işlenmesi" şartıyla yumuşamışken, yepyeni bir gözetim ağına giriyor olabilir miyiz? Bugüne dek ciddi tepkiler çeken gözetim kültürü,

insanlardaki virüs korkusu kullanılarak meşrulaştırılıyor mu? Bu analizde dünyada gözetim kültürünün nasıl ortaya çıktığını, bugüne dek nasıl evrildiğini ve COVID-19 salgını kapsamında yönetimlerin aldığı gözetim önlemleri ile geleceğe dair öngörüleri değerlendireceğiz.

## 2. GÖZETİM KÜLTÜRÜNÜN TARİHİ

Gözetim kültürünün evrimini irdeleme arayışında tarihte incelenmesi gereken ilk örnek, filozof ve sosyal teorisyen Jeremy Bentham tarafından 18'inci yüzyılda tasarlanan ve daha sonra Fransız filozof Michel Foucault tarafından 20'nci yüzyılda disiplin ve güç kavramları ışığında yeniden yorumlanan "Panopticon" modelidir. Panopticon, basit olarak bir mimari tasarım olarak tanımlanabilse de, modern gözetim kültürünün temelini oluşturan yapı olarak öne çıkmaktadır. Bir yapı içinde disiplinin tam olarak sağlanabilmesi için yapı içerisindeki bireylerin devamlı olarak gözetim altında tutulması ya da tutulduklarını düşünmesi gerektiği fikrini savunan sosyal reform savunucusu Bentham, bundan hareketle silindirik yapıya sahip, çevresinde koğuş ya da odaların sıralandığı, tam ortada bir gözetim kulesinin bulunduğu Panopticon'u 1785 yılında tasarlamıştır. Panopticon'un tam ortasında bulunan ve çevresinde sıralanan tüm hücreleri görebileceği açıyla yükselen gözetim kulesinin içi görülememekte; dolayısıyla içeride birinin olup olmadığı bilinememektedir. Kulenin içindeki görevlinin gözetimindeki her hücrede tek bir kişi kalmaktadır. Ancak gözetim altındaki kişiler kulenin içini göremediğinden, gözetim kulesinde her daim bir görevlinin bulunması gerekmez. Zira bu tasarımın ardındaki fikre göre, izlenip izlenmediğini bilememe durumu, yapıda bulunan kişilerin o an görevlinin onlara bakıyor olma ihtimali üzerinden kurallara her daim uygun davranmasıyla sonuçlanacaktır. Panopticon temelde bir hapishane olarak tasarlanmış olsa da, Bentham aynı modeli hastane, okul, sanatoryum ve akıl hastanelerine de uygulamayı planlamıştır. O dönemde Birleşik Krallık parlamentosunda beğeni alan, hatta Millbank Prison ismiyle hayata geçirilmiş bu yüksek güvenlikli yapı modeli, diğer yandan "baskıcı," "gaddarca" ve hatta "totaliter rejimin önünü açıcı bir fikir" olarak tanımlanıp ciddi eleştiriler almıştır[3], [4].

### 2.1 Modern Toplum Dev Bir Panopticon mu?

Panopticon modelinde "görünmez bir gözle" elde edilen kesintisiz disiplin, günümüz gözetim modellerinde makine kullanımıyla sağlanan "kesintisiz izlenme" sistemiyle paralellik çizmektedir. Peki COVID-19 bizim için yeni ve devasa bir Panopticon yaratıyor olabilir mi? Bu görüş, 2000'li yıllara geldiğimizde, cep telefonlarından güvenlik kameralarına uzanan gözetim ağlarından hareketle pek çok teorisyen tarafından savunulmuştur. COVID-19 salgınından çok daha önce bu görüşü dile getiren isimlerden biri de Michel Foucault'dur. Bu konuyu gözetim sisteminin çok daha etkili olmaya başladığı 1970'lerin ortasında ele alan Foucault, *Hapishanenin Doğuşu* eserinde Panopticon'u bir mimari yapı modelinden öte, modern toplumun bir yansıması olarak yorumlamıştır. Avrupa'da acıya dayalı disiplin sisteminin halka açık idamlar ve işkencenin yasaklanmasıyla zayıfladığını ifade eden Foucault, düzenin sürdürülebilmesi için yönetimlerin "gözetim gücüne" eğildiğini belirtmektedir ki bu, çok daha zor fark edilen, etkili bir güçtür. Onun sayesinde gözetimin sürdüğü toplumda birey sosyal normlara ceza korkusuyla değil, dominant inanç ve değerleri içselleştirmenin sonucu ortaya çıkmış doğal davranışlarıyla uyum sergiler. Yapılabilecek tüm "kural dışı" hareketler, görünmez bir göz tarafından izlenirken, düzen de güvence altına alınabilmektedir. Jeremy Bentham'ın Panopticon'u ise, içinde yaşanılan gözetim çağındaki modern toplumsal sistemi anlatan yekpare bir metafordur[5], [6]. COVID-19 esnasında veriler kamuoyu yararına toplanıyor olsa dahi, bu artırılmış gözetim ağının içselleştirilmesi ve dolayısıyla normalleştirilmesi tehlikesi, Foucault'nun teorisine göre mümkündür.

#### 2.1.1 Güney Kore'de Gözetim Uygulamaları Genişliyor

Peki bugün, özellikle salgının başladığı süreçten itibaren modern toplumda gözetim kültürü nasıl bir değişim göstermektedir? Örneğin yaklaşık yüzde 1'lik ölüm oranıyla süreci en iyi şekilde yönettiği düşünülen ülkelerden olan Güney Kore, ülkeye yurtdışından giriş yapan herkesin akıllı cep telefonlarına, -varsa- semptomlarını bildireceği bir uygulama yüklemesini zorunlu tutmaktadır[7]. 6 Nisan tarihi itibariyle toplamda 466 bin 804 test uygulayan Güney Kore[8], bu yöntemle tespit ettiği bireylerle etkileşime geçen potansiyel hastaları da, mevcut hastaların kredi ve banka kartıyla alışveriş geçmişleri, mobil telefon sinyalleri ve güvenlik kameralarındaki yüz tanıma sistemleri üzerinden tespit edebilmektedir.

Tüm bu süreç toplum sağlığı için son derece faydalı bulunurken, diğer yandan da bu gözetim verilerinin sadece sağlık otoritelerine değil, herkesin erişimine açık olduğunu belirtmekte fayda var. Yani Güney Kore'de ve bu teknolojiyi kullanan ülkelerde yaşayan herkes, akıllı telefonları üzerinden virüsle enfekte olmuş kişilerin konumunu görebilmekte. Bu durum, halkın paniğe sürüklenmesini ve aşırı yiyecek stoku yapmasını engellese de, liberal ve demokratik toplumlarda uygulanması zor bir yöntem olarak gösterilmektedir[9]. Zira sağlığa dair kişisel verilerin herkesin erişimine bu denli açık olması, gelecekte bu verilerle neler yapılabileceği henüz bilinmediği için, endişe verici bulunmaktadır[10]. Dünyanın en kapsamlı gözetim ağlarından birine sahip Güney Kore'de 2014 yılında yapılan bir araştırmada 8 milyon adet, yani 6,3 kişi başına bir adet güvenlik kamerası bulunduğu ortaya çıkmıştır. 2010 yılı verilerine göre, ülkede yaşayan ortalama bir birey günde tam 83,1 kez farkında dahi olmadan kapalı devre güvenlik kameralarına yakalanmaktadır[10]. 2018 verilerine göre ise son beş yılda ülkenin gözetim ağına, önceki döneme kıyasla yüzde 200'lük bir artış hızıyla 1 milyon güvenlik kamerası daha katılmıştır[11]. COVID-19 sonrası bu gözetim ağının ne kadar genişletildiği ya da genişletileceği merak edilmektedir.

### 2.1.2 Çin'de Gözetim Programını İndirmek Zorunlu

Dünyanın en ileri kameralı gözetim sistemine sahip ülkesi Çin'de BBC tarafından 2017 yılında çekilen belgeselde hükümetin veritabanında ülkede yaşayan hemen her bireyin görsellerinin mevcut olduğu; herhangi bir şahsın nerede olduğu bilgisinin yapay zekâ ile geliştirilmiş güvenlik kameralarının yüz tarama sistemi sayesinde sadece 7 dakikada bulunabildiği ifade edilmektedir. Bu sistem dahilinde Çin'de yaşayanların fotoğrafları arabalarıyla, akraba ve arkadaşlarıyla da eşleştirilmekte; böylece kişinin sadece nerede olduğu değil neler yaptığı ve kimlerle görüştüğü ile ilgili de daha ayrıntılı bilgi edinilebilmektedir. Yetkililer herkes hakkında veri toplandığını ancak bu verilerin sadece şüpheli durumlarda incelendiğini ifade etse de, bu veri depolarının hacker'ların saldırılarına karşı ne kadar güvende olduğu da sorgulanmaktadır[12].

Mevcut sistemi COVID-19 salgını sonrası geliştiren ülkede, artık herhangi bir kişi vatandaşlık numarasını kullanarak bir uygulamada profil oluşturabilmekte ve birlikte yaşadığı, çalıştığı ya da eğitim aldığı kişilerin, doktorunun, aile üyelerinin, onlarla aynı araçlarda seyahat etmiş insanların COVID-19 virüsü taşıyıp taşımadığını görebilmektedir[13]. The Baidu Inc. tarafından geliştirilen bir uygulama, COVID-19 test sonucu pozitif çıkan ya da virüsü taşıma ihtimali olan insanların gittiği yerleri haritada göstermektedir[14]. Sokağa çıkma yasağının kısa bir süre önce kalktığı ülkenin en çok kullanılan iki uygulaması[15] olan WeChat ve Alipay'e yüklenen bir diğer yazılım ise insanların seyahat edebilmek için kısa bir sağlık testini doldurmalarını zorunlu kılmaktadır. Koronavirüs semptomlarına verdikleri yanıtlara göre insanlara yeşil, sarı ve kırmızı etiketler verilirken, sadece yeşil etikete sahip kişiler evlerini terk edebilmektedir[16]. *New York Times*'ta yer alan 1 Mart 2020 tarihli haberde bu yazılımı yüklemenin zorunlu olduğu ifade edilirken, karantina dikte eden sistemin kaydolunduğu anda, kullanıcısı farkında olmadan yerel polise; şahsın adres, isim ve kimlik numarası gibi bilgilerini gönderdiği iddia edilmektedir. Haberde Çin merkezli firmaların hükümet ile sık sık veri paylaştığı, ancak bu paylaşımın nadiren doğrudan, yani aracısız olduğunun altı çizilmektedir[17].

Çin'de gözetim ağı bunlarla da sınırlı değil. Ülkede emniyet güçleri, potansiyel COVID-19 taşıyıcılarını saptayabilmek için yapay zekâ teknolojisiyle geliştirilmiş, vücut ısısı ölçümü yapabilen, maske takmayanları tespit eden başlıklarla kamuya açık alanlarda tarama yapmaktadır[18]. Bugüne dek ülke sokaklarına dezenfektan püskürtmede değerlendirilen drone'lar, artık hata oranı ancak yarım derece olan vücut ısısı ölçümleri yapabilmektedir[19]. Ülkede bir parkın yönetimi, tüm güvenlik görevlilerini, ziyaretçilerin kimliğini tespit edip vücut ısısını ölçen sanal gerçeklik gözlükleriyle donatmıştır[20]. Ülkedeki pek çok halka açık alanın girişinde emniyet güçleri tarafından kimlik ve etiket kontrolleri yapılmakta, her bir kişinin giriş izni, gittiği son yerler göz önünde tutularak verilebilmektedir. Human Rights Watch Araştırmacısı Maya Wang,

salgının Çin hükümetinin süregelen gözetim önlemlerini artırmak için bir katalizör görevi gördüğünü ve bu tekniklerin salgından sonra da kalıcı hale gelmesini beklediklerini ifade etmiştir[21].

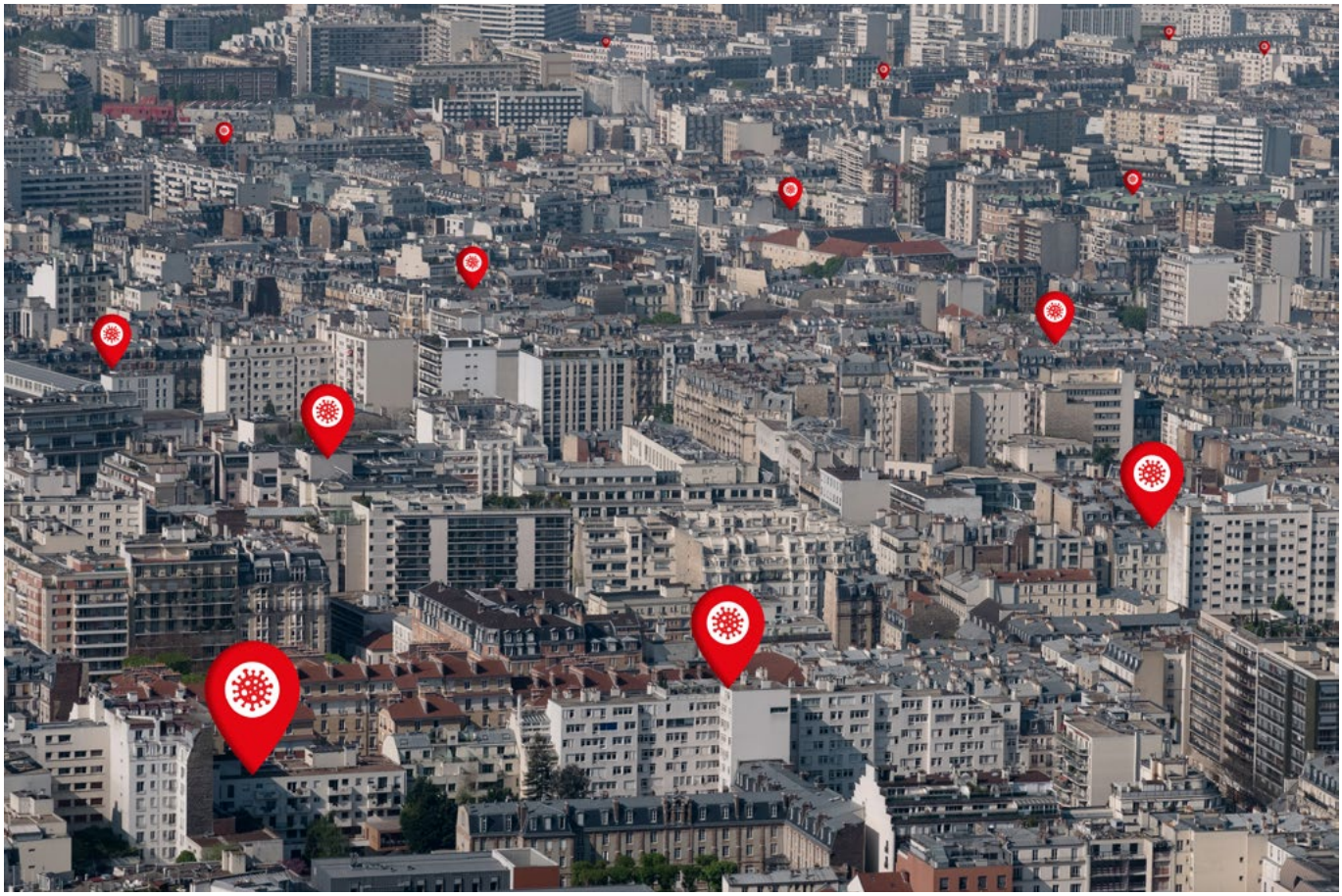
### 2.1.3 İsrail Tüm Vatandaşlarını İzliyor

Bir karantina merkezi oluşturan İsrail, bugüne dek terörle mücadelede kullandığı teknolojileri COVID-19 salgını kapsamında da değerlendirmektedir. İç İstihbarat Servisinin karantinadaki ya da virüsle temasa geçmiş olan vatandaşların mobil telefonlarına ulaşmasının önü açılmış durumdadır. Emniyet güçleri, karantinaya uymayan kişileri bu yolla tespit edip gözaltına almakta; temasa geçmiş kişilere ise kısa mesaj yoluyla ulaşarak karantinaya girmeleri için uyarıda bulunmaktadır[22]. Ayrıca ülkenin gözetim teknolojileri firmalarından NSO Group'un geliştirdiği yazılım sayesinde insanların nereye gittiği, kimlerle ne kadar süreliğine görüştüğü izlenebilmektedir. Yazılım analistleri seçtikleri, ancak rastgele bir kimlik atanmış özel bireye ait çoğu bilgiye erişebilirken, bu programın NSO Group'a ait Pegasus isimli, insanların mobil telefonlarına sızıp veri çalan zararlı yazılımla birlikte kullanılması soru işaretlerine sebep olmaktadır[23]. Ülkenin Savunma Bakanı Naftali Bennet, Nisan ayında bu arayüze ait bazı ekran görüntüleri paylaşmış; görüntülerde "4676 ile 661 13/03/2020'de buluştu" gibi bilgilerin yanı sıra kişilerin görüşmelerine ait konum ve süre bilgilerinin verildiği, hasta ya da şüpheli kişilerin konumlarının da paylaşıldığı görülmüştür[24]. Bennet aynı zamanda, çok yakında İsrail vatandaşlarının COVID-19 virüsüne yakalanmış olma ihtimalini 1 ila 10 arasında puan vererek bildirecek bir yapay zekâ sistemi üzerinde de çalıştıklarını, ancak bu teknolojinin henüz onay almadığını bildirmiştir[25]. Bu önlemlerin 30 günle sınırlı olduğunun altını çizen Başbakan Benjamin Netanyahu, "Demokratik bir ülke olarak vatandaş hakları ve kamu gereksinimleri arasında denge gözetmemiz gerekmektedir" açıklamasını yapmıştır[22].

COVID-19 salgınına karşı her yönetim kendi imkânları dahilinde gözetim önlemleri almaktadır. Örneğin Hindistan'ın güney kesimindeki Karnataka eyaleti, vatandaşların her saat başı hükümete evde olduklarını kanıtlayan bir özçekim göndermesini zorunlu tutmaktadır. Kişi fotoğrafını göndermezse bu bilgi karantina merkezlerine iletilmekte, gerekli görülürse kişi karantinaya alınmaktadır[26].

### 2.1.4 İtalya'da Gönüllü Gözetim

COVID-19'un 21 binden fazla can aldığı İtalya'da ise, Roma merkezli Cy4Gate isimli teknoloji firması, gözetim yazılımını ülke yönetimine ücretsiz olarak sunmaktadır. Kişilerin konumunu GPS, mobil veri sinyali ya da Bluetooth aracılığıyla belirleyen yazılımı geliştiren firmanın CEO'su Eugenio Santagata, veriyi devlete anonim olarak, yani kişisel verileri şifreleyerek sunduklarını; ancak devletin bu şifreleri kaldırabileceğini ifade etmiştir. İnsanların gönüllülük esasıyla kaydolarak dahil oldukları bu gözetim sisteminin birincil amacı, "virüsü taşıyan kişilerin kimlerle yakın temasta bulunduğunu bulmak" olarak açıklanmıştır[23].



### 2.1.5 Türkiye'de "Hayat Eve Sığar" Uygulaması

Türkiye ise, virüsten etkinlenmiş veya COVID-19 pozitif kişilerle temasa geçmiş kişilerin telefonlarına yüklemelerinin zorunlu tutulacağı bir uygulama geliştirmiştir. Türkiye Cumhuriyeti Sağlık Bakanı Fahrettin Koca tarafından 7 Nisan tarihli Bilim Kurulu toplantısı akabinde tanıtılan "Hayat Eve Sığar" isimli akıllı telefon uygulaması bireylerin hem konumunu takip edecek, hem de semptomlarına göre anlık durum sorgulaması yapmalarını sağlayacaktır. Uygulama ayrıca karantina kurallarının ihlal edildiğini, kişinin evini terk ettiğini saptarsa; güvenlik güçlerine haber verebilecektir. Ülkenin üç operatörü ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğinde Türkiye'de geliştirilen uygulamanın yakında kullanıma açılacağı ifade edilmektedir[27], [28].

### 2.1.6 ABD; Google, Facebook ve ClearView ile Masada

Amerika Birleşik Devletleri (ABD) hükümeti geçtiğimiz dönemde Google ve Facebook ile temasa geçmiş; virüse karşı savaşta akıllı telefonların konum bildirme özelliğinin kullanıldığı yeni bir işbirliği için adımlar atmıştır[29]. Ayrıca, Facebook'un Data for Good ekibi insanların sosyal mesafe kurallarına uyup uymadığını gösteren bir harita uygulaması için çalıştığını açıklamıştır. İnsanların hareketlerini popülasyon seviyesinde kaydedecek uygulama, nüfusun genel hareket eğilimlerini izleyecek, konum bilgilerini saklayacak, enfekte riski en yüksek bölgeleri belirleyebilecektir[30]. Facebook bu araştırma kapsamında elde edilecek verilerin gizli kalacağını belirtse dahi, ABD'nin 2016 Başkanlık Seçimleri'nde yaşanan Facebook veri manipülasyonu, güvenilirliği azaltmaktadır[31]. Bu manipülasyonu ABD Ulusal Güvenlik Dairesinin küresel gözetim programı verilerini sızdırarak ortaya çıkaran ve bunun sonucunda ülke dışına çıkmak zorunda kalan eski CIA ve NSA çalışanı Edward Snowden'in Facebook'u bir sosyal medya değil "istihbarat şirketi" olarak tanımladığını ve şirketin özel hayata ilişkin çok detaylı kayıtları toplayıp sattığını belirttiğini hatırlatmakta da fayda var. Çok kısa bir süre önce yüz tanıma sistemindeki; Facebook, YouTube ve Twitter'dan toplanmış 3 milyar fotoğrafın hacker'lar tarafından çalındığı iddia edilen Clearview AI şirketi de[32], *Wall Street Journal*'ın haberine göre, ABD'nin kamu kuruluşlarıyla görüşmekte; Camber Systems isimli bir start up üzerinden salgın süresince bireylerin konum değişimlerini izleyip veri depolamayı amaçlamaktadır[33].

COVID-19 salgınını konum verilerinin yanı sıra, diğer ülkelerde olduğu gibi termal kameralarla da kontrol altında tutmayı amaçlayan ABD, bu hedefle Athena Security isimli firmayla da masaya oturmuştur. Sipariş edilen yapay zekâ teknolojili termal kameralar, vücut ısısı yüksek kişileri tespit edecektir. Aynı firma daha önce de piyasaya, bıçak ve silahları tespit eden görüntü tanıma sistemi sunmuştu[34].

ABD hükümetinin gözetim ağını daha önce güvenilirliği sarsılmış Facebook ve Clearview AI gibi şirketlerle birlikte devam ettirmesinin yanı sıra bir diğer düşündürücü etmen de, 11 Eylül saldırısından sonra, "ABD demokrasisini yıkmaya çalışan iç ve dış düşmanlara karşı" çıkarılan, 2019 yılında yenilenen Vatanseverlik Yasası'nın uzatılmasının gündemde olmasıdır. Bireyleri Google aramalarına kadar takip edebilen çok kapsamlı gözetim önlemlerinin ulusal güvenlik gerekçesiyle yasal hale gelmesinin önünü açan, 11 Eylül döneminin tıpkı bugünkü COVID-19 salgınındaki gibi olağanüstü koşulları ve halktaki panik havası sebebiyle onaylanan yasa 15 Mart'ta tekrar görüşülmüş ve 77 günlük uzatma kararı alınmıştır[35],[36].

## 3. GÖZETİM TOPLUMUNDA KİŞİSEL VERİLERİN MAHREMİYETİ

ABD Hükümeti veri toplayadursun, 2019'un sonunda, *New York Times*'ın 12 milyondan fazla ABD'linin telefonuna ait 50 milyardan fazla lokasyon verisini elde edip bunu bir rapor halinde paylaştığını unutmamak gerekmektedir. Bir gazetenin devasa boyutlardaki kişisel veriye nispeten kolayca erişim sağlayabildiği düşünülürse, hangi veri gerçekten güvende olabilir? Raporda kaynağını açıklamayan *New York Times*, bunun sebebi olarak kaynağın buna yetkisinin olmamasını ve ciddi cezalarla karşılaşabileceğini öne sürmüştür. Hangi firmanın veritabanından alındığı bilinmeyen veri Beyaz Saray, Pentagon ve daha pek çok önemli noktadan telefon sinyal verisi içermektedir. Dahası, raporda Johnny Depp, Tiger Woods ve Arnold Schwarzenegger gibi isimlerin evlerine gelen misafirlerin de mobil veri aracılığıyla kısa sürede bulunduğu ifade edilmektedir[37]. Bunlar, sadece *New York Times*'ın uzaktan eriştiği veriler. Peki ya hükümetler, cep telefonumuzdaki uygulamaların sahibi olan firmalar ellerinde bizlere ait ne gibi veriler tutuyor olabilir? Salgının doğurduğu panik sürecinde bireyler gözetime her zamankinden fazla izin veriyorken, bu ağın nereye kadar uzayabileceğini öngörmek son derece zor görünmektedir.

### 3.1 Veri Güvenliği Niçin Önemli?

Kişisel verilerin toplanmasının bir sorun olarak görülmesinin elbette pek çok sebebi mevcuttur. Öncelikli kaygı, toplanan büyük boyutlu verilerin bunları kötü amaçla kullanacak kişilerin eline geçmesi ihtimaline yöneliktir. Daha önce bir akademisyen aracılığıyla Cambridge Analytica'nın Facebook verilerini nasıl elde ettiği ve ABD'nin 2016 Başkanlık Seçimleri öncesinde seçmeni manipüle etmede nasıl kullandığı, gündemi bugün bile meşgul eden bir konu olarak öne çıkmaktadır[38]. Aynı yıl 50 milyon Türkiye Cumhuriyeti vatandaşının TC kimlik numarası, açık adresi, doğum tarihi, aile bireylerinin isimleri gibi pek çok bilgisinin çalındığı iddia edilmektedir. "Bit kaydırma" isimli basit bir şifreleme sistemiyle korunan bilgilerin kolayca açık hale getirilebildiği belirtilmektedir. Çalınan bilgilerle kredi ve kredi kartı almanın, sahte kimlik çıkarmanın, e-devlet hesabı

açmanın ve online portal üzerinden tüm işlemleri yapmanın mümkün olduğu ifade edilmektedir[39]. Aynı zamanda 5 milyon Bulgaristan vatandaşının vergi idaresinde depolanan verilerinin[40], bütün Ekvador vatandaşlarının kimlik numarası, telefon numarası, eğitim ve iş geçmişi gibi bilgilerinin[41], 6,5 milyon İsrailli oy verenin kişisel bilgilerinin çalındığı iddia edilmektedir[42]. Toplanan verilerle, bu verilerin ait olduğu kişileri maddi zarara uğratacak girişimlerde bulunulabilir ya da herhangi bir şirketin rakibine karşı haksız bir üstünlük elde etmesinin önü açılabilir[43]. Üstelik, herhangi bir suç şebekesi, bir okulun sorunlu gençlere özel oluşturduğu veritabanını çalarak bunu gençleri suç dünyasına çekmek için kullanabilir. Veri güvenliğinin sağlanması tüm bu sebeplerle çok önem taşımaktadır.

Bugün veri güvenliği konusunda ne durumda olduğumuza bakmak gerekirse, akıllı cep telefonlarına yüklenen en basit uygulamalar arasında gösterilen el fenerlerinin bile kişisel verilere erişim konusunda nasıl tehlike saçabildiğini düşünmek yeterlidir. Google Play geçen yıl yaptığı açıklamada milyonlarca kişi tarafından kullanılan bu uygulamalarda verileri gizlice çalan yazılımlar bulunduğunu kabul etmiş ve kullanıcılarını uyarmıştır. 937 adet el feneri uygulamasını inceleyen Avast araştırmacısı Luis Corrons, kullanıcının talep ettiği hizmeti sağlamak için sadece telefonun kendi flaş ışığı, kilit ekranı ve reklamlar için internete erişim izni istemesi yeterli olan bu programların ortalama 25 farklı izin talep ettiği, bu izinler arasında ses kaydetme, telefon rehberini görüntüleme, yeni programlar yükleme, aramalar yapma ve kullanıcının lokasyonunu görüntüleme gibi hizmetle ilintisiz taleplerin olduğunu ortaya koymuştur[44], [45].

Bu basit el feneri yazılımları dahi kullanıcıların hangi gün nerede olduğunu, kimlerle ne konuştuğunu gözlemleyip bu bilgileri kullanabilirken; yüksek hacimli veri depolama, yüz ve/veya parmak izi tanıma sistemlerine sahip, bunları yapay zekâ teknolojisiyle işleyebilen teknoloji devlerinin veya hükümetlerin atabilecekleri adımlar kamuoyunda ciddi tartışmalara yol açmaktadır.

Buna ilave olarak, COVID-19 salgınıyla mücadele kapsamında kişilerden çoğu zaman bilgilendirme dahi yapılmadan toplanan verilere ne olacağı, verilerin toplanması amacıyla gerek özel sektör gerek hükümetlerce satın alınan yüksek teknoloji ürünü termal ve yüz tanıma sistemli kameraların salgından sonra kullanılmaya devam edilip edilmeyeceği de merak konusudur.

### 3.2 Veri Mahremiyetini Koruduğunu İddia Eden Gözetim Sistemleri

Salgın esnasında toplanan kapsamlı verilerin "daha az tartışmalı amaçlarla" kullanıldığı durumlar da mevcut. Örneğin İngiltere, ülkenin dört telekomünikasyon firmasıyla iletişime geçerek, uçuş kısıtlamaları sebebiyle yurtdışında mahsur kalmış Britanyalılara ulaşmak ve koordine uçuşlar planlayabilmek amacıyla kullanılacak veriler talep etmiştir[46]. Ancak bu gelişme de *Forbes* Yazarı Simon Chandler tarafından hükümetin vatandaşları hakkında daha fazla veri elde edebilmek için attığı bir adım olarak tanımlanmaktadır. Almanya'nın on binlerce vatandaşı için böyle bir veriye ihtiyaç duymadan ülkeye getirebildiğini hatırlatan Chandler, bu ve benzeri adımların Avrupa İnsan Hakları Sözleşmesi'ne aykırı olduğunu hatırlatmaktadır[47].

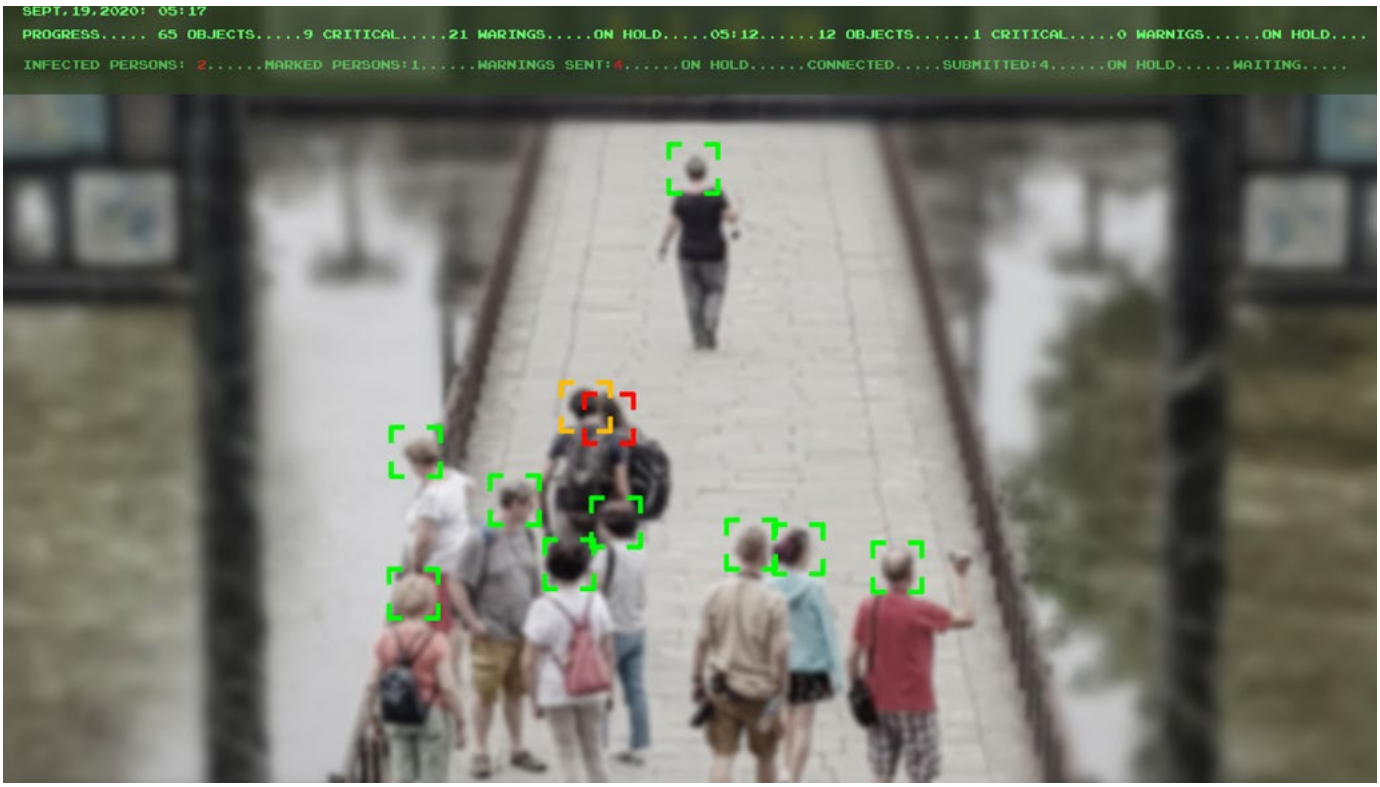
Dünyanın en sıkı veri koruma yasalarına sahip Avrupa ülkelerinde gözetim önlemleri nispeten daha ciddi tepkiler çekerken, Birleşik Krallık'ın talep ettiği veri bunlarla sınırlı kalmamaktadır. Ülkenin edindiği, henüz test aşamasındaki konum temelli gözetim sistemi de kamuoyu gündemini meşgul etmektedir. Çin'deki sistemin aksine indirmenin gönüllülük esasına dayalı olacağı ifade edilen bir akıllı telefon uygulamasının salgın boyunca kullanıcıların konum bilgilerini depolayacağı bildirilmiştir. Avrupa ve ABD'de Çin'deki gibi uygulamaların yapılamayacağını ifade eden Oxford Üniversitesi Bioetik Profesörü Michael Parker, kişisel veri ihlali tartışmalarına cevaben, "Bu teknolojileri kullanmanın pek çok yolu var. Demokratik bir ülkede yaşıyor olmamız başka insanları umursamamamız ya da sorumsuzca davranmamız gerektiği anlamına gelmez" cümlelerini kullanmıştır[48].

Avrupa Komisyonu da Nisan ayının ilk haftasında yaptığı açıklamada Avrupa Birliği üyesi ülkelerin dijital sistemlerin etkinliğini artırmak için birlikte hareket etmesi gerektiğini, diğer yandan, temel hak ve özgürlüklerin korunmasının elzem olduğunu bildirmiştir. Verilerin sıralanması, anonimleştirilmesi, yığılması, şifrelenmesi ve tek elden yönetilmemesi gerektiği ifade edilen açıklamada mahremiyete özen gösterilmesi gerektiği yinelenmiştir[49].

Aynı hedefle Avrupalı 25 güvenlik sistemleri uzmanı akademisyen tarafından tasarlanan, Bluetooth temelli gözetim programının, insanlara ait verilerin yanlış ve istenmeyen amaçlarla kullanımının önüne geçtiği iddia edilmektedir. Kişinin COVID-19 testinin pozitif çıkması üzerine devreye giren programdan, sağlık görevlileri, enfeksiyonun sürdüğü döneme ait verileri indirebilmektedir. Diğer yazılımlardan farklı olarak bu programda anonimleştirilmiş verilerin açığa çıkmasına, yani kişiye ait kimlik bilgilerinin bilinmesine gerek olmadığı ifade edilmektedir. İndirilen verilerle hastanın son dönemde gittiği yerler ve görüştüğü kişiler tespit edilerek yine kimliği gizli kalan bu kişilere de Bluetooth üzerinden mesaj gönderilmektedir[50].

Veri güvenliğini olabildiğince koruyan bir yazılım geliştirmeye çalışan bir diğer ülke de Fransa. Ülkenin Sağlık Bakanı Olivier Véran ve Teknoloji Bakanı Cédric O, yaptıkları açıklamada COVID-19'un yayılımını, yani insanların konumlarını ve yüz yüze görüşmelerini kayıt altına alacak bir uygulama üzerinde çalıştıklarını açıkladı. Sadece Bluetooth kullanarak gönüllülük esasıyla veri toplayarak uygulamanın 3-6 hafta arasında hazır olması beklenmektedir[51].

Alman kamu sağlığı yetkilileri ise Thryve isimli sağlık teknolojisi start up firmasıyla işbirliğine imza atarak akıllı saatlerle uyumlu ve COVID-19 yayılımının gözetimini sağlayacak *The Corona Data Donation*, yani "Korona Veri Bağışı" uygulamasını hayata geçirdi. Kişinin tansiyonunu, vücut ısısını, uyku rutinini analiz edip koronavirüs semptomları gösterip göstermediğini analiz eden uygulama, sadece gönüllüler tarafından, özellikle hükümet




tarafından alınan önlemlerin işe yarayıp yaramadığını tespit etmek amacıyla kullanılmaktadır. Sonuçlar interaktif bir haritada sergilenirken, hastaların posta kodu bilgisine kadar paylaşılan verilere herkes erişebilecektir[52].

### 3.3 Gözetim Önlemleri Salgından Sonra Devam Edebilir mi?

Diğer yandan, Avusturya merkezli telekomünikasyon firması A1 de kullanıcılarına ait verileri salgın süresince kamu sağlığı yararına olduğu sürece paylaşacağını beyan etmiştir[53]. Ülkenin teknoloji firması Rapid-Tech Equipment geliştirdiği yüksek vücut ısısı tespit eden kameraların Türkiye, Avustralya, Yunanistan, Suudi Arabistan, Fransa, Mısır, Cezayir, Fas ve daha pek çok ülkede kullanımda olduğunu açıklamıştır[54]. Termal görüntüleme kameraları geliştiren bir diğer firma olan ABD merkezli Testo'nun yetkilisi ise verdiği röportajda dünyanın dört bir yanından inanılmaz bir talep aldıklarını ifade etmiştir. İmza atılan kontratlar üzerinde yorumda bulunan Electronic Frontier Foundation Analisti Matthew Guariglia ise, "6 aylık olsalar da satın alınan kameraların kalacağından eminim" açıklamasında bulunmuştur[55].

### 3.4 Ülkeler Birbirine de Gözetimi Artırdı!

COVID-19 sebebiyle genişletilen gözetim ağları, diplomatik krizlere de sebep olmaktadır. ABD geçtiğimiz günlerde Çin'i, Güney Çin Denizi'ndeki hareketliliği gözetlemek ve yasa dışı müdaheleler yapabilmek amacıyla bir bahane olarak kullanmakla suçlamıştır. Çin'in sahil güvenlik gemisinin Vietnam bayraklı bir balıkçı teknesini batırması üzerine Pentagon'dan yapılan sert açıklamada, salgının ardından Çin'in, diğer Güneydoğu Asya ülkelerinin de hak iddia ettiği bölgelerde militarist faaliyetlerini artırdığına dikkat çekilmiştir. Çin Dışişleri Bakanı Zhao Lijan ise aynı dönemde ABD'nin Güney Çin Denizi'ne sürekli savaş jetleri gönderdiğini, Çin'in denizcilik haklarını ihlal ettiğini iddia etmiştir[56].

COVID-19 boyunca artan bir diğer gözetim ağı da üretim ve depolama tesislerini kapsamaktadır. ABD merkezli Ursa Space Systems şirketi müşterilerine, uydularının radar sisteminde gözlemlenebilen 11 bin petrol depolama tankerini uzaktan izleme ve salgının yarattığı etkileri görebilme imkânı sunmaktadır. Firmanın Global Enerji Analisti Geoffrey Craig, özellikle Çin'deki depoları izlemek için ciddi bir talep aldıklarını ifade ederken, bir diğer uydu verisi analiz firması SpaceKnow'un kurucusu Pavel Machalek ise beş yıldan uzun süredir Çin'deki 6.000'den fazla fabrikayı uydu verileriyle izlediklerini ve yeni dönemde salgının ülkedeki üretime etkisini incelemeye yoğunlaştıklarını ifade etmektedir[57].

COVID-19 ile beraber hükümetler, bireyler, üretim ve hammadde başta olmak üzere pek çok sektör arasında eskisine göre çok daha sıkı ve karmaşık bir gözetim ağı kurulmuş durumda. Brookings Institution Center'ın Teknoloji Departmanı Yöneticisi Darrell West, asıl tehlikenin bu durumun normalleşmesi ve pandemi sonrasında da sürdürülme ihtimali olduğunu hatırlatmaktadır. Foucault'nun 70'lerde ifade ettiği üzere, insanların zamanla bu gözetim ağını, yani attıkları her adımın, yaptıkları her internet aramasının izlenmesini normal bulmaya başlamasının mümkün olduğunu ifade eden başka uzmanlar da var. Washington Üniversitesi ve Stanford Üniversitesi bünyesindeki İnternet ve Toplum Merkezinde araştırmalar yapan Ryan Calo da, "Acil durumlarda uygulanan gözetimin en büyük tehlikesi, insanların bu iklime alışma ihtimalidir" demektedir[58].

### 3.5 Gözetime Rıza Gösterenler Artıyor

Salgın süresince gözetim ağının sadece hükümetler ve onların işbirliği yaptığı firmalarla sınırlı olmadığını da belirtmek gerekmektedir. Salgının 12 Nisan itibariyle 21 binden fazla can aldığı İtalya'da yapılan bir ulusal ankete göre[59], İtalyanların yüzde 63'ü insanların hareketlerini ve buluştukları insanları inceleyip veri haline getiren gözetim teknolojilerini desteklemektedir. Halkın yüzde 64'ü ise, karantinada olan insanların elektronik bilekliklerle gözetim altında tutulması gerektiğini düşünmektedir[60].

7 Nisan tarihli Open Democracy raporunda[60], panik döneminde gözetim cihazlarındaki artıştan ziyade, bireylerin bu tip önlemlerin artmasına yönelik isteğinin yükselişte olmasının çok daha önemli olduğuna dikkat çekilmektedir. İtalya özelinde hükümet drone'lar, dijital güç ve polis ekseninde gözetimi sürdürürken, insanların birbirini gözetleyerek bu ağın daha da genişlemesine katkıda bulunduğuna dikkat çekilmektedir. "Bireyler arası gözetim" olarak adlandırılan bu ağ kapsamında bireylerin, hükümetin aldığı karantina ve diğer önlemlere uymayan komşularını ihbar ettiği, sosyal medyada dolaşan ihbar niteliğindeki videoların arttığı belirtilen raporda, insanların balkonlardan gözetlenmekten rahatsız oldukları ifade edilmektedir. Bu dönemin gelecekteki ilişkileri elbette şekillendireceği vurgulanan raporda, ihbar edilen kişilerin "Korona yayıcı" ya da sorumsuz vatandaş olarak yaftalanabileceği ifade edilmektedir.

## 4. SONUÇ: 21'İNCİ YÜZYILDA 1984 DİSTOPYASINA MI DÖNÜYORUZ?

Birbirini ihbar eden komşular, sorumsuz vatandaş olarak yaftalanıp dışlananlar, gerek hükümet, gerekse etrafındakiler tarafından devamlı gözetlendiğinden şüphelenme, evinde bulunduğu an bile dijital araçlar vasıtasıyla takip edilip dinlenme ihtimali, çoğunluğun bu gözetim kültürünü normal bulmaya başlaması ve hatta artmasını istemesi... Hiç şüphesiz tüm bunlar bize George Orwell'in 1949 yılında yayımlanan distopik romanı *1984*'ü anımsatmaktadır. Southampton Üniversitesinden Doç. Dr. Kieron O'Hara, Orwell'ın *1984* distopyası ile 2018 yılını karşılaştırırken iki dönemde de insanların her daim "izlenmeye açık" olduğunu, ancak *1984* distopyasında bile insanların her an izlenmeyip günümüzde ise kesintisiz bir gözetim altında bulunduğuna dikkat çekmektedir. Bir diğer fark, *1984* distopyasında gözetimin insanlar, günümüzde ise makineler tarafından yapılması; dolayısıyla gözetimin çok daha sürdürülebilir kılınmış olmasıdır. Orwell'ın distopyasından son fark da distopyada insanların ne zaman izlendiğini bilmemesi, modern insanların ise bunu "her an" olarak bilmesidir[61]. Bu karşılaştırmaya göre, kesintisiz izlenmenin eklenmesiyle, bugün modern insanın Büyük Birader'in distopyasındakinden de etkin bir gözetim ağının içinde olduğunu söylemek mümkün görünmektedir.

"Bu kadarı gerçek hayatta olamaz" dedirten pek çok şeyin 21'inci yüzyılda yaşanıyor olması dünya nüfusunun pek azını endişelendirmektedir. Gözetim ağının sınırları görülemezken, önce Panopticon'u, sonra da *1984* distopyasını aşan gözetim ağının tam ortasında duran insan, bu ağı normalleştirip kabul mü edecek; yoksa kişisel verilerinin korunması için harekete mi geçecek? Jeremy Bentham'ın Panopticon tasarımından hareketle hayata geçirilen Millbank Hapishanesi'nde kesintisiz bir gözetim disiplini altında tutulan mahkûmların bir süre sonra psikolojik problemler yaşamaya başladığını[62] düşünürsek, kamu sağlığını gözetmek için haklı gerekçelerle kullanılan gözetim ağının bir süre sonra normalleşip içselleştirilerek topluma zarar vermeye başlaması, yüksek bir ihtimal olarak görülmektedir. Büyük Birader'in salgın esnasında "sizin için" izliyor olması, yine de "izliyor" ve hatta "paylaşıyor" olduğu gerçeğini değiştirmemektedir.

## KAYNAKÇA


[1] *United Nations Human Rights Office of The High Commissioner*, (1966), "International Covenant on Civil and Political Rights", https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. (Erişim Tarihi: 16 Nisan 2020)

[2] *Idle Words*, (2020), "We Need A Massive Surveillance Program", (23 Mart 2020), https://idlewords.com/2020/03/we_need_a_massive_surveillance_program.htm. (Erişim Tarihi: 16 Nisan 2020)

[3] Semple, Janet; "Bentham's Prison: A Study of the Panopticon Penitentiary", *Questia*, https://www.questia.com/library/3859782/bentham-s-prison-a-study-of-the-panopticon-penitentiary. (Erişim Tarihi: 16 Nisan 2020)

[4] Sheridan, Connor; (2016), "Foucault, Power and the Modern Panopticon", *Trinity College*, https://digitalrepository.trincoll.edu/cgi/viewcontent.cgi?article=1564&context=theses. (Erişim Tarihi: 16 Nisan 2020)

[5] Pollard, Christopher; (2019), "Explainer: the ideas of Foucault", *The Conversation*, (26 Ağustos 2019), http://theconversation.com/explainer-the-ideas-of-foucault-99758. (Erişim Tarihi: 16 Nisan 2020)

[6] Galič, Maša; Timan, Tjerk; Koops, Bert-Jaap; (2016), "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation", *Springer*, (13 Mayıs 2016), https://link.springer.com/article/10.1007/s13347-016-0219-1. (Erişim Tarihi: 16 Nisan 2020)

[7] *BBC*, (2020), "Güney Kore koronavirüs vakalarını izleyebilmek için yurt dışından gelenlerin telefonlarına bir uygulama yüklemesini zorunlu kıldı", (16 Mart 2020), https://bbc.in/3amlnTY. (Erişim Tarihi: 16 Nisan 2020)

[8] Hasell, Joe; (2020), "To understand the global pandemic, we need global testing – the Our World in Data COVID-19 Testing dataset", *Our World in Data*, (31 Mart 2020), https://ourworldindata.org/covid-testing#south-korea. (Erişim Tarihi: 16 Nisan 2020)

[9] Kim, Nemo; (2020), "Covid-19: South Koreans keep calm and carry on testing", *The Guardian*, (18 Mart 2020), https://www.theguardian.com/world/2020/mar/18/covid-19-south-koreans-keep-calm-and-carry-on-testing. (Erişim Tarihi: 16 Nisan 2020)

[10] Won Sonn, Jung; (2020), "Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance", *The Conservation*, (19 Mart 2020), https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068. (Erişim Tarihi: 16 Nisan 2020)

[11] So, Won; (2019), "Number of installed closed-circuit television (CCTV) cameras in public places in South Korea from 2013 to 2018", *statista*, (20 Kasım 2019), https://www.statista.com/statistics/651509/south-korea-cctv-cameras/. (Erişim Tarihi: 16 Nisan 2020)

[12] BBC, (2017), "China: 'the world's biggest camera surveillance network'", *Youtube*, (25 Aralık 2017), https://www.youtube.com/watch?v=pNf4-d6fDoY. (Erişim Tarihi: 16 Nisan 2020)

[13] *BBC*, (2020), "China launches coronavirus 'close contact detector' app", (11 Şubat 2020), https://www.bbc.com/news/technology-51439401. (Erişim Tarihi: 16 Nisan 2020)

[14] Hamilton, Isobel Asher; (2020), "Chinese tech giant Baidu has made a maps app that shows the location of coronavirus patients", *Business Insider*, (5 Şubat 2020), https://www.businessinsider.com/baidu-map-app-coronavirus-cases-location-2020-2. (Erişim Tarihi: 16 Nisan 2020)

[15] *China Whisper*, "Top 10 Most Popular Apps in China", https://www.chinawhisper.com/top-10-most-popular-apps-in-china/. (Erişim Tarihi: 16 Nisan 2020)

[16] Ankel, Sophia; (2020), "As China lifts its coronavirus lockdowns, authorities are using a color-coded health system to dictate where citizens can go. Here's how it works.", *Business Insider*, (1 Nisan 2020), https://www.businessinsider.com/coronavirus-china-health-software-color-coded-how-it-works-2020-4. (Erişim Tarihi: 16 Nisan 2020)

[17] Mozur, Paul; Zhong, Raymond; Krolik, Aaron; (2020), "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", *New York Times*, (1 Mart 2020), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. (Erişim Tarihi: 16 Nisan 2020)

[18] *South China Morning Post*, (2020), "Chinese police now have AI helmets for temperature screening", 28 Şubat 2020), https://www.scmp.com/tech/article/3052879/chinese-police-now-have-ai-helmets-temperature-screening. (Erişim Tarihi: 16 Nisan 2020)

[19] Borak, Masha; (2020), "DJI improves temperature-measuring drones with a simple cotton swab", *Abacus*, (20 Şubat 2020), https://www.abacusnews.com/tech/dji-improves-temperature-measuring-drones-simple-cotton-swab/article/3051513?_ga=2.3731320.934848059.1586441571-707932704.1581026156. (Erişim Tarihi: 16 Nisan 2020)

[20] Adlina AR; (2020), "AR smart glasses can help mitigate COVID-19 resurgence in China", *Techwire Asia*, (1 Nisan 2020), https://techwireasia.com/2020/04/can-ar-smart-glasses-help-china-identify-virus-carriers/. (Erişim Tarihi: 16 Nisan 2020)

[21] Kuo, Lily; (2020), "'The new normal': China's excessive coronavirus public monitoring could be here to stay", The Guardian, (9 Mart 2020), https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay. (Erişim Tarihi: 16 Nisan 2020)

[22] Deutche Welle, (2020), "İsrail Corona virüs nedeniyle vatandaşlarını cep telefonlarıyla takip edecek", *Youtube*, (24 Mart 2020), https://www.youtube.com/watch?v=RHFo-8Cu0_q0&feature=youtu.be. (Erişim Tarihi: 16 Nisan 2020)

[23] Franceschi-Bicchierai, Lorenzo; (2020), "We Saw NSO's Covid-19 Software in Action, and Privacy Experts Are Worried", *Vice*, (2 Nisan 2020), https://www.vice.com/en_us/article/epg9jm/nso-covid-19-surveillance-tech-software-tracking-infected-privacy-experts-worried. (Erişim Tarihi: 16 Nisan 2020)

[24] Bennett, Naftali; (2020), *Twitter*, (30 Mart 2020), https://twitter.com/naftalibennett/status/1244534719540277248. (Erişim Tarihi: 16 Nisan 2020)

[25] Bennett, Naftali; (2020), *Twitter*, (30 Mart 2020), https://twitter.com/naftalibennett/status/1244534722035924992. (Erişim Tarihi: 16 Nisan 2020)

[26] Dixit, Pranav; (2020), "This Indian State Wants People In Coronavirus Quarantine To Send Them Selfies Every Hour", *BuzzFeed News*, (30 Mart 2020), https://www.buzzfeednews.com/article/pranavdixit/karnataka-coronavirus-quarantine-selfies. (Erişim Tarihi: 16 Nisan 2020)

[27] *Hürriyet*, (2020), "Aplikasyon nedir? Corona virüs aplikasyon uygulaması ne demek, ve nasıl indirilir?", (7 Nisan 2020), https://www.hurriyet.com.tr/gundem/aplikasyon-nedir-corona-virus-aplikasyon-uygulamasi-ne-demek-ve-nasil-indirilir-41489087. (Erişim Tarihi: 16 Nisan 2020)

[28] *Digital Age*, (2020), "Coronavirus takip uygulaması devreye giriyor: 'Hayat Eve Sığar'", (7 Nisan 2020), https://digitalage.com.tr/coronavirus-takip-uygulamasi-devreye-giriyor-hayat-eve-sigar/. (Erişim Tarihi: 16 Nisan 2020)

[29] Romm, Tony; Dwoskin, Elizabeth; Timberg, Craig; (2020), "U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus", *The Washington Post*, (18 Mart 2020), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/. (Erişim Tarihi: 16 Nisan 2020)

[30] Farr, Christina; (2020), "Facebook is developing new tools for researchers to track if social distancing is working", *CNBC*, (6 Nisan 2020), https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html. (Erişim Tarihi: 16 Nisan 2020)

[31] Detrow, Scott; (2018), "What Did Cambridge Analytica Do During The 2016 Election?", *npr*, (20 Mart 2018), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election. (Erişim Tarihi: 16 Nisan 2020)

[32] *BBC*, (2020), "Clearview AI: Face-collecting company database hacked", (27 Şubat 2020), https://www.bbc.com/news/technology-51658111. (Erişim Tarihi: 16 Nisan 2020)

[33] Grind, Kirsten; McMillan, Robert; Mathews, Anna Wilde; (2020), "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits", *The Wall Street Journal*, (17 Mart 2020), https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841. (Erişim Tarihi: 16 Nisan 2020)

[34] Cox, Joseph; (2020), "Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US", *Vice*, (17 Mart 2020), https://www.vice.com/en_us/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras. (Erişim Tarihi: 16 Nisan 2020)

[35] C. McCarthy, Andrew; (2020), "FISA Update", *National Review*, (18 Mart 2020), https://www.nationalreview.com/corner/fisa-update/. (Erişim Tarihi: 16 Nisan 2020)

[36] *Wired*, (2020), "How Surveillance Could Save Lives Amid a Public Health Crisis", (21 Mart 2020), https://www.wired.com/story/surveillance-save-lives-amid-public-health-crisis/. (Erişim Tarihi: 16 Nisan 2020)

[37] Thompson, Stuart A.; Warzel, Charlie; (2019), "Twelve Million Phones, One Dataset, Zero Privacy", *The New York Times*, (19 Aralık 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. (Erişim Tarihi: 16 Nisan 2020)

[38] Rosenberg, Matthew; Confessore, Nicholas; Cadwalladr, Carole; (2018), "How Trump Consultants Exploited the Facebook Data of Millions", *The New York Times*, (17 Mart 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html9. (Erişim Tarihi: 16 Nisan 2020)

[39] Tait, Robert; (2016), "Personal details of 50 million Turkish citizens leaked online", *The Telegraph*, (4 Nisan 2016), https://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha/. (Erişim Tarihi: 16 Nisan 2020)

[40] Santora, Marc; (2019), "5 Million Bulgarians Have Their Personal Data Stolen in Hack", *The New York Times*, (17 Temmuz 2019), https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html. (Erişim Tarihi: 16 Nisan 2020)

[41] *BBC*, (2019), "Data on almost every Ecuadorean citizen leaked", (16 Eylül 2019), https://www.bbc.com/news/technology-49715478. (Erişim Tarihi: 16 Nisan 2020)

[42] Victor, Daniel; Frenkel, Sheera; Kershner, Isabel; (2020), "Personal Data of All 6.5 Million Israeli Voters Is Exposed", *The New York Times*, (10 Şubat 2020), https://www.nytimes.com/2020/02/10/world/middleeast/israeli-voters-leak.html. (Erişim Tarihi: 16 Nisan 2020)

[43] *Norton LifeLock*, "What Is Data Privacy and Why Is it Important?", https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html. (Erişim Tarihi: 16 Nisan 2020)

[44] Doffman, Zak; (2019), "Google Play Warning: Even Harmless Flashlight Apps Used By Millions Secretly Access Our Data", *Forbes*, (15 Eylül 2019), https://www.forbes.com/sites/zakdoffman/2019/09/15/google-warning-as-harmless-apps-installed-by-millions-secretly-access-user-data-report/#6375315147e4. (Erişim Tarihi: 16 Nisan 2020)

[45] Cimpanu. Catalin; (2019), "Most Android flashlight apps request an absurd number of permissions", *ZDNet*, (11 Eylül 2019), https://www.zdnet.com/article/most-android-flashlight-apps-request-an-absurd-number-of-permissions/. (Erişim Tarihi: 16 Nisan 2020)

[46] Seal, Thomas; (2020), "U.K. Asks Phone Carriers for Data to Help Fly Brits Abroad Home", *Bloomberg*, (1 Nisan 2020), https://www.bloomberg.com/news/articles/2020-04-01/u-k-asks-phone-carriers-for-data-to-help-fly-brits-abroad-home. (Erişim Tarihi: 16 Nisan 2020)

[47] Chandler, Simon; (2020), "U.K. Government Is Using Coronavirus As Excuse To Ramp Up Surveillance", *Forbes*, (2 Nisan 2020), https://www.forbes.com/sites/simonchandler/2020/04/02/uk-government-is-using-coronavirus-as-excuse-to-ramp-up-surveillance/#164519f62080. (Erişim Tarihi: 16 Nisan 2020)

[48] Valentino-DeVries, Jennifer; (2020), "Translating a Surveillance Tool into a Virus Tracker for Democracies", *The New York Times*, (19 Mart 2020), https://www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html. (Erişim Tarihi: 16 Nisan 2020)

[49] Lomas, Natasha; (2020), "Call for common EU approach to apps and data to fight COVID-19 and protect citizens' rights", *Tech Crunch*, (8 Nisan 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626. (Erişim Tarihi: 16 Nisan 2020)

[50] Troncoso, Carmela; (2020), "Decentralized Privacy-Preserving Proximity Tracing", *GitHub*, (12 Nisan 2020), https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. (Erişim Tarihi: 16 Nisan 2020)

[51] Dillet, Romain; (2020), "France is officially working on 'Stop Covid' contact-tracing app", *Tech Crunch*, (8 Nisan 2020), https://techcrunch.com/2020/04/08/france-is-officially-working-on-stop-covid-contact-tracing-app/. (Erişim Tarihi: 16 Nisan 2020)

[52] Busvine, Douglas; (2020), "Germany launches smartwatch app to monitor coronavirus spread", *Reuters*, (7 Nisan 2020), https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-launches-smartwatch-app-to-monitor-coronavirus-spread-idUSKBN21P1SS. (Erişim Tarihi: 16 Nisan 2020)

[53] *Kronen Zeitung*, (2020), "Mobilfunker lieferte Regierung Bewegungsprofile", (17 Mart 2020), https://www.krone.at/2118142. (Erişim Tarihi: 16 Nisan 2020)

[54] *Rapid Tech*, "Minimizing the spread Coronavirus infections with Fever Detection", https://rapid-tech.com.au/flir-thermal-imaging-camera-for-scanning-elevated-body-temperature/

[55] Gray, Rosie; Haskins, Caroline; (2020), "The Coronavirus Pandemic Has Set Off A Massive Expansion Of Government Surveillance. Civil Libertarians Aren't Sure What To Do.", *BuzzFeed News*, (30 Mart 2020), https://www.buzzfeednews.com/article/rosiegray/they-were-opposed-to-government-surveillance-then-the. (Erişim Tarihi: 16 Nisan 2020)

[56] Huang, Kristin; (2020), "US accuses Beijing of using coronavirus as cover for South China Sea activity", *South China Morning Post*, (7 Nisan 2020), https://www.scmp.com/news/china/diplomacy/article/3078757/us-accuses-beijing-using-coronavirus-cover-south-china-sea. (Erişim Tarihi: 16 Nisan 2020)

[57] Werner, Debra; (2020), "Pandemic fuels demand for satellite imagery", *Space News*, (23 Mart 2020), https://spacenews.com/earth-imagery-demand-pandemic/. (Erişim Tarihi: 16 Nisan 2020)

[58] *The Asian Age*, (2020), "Privacy could become the next victim of the coronavirus as governments step up mass surveillance", (29 Mart 2020), https://www.asianage.com/technology/in-other-news/290320/privacy-could-become-the-next-victim-of-the-coronavirus-as-governments-step-up-mass-surveillance.html. (Erişim Tarihi: 16 Nisan 2020)

[59] *Statista*, (2020), "Cumulative number of Coronavirus (COVID-19) deaths in Italy since February 24, 2020", (16 Nisan 2020), https://www.statista.com/statistics/1104964/coronavirus-deaths-since-february-italy/. (Erişim Tarihi: 16 Nisan 2020)

[60] Tazzioli, Martina; (2020), "COVID's borders: between peer-to-peer surveillance and the "common good"", *Open Democracy*, (7 Nisan 2020), https://www.opendemocracy.net/en/can-europe-make-it/covids-borders-between-peer-to-peer-surveillance-and-the-common-good/. (Erişim Tarihi: 16 Nisan 2020)

[61] Science & Engineering South, (2018), "Dr. Kieron O'Hara - Ethics of Surveillance, Power and Citizenship", *Youtube*, (17 Temmuz 2018), https://www.youtube.com/watch?v=Ktpq8Hzc3QY. (Erişim Tarihi: 16 Nisan 2020)

[62] Cox, Catherine; Marland, Hilary; (2018), "'We Are Recreating Bedlam': A History of Mental Illness and Prison Systems in England and Ireland", *NCBI*, (20 Kasım 2018), https://www.ncbi.nlm.nih.gov/books/NBK539382/. (Erişim Tarihi: 16 Nisan 2020)

thinktech

STM Teknolojik Düşünce Merkezi

http://thinktech.stm.com.tr