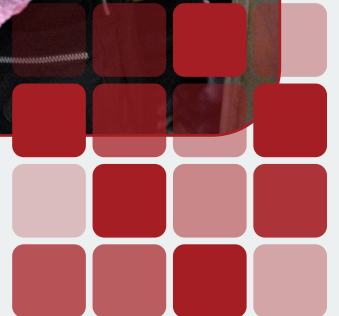


# COVID-19 İLE DİJİTAL MÜCADELE VE ULUSLARARASI REKABET



GÖKTUĞ SÖNMEZ & EMİNE ÇELİK





## Telif Hakkı

### Ankara - TÜRKİYE ORSAM © 2020

Bu alıřmaya ait ierięin telif hakları ORSAM'a ait olup, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu uyarınca kaynak gsterilerek kısmen yapılacak makul alıntılar dıřında, hibir Őekilde nceden izin alınmaksızın kullanılamaz, yeniden yayımlanamaz. Bu alıřmada yer alan deęerlendirmeler yazarına aittir; ORSAM'ın kurumsal grüşünü yansıtmamaktadır.

ISBN : 978-605-06852-8-2

### Ortadoęu Arařtırmaları Merkezi

Adresi : Mustafa Kemal Mah. 2128 Sk. No: 3 ankaya, ANKARA

Telefon: +90 (312) 430 26 09 Faks: +90 (312) 430 39 48

Email: info@orsam.org.tr

Fotoęraflar: Shutterstock

# COVID-19 İLE DİJİTAL MÜCADELE VE ULUSLARARASI REKABET

## Yazarlar Hakkında

### Dr. Gökтуğ Sönmez

Lisans derecesini Bilkent Üniversitesi Uluslararası İlişkiler Bölümü'nden, yüksek lisans derecesini London School of Economics (LSE) Uluslararası İlişkiler Bölümü'nden ve doktora derecesini School of Oriental and African Studies (SOAS)'den almıştır. Akademik araştırma alanları arasında radikalleşme, şiddete varan aşırıcılık, uluslararası ilişkiler teorisi ve Türk dış politikası bulunmaktadır. Bu alanlarda Türkiye Cumhuriyeti Dışişleri Bakanlığı SAM, Global Strateji Enstitüsü ve ORSAM gibi çeşitli düşünce kuruluşlarında arařtırmalarda bulunmuştur. Halihazırda ORSAM'da Güvenlik Çalışmaları Direktörü olarak çalışmaktadır.

### Emine Çelik

Lisans derecesini Anadolu Üniversitesi'nden aldıktan sonra yüksek lisansını Necmettin Erbakan Üniversitesi Siyaset Bilimi ve Kamu Yönetimi'nde tamamlamış ve aynı üniversitede doktorasına devam etmektedir. Akademik araştırma alanları arasında terörizm, siber terörizm, radikalleşme ve yoksulluk bulunmaktadır.

## İçindekiler

Giriş .....	3
Dijital M¼cadelede Farklı Yöntem ve Araçlar: Dünya Örnekleri .....	4
Kişisel Veriler ve Mahremiyet Tartışmaları .....	8
COVID-19 Bağlamında Tıbbi Ekipman ve Teknoloji Yarışı .....	10
Sonuç .....	14
Kaynakça .....	17
Sonnot .....	19

## Giriş

COVID-19 salgını sağlık boyutunun ötesinde yalnızca uluslararası güvenlik gündemi ve uluslararası sistemin geleceği, hegemon ve olası meydan okuyucular arasındaki ilişkiler ve siber güvenlik konusunda önemli değişimlere müsait bir ortam oluşturmamaktadır. Salgın, aynı zamanda ulusal ve/ya bölgesel kimi güvenlik aygıtlarının yeni araçları kullanımı ve/ya eski araçları mevcut duruma uyarlaması, operasyonel anlamda mevcut kapasitelerini salgınla ilgili hareketlere kaydırmaları gibi sonuçlar da doğurmuştur. Güvenliğin ilgi alanının son yüzyılda ilk kez bu düzeyde ciddiyetle ve küresel manada insan sağlığını kapsar şekilde genişlemesi nedeniyle ortaya çıkan durumun yansımaları olacaktır. Salgının güvenliğin kadim konuları üzerinde yapabileceği doğrudan ve dolaylı etkiler neticesinde muhtemeldir ki, toplumsal sağlık ve biyolojik tehditler bu süreçteki konumunu aynı oranda korumasa dahi COVID-19 sonrası dönemde eskisinden çok daha önemli ve öncelikli bir mesele olarak yalnız sağlık alanındaki ulusal, bölgesel ve küresel aktörlerin değil, tüm ulusal ve uluslararası örgütlerin gündeminde olacaktır. İşte bu nedenledir ki COVID-19, geldiği nokta itibarıyla devlet aygıtının yalnız

sağlıkla ilgili değil, güvenlikle doğrudan ilgili aktörlerinin de gündemini teşkil etmektedir.

COVID-19 salgınının pandemi olarak ilan edilmesi ve enfekte sayıları ile ölüm vak'alarının hızla artmasıyla birlikte dünyada farklı kapsamlarda olmak üzere sokağa çıkma kısıtlamaları getirilmiştir. İletişimin ve iş devamlılığının siber dünyaya kaymasıyla oluşan siber tehdit, sokaktaki hareketliliğin azalmasıyla oluşabilecek fiziki tehditler ve bunlara karşı tedbirlerle dair kısa bir değerlendirmeyi daha önce yapmıştık. Bununla birlikte daha özeldir mevcut meydan okumalara karşı ülkelerin ellerindeki kimi imkânları nasıl dönüştürmeye ve mevcut araçları nasıl çeşitlendirmeye başladıkları bu yazının ana tartışması olacaktır.

Her ne kadar önde gelen ülkelerin salgın hastalığa karşı tasarlanmış önlemleri ve genel bir eylem planı olsa dahi gerek bu planların uygulanabilirlikteki zorluğu, gerek zamanlamayla ilgili sıkıntılar gerekse de COVID-19 salgınının böylesi bir planlamada öngörülenden daha hızlı yayılması gibi sebeplerle mücadele pek çok ülkede tasarlanandan daha zor bir hal almıştır. Temelde salgının ülkelerin sağlık kapasitelerini aşma ihtimalinden kaynaklanan, hastalığın ken-



disinden daha büyük ve esas itibariyle de hastalığı bugünkü ölçekte bir tehdit haline getiren bu endişeler yalnızca sağlık sektörünün gündemi olmaktan hızla çıkmıştır. Sağlık odaklı ve hastalığın yayılması engellenemediği takdirde oluşabilecek güvenlik risklerinin muhtemel artışına yönelik endişeler, COVID-19 salgınına hızla güvenlik alanı ve güvenlik aygıtlarının konusu haline getirmiştir.

Salgının ilk olarak ortaya çıktığı Çin’de Alipay ve WeChat platformlarında çalışan Health Code sistemi sayesinde her bireye kullanması için bir sağlık kodu atanmıştır.

### Dijital Mücadelede Farklı Yöntem ve Araçlar: Dünya Örnekleri

COVID-19 salgını sonrası ülkelerin salgını kontrol altına alabilmek adına kısmi karantina uygulamaları, sokağa çıkma yasakları, sosyal mesafenin korunması gibi çeşitli yöntemler uyguladıkları bilinmektedir. Bu uygulamalarla salgının yayılım hızının yavaşlatılması hedeflenmektedir.

Ancak, yalnız salgına yakalanan kişilerin değil, aynı zamanda bu kişilerin salgın öncesi ve sonrası iletişim kurduğu kişilerin, kullandıkları ulaşım araçlarının tespiti, hareketlerinin hastalığa yakalandığı teşhis edildikten sonra kısıtlanması, buralarda iletişim kurdukları kişilerin teşhis ve tedavi süreçlerinin başlatılması, hastaneye yatırıldıysa sonraki sürecin takibi gibi

konular salgınla bağlantılı endişelerin başında gelmiştir.

Bu bağlamda da ülkeler web sitelerini kullanarak ve/ya çeşitli telefon uygulamaları geliştirerek salgınla mücadele alanlarını siber alana taşımışlardır. Kullanılan telefon uygulamaları ise çeşitli güvenlik sorunlarını beraberinde getirmiştir. Bu endişelerin temelinde hastaların takibi ve diğer kişilerin hastalığa yakalanmasının engellenmesi kapsamında öne çıkan unsurlardan biri farklı veritabanlarından elde edilen verilerin harmanlamasıyla bütüncül takip ve bu takipte olası hata payını en aza indirme amacıyla kullanılan yüz tanıma sistemlerinin entegrasyonu olmuştur. Her ülke bu araçların hepsine erişim ve/ya kullanımı noktasında yeterli yetkinlikte olmadığından ve/ya ülkenin demokratik dinamikleri bu konuda önemli meydan okumalar doğurduğundan farklı pek çok uygulama görmek mümkündür. Öncül hamlelere bakıldığında özellikle Çin ve İsrail bu konuda bilinen etkin örnekleri ülke nüfusuna oranla en yüksek oranda hayata geçiren iki ülke olarak ön plana çıkmaktadır. Bunun yanında Güney Kore, Kanada ve İngiltere’de de benzer uygulamalar hayata geçirilmiştir veya geçirilmesi için veri toplama safhasında bulunmaktadır. Singapur, Japonya ve Almanya’da da süreç farklı dinamiklerle ve farklı safhalarda olmak üzere işlemektedir.

Salgının ilk olarak ortaya çıktığı Çin’de Alipay ve WeChat platformlarında çalışan Health Code sistemi sayesinde her bireye kullanması için bir sağlık kodu atanmıştır.<sup>1</sup> Uygulamaya girişte kişiler kimlik numaraları, yaşadıkları yerler, virüsü taşıyan kişilerle birlikte olup olmadıklarına ve semptomları taşıyıp taşımadıklarına dair bilgileri girmektedirler.<sup>2</sup> Uygulama içerisine kaydedilen bilgilerin akabinde ise kişilere Yeşil (COVID-19 Negatif), Sarı (COVID-19 Muhtemel Taşıyıcı) ve Kırmızı (COVID-19 Pozitif) renkleri atanmaktadır. Yeşil koda sahip kişilerin hareket serbestliği, Sarı koda sahip kişilerin 7 gün karantina ve Kırmızı

İsrail Sağlık Bakanlığı tarafından COVID-19 salgınının yayılmasını önlemek adına HaMagen (Kalkan) isimli bir telefon uygulaması hayata geçirilmiştir. HaMagen Google Play’de ve App Store’da indirilebilir biçimde İsrail İç İstihbarat Servisi olan Shin Bet tarafından tasarlanmıştır.

koda sahip kişilerin ise 14 gün karantina zorunlulukları vardır.<sup>3</sup> Çin’de Alipay Health Code olarak atıf yapılan sistem, ülke genelinde 200 şehirde aktif duruma gelmiş bulunmakta ve kişilerin yerleri, hareketleri gibi bilgileri şehrin emniyet birimlerine iletmektedir. İlâveten özellikle toplu taşıma araçlarında kişilerin kimlik bilgileri

ve güzergahları kaydedilerek bu veriler de aynı havuza aktarılmaktadır. Yüz tanıma sistemleri ve uzaktan vücut ısı ölçme sistemlerinin de bu araçlara ilave edilmesiyle Çin’in uzun süredir önemli gelişmeler kaydettiği yüz tanıma ve kişi takibi sistemini bütüncül ve şu ana kadarki en eksiksiz haline taşıdığı görülmektedir. 900 milyon ile 1.5 milyar arası kullanıcısı bulunan Alipay ve WeChat gibi Çin merkezli dijital platformlar da bu çabanın entegre parçaları olmaları yoluyla COVID-19 mücadelesinde ulusal sınır ve firmalar kadar özel sektör ile devlet işbirliğinin önemini de altını çizmektedir.<sup>4</sup> Öte yandan Çinli vatandaşlara yönelik bu dijital gözetleme insan hakları ihlallerinin olduğuna dair savı güçlendirmektedir. Bu süreç bireylere dair “kesintisiz istihbarat ve gözetleme”yi hayata geçirme noktasında yüz tanıma teknolojisini diğer verilerle birlikte etkin biçimde kullanma noktasında önemli yatırımlar yapan Çin açısından önemli bir fırsat sunmakta, rejimin yapısı sayesinde kişisel özgürlüklere dair yaygın endişeleri de aşarak bu çabaları en eksiksiz haline yaklaştırmaktadır.

Çin’deki uygulamaların değişik versiyonları salgınla mücadele eden birçok ülkede kulla-





nılmaya başlanmıştır. İsrail Sağlık Bakanlığı tarafından COVID-19 salgınının yayılmasını önlemek adına HaMagen (Kalkan) isimli bir telefon uygulaması hayata geçirilmiştir. HaMagen Google Play’de ve App Store’da indirilebilir biçimde İsrail İç İstihbarat Servisi olan Shin Bet tarafından tasarlanmıştır. Bu bağlamda da Shin Bet’in faaliyet alanı ve yetkileri Netanyahu tarafından COVID-19 salgınıyla mücadele bağlamında genişletilmiştir.<sup>5</sup> Uygulama bir kullanıcının önceki 14 gün içerisinde Korona virüs teşhisi konan kişilere yakın olup olmadığını ya da temasta bulunup bulunmadığını anında bilme yeteneğini kazandırmayı amaçlamaktadır. İsraili yetkililer uygulama ile salgını kontrol altına almayı hedeflediklerini söylemekte, kullanıcıların hareketlerinin ve kişisel verilerinin ise yalnızca akıllı telefonda kayıtlı kaldığını iddia etmektedirler. Sağlık Bakanlığı tarafından verilerin sürekli güncellendiği ve tek taraflı olarak akıllı telefonlara gönderildiği, sistemin açık kaynaklı bir kod yapısına sahip olduğu için de güvenilir olduğu ifade edilmektedir.<sup>6</sup> Sistem, bu çerçevede Hamas ve Hizbullah saldırıları için de kullanılan platformu salgın sürecin-

de hastalığa odaklı olarak genişletmektedir ve veri tabanını verilerin bir süreliğine saklanacağı söylemiyle bu alanda da kullanmaya başlamış durumdadır. Netanyahu, verilerin korunması ve kişisel özgürlüklerle ilgili eleştirileri, böyle bir durumda söz konusu araçların kullanılmasının gecikmesinin İsraililerin hayatlarına mal olabileceğini söyleyerek reddetmiştir. Neticesinde 1.5 milyon İsrail vatandaşı HaMagen programına kaydolmuştur ve böylelikle hastalığa sahip kişiler yakın yerlerden geçtiklerinde diğerleri program tarafından uyarılmaktadırlar. Bununla birlikte İsrail Yüksek Mahkemesi, Nisan sonu itibarıyla sistemin kullanımının mahremiyeti ihlal dolayısıyla telefon konum verilerinin takibinin yasaklanması ve alternatif uygulamalar geliştirilmesi kararı almıştır.

Avrupa merkezli olarak ortaya konulan telefon uygulaması projesinde ise insanların COVID-19 salgınından kaçınmaları için yeni bir telefon uygulaması tasarlanmıştır. Proje kapsamında geliştiriciler, Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) isimli uygulamanın zorunlu olmadığını, kullanacak olan

kişilerin kendi istekleri doğrultusunda telefonlarına indirilebileceklerini, uygulamada uçtan uca şifreleme algoritmalarının kullanılacağını ve bu bağlamda da kişisel bilgilerin tamamen gizli kalacağını ifade etmektedirler. Projenin kurucu ekibinde yer alan ve aynı zamanda da Angela Merkel yönetimine dijital politika konularında danışmanlık yapan Berlin merkezli yapay zeka şirketi Arago'nun CEO'su Chris Boos, hayata geçirilen projenin kişisel güvenliği ihlal etmeyeceğini ve Avrupa'nın çok uzun zamandır gizlilik geleneğine sahip olduğunu vurgulamaktadır.<sup>7</sup>

Proje, COVID-19 salgınının yayılmasını kontrol altına almak için enfekte olan kişilerin izlenmesi gerekliliğinden söz etmiş ve projenin amacının doğru önlemlerin alınabilmesi için enfekte olan kişilerin koordinatlarının işlenerek diğer kişilerin izolasyonunun sağlanması olduğu belirtilmiştir. Kar amacı gütmeyen PEPP-PT uygulamasının insanların virüse maruz kalma risklerine dair bilgilendirilmesi için geliştirildiği vurgulamaktadırlar. Uygulamanın temel çalışma prensibi, Bluetooth sinyalleri ile kişiler arasındaki mesafeyi ölçme ve enfekte olan kişilerin koordinatlarının uygulamayı kullanan diğer kişilere iletme üzerine kurgulanmıştır. Bu bağlamda da enfekte olan kişilerin hareketleri takip edilerek salgının yayılma hızının yavaşlatılması hedeflenmektedir.<sup>8</sup>

ABD'de özellikle ülke dışı askeri varlığın hastalıklara karşı savunma araçlarından olması maksatlı kurulan NCMI (The National Center for Medical Intelligence/Ulusal Tıbbi İstihbarat Servisi), kurulduğu tarihten bu yana en kritik süreçlerden birini yaşamaktadır. NCMI, tıp alanından yetkin isimlere ilaveten uydu görüntülerinden insan istihbaratına ve iletişimin dinlenmesine kadar pek çok yöneme dair kapasitesini hızla artırmış durumdadır.<sup>9</sup> Özellikle küresel askeri projeksiyon kabiliyeti ve farklı coğrafyalarda askeri üslere sahip ülkeler için bu askeri noktalarda oluşacak salgın ve buna dair bilginin

yayılması bu aktörlerin küresel erişimine ve gücüne önemli bir negatif etki yapma potansiyeli taşımaktadır. ABD bağlamında ülkenin özellikle Afganistan, Irak, Suriye gibi ülkelerden askerini çekmesine dair tartışmaların yaşandığı bir dönemde bu gelişme ayrıca önem arz etmektedir.

Toronto'da başlatılan uygulamada telefon şirketlerinden kişi ve konum bilgileri toplanmakta, kişilerin toplandığı yerlerin ve hastalığın olası yayılma alanlarının tespiti amaçlanmaktadır. Toronto yönetiminden varlığına dair ilk etapta tutarsız açıklamaların geldiği konu Toronto valisinin doğrulaması neticesinde kesinleşmiş, Ottawa'da da benzer bir uygulamanın başlayabileceğine dair sağlık yetkililerinden açıklamalar gelmiştir. Verilerin her ne kadar anonim olduğu ve insanların bir araya gelmesi yönünde baskı kurmayı amaçladığı iddia edilse dahi yalnız bu işlevin ne kadar gerçekçi ve ötesinde amaca ne denli hizmet ettiği ve dolayısıyla bununla sınırlı kalıp kalmadığı soru işaretidir.

İngiltere'de Oxford Üniversitesi ile NHS'in ortak olarak geliştirdiği projede ise Çin'deki uygulamanın verilerin rıza ile toplandığı ve silindiği, "demokrasiye daha uygun" bir versiyonu üzerinde çalışılmakta, telefon uygulaması olarak kısa süre sonra hayata geçirilmesi beklenmekte<sup>10</sup> olduğu yönünde açıklama yapılmıştır. Bu haliyle uygulama Güney Kore'deki benzer takip uygulaması olan ve hastalığa yakalanan kişilerin verilerini kendi rızalarıyla yayınladığı coronavirus100m ve coronamap.site gibi araçlara büyük benzerlik taşıyacaktır. Güney Kore, Çin'e benzer ancak daha şeffaf ve gönüllü paylaşım dayalı biçimde kişilerin mobil verilerini, kredi kartı bilgilerini ve yüz tanıma teknolojisini birleştiren bütüncül bir yol izlemektedir.<sup>11</sup> Benzer şekilde Avusturya'da gönüllü kullanıma dayanan Stopp Corona uygulaması 130 binden fazla kullanıcı tarafından kullanılır durumdadır.<sup>12</sup> Almanya'da telekomünikasyon enstitüsü

HHI ve halk sađlığı ajansı Robert Koch Enstitüsü gönüllülük temelli bir uygulama üzerinde çalıştıklarını belirtmiştir.<sup>13</sup> Polonya ve Singapur'da salgına yakalanan kişilerin karantinaya uduđunu kontrol odaklı sistemler hayata geçirilmiştir. Rusya'nın mobil veriler ve telefon tabiline ilaveten Çin'e benzer biçimde yüz tanıma sistemlerini de bu verilere entegre biçimde kullanmaya başladığı belirtilmektedir.<sup>14</sup> Japonya'da yağmur ve deprem olayları için 2018'de Agree firması tarafından geliştirilen uygulama COVID-19 bağlamında bedava erişime sunularak kişilerden gönüllülük esasıyla kendi durumları ve seyahatlerine dair veri toplamaktadır.<sup>15</sup>

COVID-19 ile dijital mücadele kapsamında Türkiye'de ise Sağlık Bakanlığı koronaelem.com sitesini yayına sokarak gönüllülük esasıyla kişilerin verilerini değerlendirerek hastalığa yakalanmış olma ihtimallerini ifade etmekte, hastalığa yakalanmış olma ihtimali olan kişilerin en kısa sürede sağlık kuruluşlarına erişimini önermektedir. Kişilerin bununla birlikte son 14 gün içerisinde seyahat ettikleri ülkeler, herhangi bir sağlık merkezinde bulunup bulunmadıkları, solunum yolu hastalığı olan kişilerle irtibat kurup kurmadıkları ve kendilerinin kronik rahatsızlığı olup olmadığına dair veriler de talep edilmektedir. Ek olarak, "Hayat Eve Sığar" isimli Android ve App Store platformlarından indirilebilen bir telefon uygulaması geliştirilmiştir. Gönüllük esaslı olarak uygulamaya konulan sistemde Bluetooth sinyalleri kullanılarak kişilere çevrelerindeki pozitif kişileri görmeleri sağlanmakta, ya da yakından geçmiş ancak sonrasında pozitif olmuş kişilerin yer ve mekan bilgileri kendilerine iletilmektedir. Uygulama ile kişiler buldukları bölgedeki enfekte yoğunluđunu görebilmektedir. Aynı zamanda uygulama kişilere her gün sağlık bilgileri sormakta ve aile bölümüne dahil edilen kişilerin herhangi birinin enfekte olması ya da pozitif biriyle temas etmesi halinde kişilere uyarı mesajı göndermektedir. Nisan ayı ortasında ise TÜBİTAK COVID-19'un teşhis ve tedavisi, COVID-19 sürecinde kritik

unsurların üretiminin kolaylaştırılması, eğitim teknolojilerinin geliştirilmesi ve risk gruplarının korunması ve toplu taşıma araçlarının güvenli kullanımı gibi başlıklardaki araştırmaları uluslararası olarak fonlanan EUREKA desteđi kapsamında destekleyeceđi geniş kapsamlı bir araştırma ilanında bulunmuştur. Sürecin TÜBİTAK, üniversiteler, yazılım firmaları ve Sağlık Bakanlığı koordinasyonunda çıktılar vermesi ve süreç içerisinde bahsi geçen diđer ülkelerdeki çabaların da analizinin yapıldığı mücadele araçları geliştirilmesi mümkün gözükmektedir.

## Kişisel Veriler ve Mahremiyet Tartışmaları

İstihbari yapılara ilaveten devletlerin farklı aygıtlarının, kurumlarının ve özel şirketlerin hastalığın yayılımı ve önlenmesine dair takip ve gözetleme içeren bu araçları kullanımı ise bu verilerin mahremiyete etkisi, kişisel ifade özgürlüğü üzerinde kurabileceđi baskı vb. nedenler dolayısıyla hem bu araçların kullanımının ne kadar süreceđi hem verilerin depolanma biçimi hem de bu verilerin ne kadar saklanacağı gibi temel soruları ortaya çıkarmaktadır. Bu bağlamda da siber alandaki dijital gözetim farkındalığını oluşturmak adına İnsan Hakları İzleme Örgütü bir çalışma başlatmış ve ülkelere salgınla mücadele ederken 8 maddelik dijital gözetim şartı sunmuştur:

1. Salgınla mücadele ederken kullanılan dijital gözetleme uygulamaları yasal ve orantılı olmalıdır. Yasal çerçevesi çizilen uygulamaların halk sađlığını korumaya yönelik olduđu yetkililer tarafından meşru bir zemin üzerinde gerekçelendirilmelidir. **COVID-19 salgınının ayırım gözetmeyen kitle gözetimi için bir bahane olarak sunulmasına müsaade edilmemelidir.**

2. Hükümet dijital gözetleme ve izleme güçlerini genişletmek isterse bu yetkiler zamansal sınırlara tabi kılınmalı ve mevcut salgın kontrol altına alındığında son bulmalıdır.



### **COVID-19 salgının süresiz bir dijital gözetime yol açmasına müsaade edilmemelidir.**

3. Devletler ve hükümetler sağlık verileri de dahil olmak üzere depolanan kişisel veriler yalnızca COVID-19 salgınının yayılmasını engellemek ya da durdurmak amaçlı kullanılmalıdır. Depolanan veriler ticari amaçlar da dahil olmak üzere hiçbir şekilde kullanılmamalıdır. **COVID-19 salgının bireyin mahremiyet hakkına saldırı gerçekleştirilmesine müsaade edilmemelidir.**

4. Devletler ve hükümetler kişilerin sağlık bilgileri de dahil olmak üzere topladıkları ve depoladıkları kişisel tüm verilerin güvenliğinden sorumlu olmalı ve verileri korumak için her türlü çabayı göstermelidir. Verilerin anonim olarak kalması sağlanmalı ve nasıl anonimleştirildiği konusunda gerekli bilgiler verilmelidir. **COVID-19 salgını ile toplanan veriler insanların dijital güvenliğine zarar vermemelidir.**

5. Big Data ve yapay zeka sistemleri de dahil olmak üzere kullanılan tüm dijital gözetleme yöntemleri kişilerin ırk, din, dil ay-

rımına yol açabilecek ve yoksulluk içinde yaşayan kişilere karşı kullanılacak hak ihlallerine sebep olacak riskleri elimine etmelidir. **COVID-19 salgının toplumdaki farklı gruplar arasında yaşanan insan hakları ihlallerini derinleştirmesine müsaade edilmemelidir.**

6. Hükümetler ve devletler özel ya da kamu şirketleri ile COVID-19 nedeniyle toplanan verilerin paylaşımına dair anlaşma yaparlarsa, bu anlaşmalar yasal çerçeveye dayandırılmalı ve gerekçeleri şeffaf bir şekilde kamuoyu ile paylaşılmalıdır. COVID-19 ile mücadeleye katılan işletmeler insan haklarına aykırı davranışlarda bulunmamalı ve veri güvenliği için gerekli özeni göstermelidirler. **COVID-19 salgını hükümetlerin ve devletlerin toplamış oldukları verilerin üçüncü taraflar ile paylaşılmasına bir bahane olmamalıdır.**

7. COVID-19 ile artan dijital gözetleme hiçbir güvenlik gücünün ya da istihbarat teşkilatlarının alanlarına girmemelidir. **Konuyla ilgili uygun ve bağımsız organlar tarafından dijital gözetleme gerçekleştirilmelidir.**

Bahsi geçen dijital boyut yanında tıbbi teçhizatın da güvenlik aygıtlarının diğer aktörlerden önce erişmeye çalıştığı stratejik önemi haiz metalar olarak hızla önem kazandığı görülmektedir.

8. COVID-19 için toplanan veriler paydaşların özellikle halk sağlığı sektöründeki uzmanların özgür, aktif katılımları için uygun araçlar içermelidir.<sup>16</sup>

Yukarıda sayılan 8 maddelik dijital gözetleme şartları ulusal ve uluslararası çeşitli sektörlerdeki sendikalar, düşünce kuruluşları, sosyal örgütler, öğrenci toplulukları ve özel şirketlerden oluşan 106 kuruluş tarafından imzalanmıştır.

Dijital gözetleme olarak salgınla birlikte güvenlik alanında daha çok tartışılan bu durum hem salgın süresince hem de salgın sonrasında temel bir sorun olan güvenlik-özgürlük ikilemini daha da derinleştireceğinden şüphe yoktur. Bununla birlikte, pek çok aktörün geliştirmekte olduğu özellikle akıllı çip ve yüz tanıma sistemleri noktasında atılımlar sağlayabileceği, bunlarla ilgili belirli mesafe kaydetmiş ülkelerin ise uygulama konusunda hem daha fazla kabul görebileceği hem de bu süreçte kapasitelerini test ederek erişimlerini artırabileceği bir dönem yaklaşmaktadır.

### COVID 19 Bağlamında Uluslararası Rekabet ve İstihbarat Servislerinin Rolü

Bahsi geçen dijital boyut yanında tıbbi teçhizatın da güvenlik aygıtlarının diğer aktörlerden önce erişmeye çalıştığı stratejik önemi haiz metalar olarak hızla önem kazandığı görülmektedir. İstihbari anlamda hastalıkla ilgili ilk gerilimlerden biri ABD'nin istihbarat kaynaklarına dayandırarak, Çin'in virüsün ciddiyetini ve



Salgının başlangıcında yalnızca 2000 solunum cihazına sahip olan İsrail’in diplomatik ilişkisi olmayan ülkelerden COVID-19 testleri ve pek çok farklı noktadan yüz binlere vardığı değerlendirilen maske teminini İsrail Savunma Kuvvetleri ve MOSSAD işbirliğiyle gerçekleştirdiği medyaya yansımıştır.

yayımlı hızını uzun süre dünyadan gizlediğini iddia etmesidir. Aynı iddia İngiltere gizli servisi MI6’in Ocak ve Şubat aylarında Çin’deki korona virüs vakaları ve ölümleri ile ilgili bilgilerin sayısal olarak eksik olduğunu İngiliz bakanlara vermiş olduğu brifingde belirtmesiyle de ortaya atılmıştır.<sup>17</sup> Bir yandan ülkeler tıbbi cihaz ve ekipmanların ihracatına sınırlamalar getirmekte, diğer yandan kimi aktörler mevcut atmosferde dünyaya aktardığı destekle salgın sonrası dünya ve dış politikaya dair önemli yatırımlar yapmakta, bir yandan ise kimi aktörler bu unsurların transferinde devreye girerek bunları kendi ülkelerine sokma yönünde çaba sarf etmektedir. Bu da her ülkede değişen bir doğaya ve koordinasyon sistematiğine sahip istihbari yapıların ve operasyonel güvenlik güçlerinin kapasitelerini artıracakları yeni bir alan doğurmaktadır. Yasadışı silah ticareti veya teknoloji hırsızlığı gibi daha kadim bazı odaklarla de benzerlikleri ve kesişim noktaları olacak biçimde, salgının çözümüne yönelik söz konusu girişimler bu yeni alanın öznesi konumundadır. Hastalığa dair çözüm geliştiren aktörün yalnızca prestij ve finansal anlamda kazancı değil, salgın

sonrası dünyada etki alanını artırma potansiyeli de düşünüldüğünde önce durumun kontrolü adına gerekli ekipmanın sağlanması, ardından olası ilerlemenin takibi, kopyalanması ve kendi ülkesi tarafından sonuçlandırılması güvenlik aygıtını öncelikle meşgul edecek konular durumdadır. Henüz meselenin teknoloji hırsızlığı boyutuna dair herhangi bir veri görmek mümkün olmamakla birlikte hem konunun doğası ve yöntemleri hem de aktörlerin çalışma tarzı itibarıyla bu oldukça olası bir durumdur. Tarihte bilinen pek çok teknoloji hırsızlığının yıllar sonra ve genelde de mevzu bahis teknolojinin transferini ve/ya etkisiz hale getirilmesini takiben gerçekleştiği ve pek çoğunun da aydınlatılmadan karşılıklı suçlamalara konu olarak rafa kalktığı düşünülürse bu önemli bir istihbari açık olmadıkça salgın sonrasındaki on yıllarda gündeme gelmesi olası bir başlıktır.

“Ekipman operasyonları” bağlamında ise iki önemli örnek ABD ve İsrail tarafından hayata geçirilmiş gözükmektedir. Salgının başlangıcında yalnızca 2000 solunum cihazına sahip olan İsrail’in diplomatik ilişkisi olmayan ülkelerden COVID-19 testleri ve pek çok farklı noktadan yüz binlere vardığı değerlendirilen maske teminini İsrail Savunma Kuvvetleri ve MOSSAD işbirliğiyle gerçekleştirdiği medyaya yansımıştır.<sup>18</sup> Bu iddia Channel 12’de yayınlanan Fact programında ismi açıklanmayan katılımcılar tarafından doğrulanmıştır. Rakamların düşük olduğu iddiasına karşın 1.5 milyon cerrahi maske ve on binlerce N95 maskenin ülkeye getirildiği ve ilaveten teknoloji noktasında yukarıda bahsedilen ihtimali doğrular nitelikte hastalığın tespiti ve tedavisine yönelik test, maske yapımı ve solunum cihazı yapımı odaklı olmak üzere teknoloji “transferi”nin gerçekleştirildiği iddia edilmektedir.<sup>19</sup> İtalya’ya Çin’den gönderilen 680 bin maske ise çalınarak Çekya’ya giriş yapmış ve burada takip edilmiştir. Çekya akabinde İtalya’ya maskeleri göndermesine karşın ülkeler arası güvensizliğin de benzer olaylarla tırmanması mümkün gözükmektedir. Avrupa’daki

pek çok ülkeyle birlikte ABD’de de oldukça sık aralıklarla yapılan operasyonlarda maskeleri toplu biçimde üretim yerlerinden çalan örgütler ve/ya fahiş fiyattan çalıntı maske satan kişi ve/ya gruplar yakalanmaktadır.<sup>20</sup>

Alman İçişleri Bakanlığı tarafından “modern korsanlık” olarak nitelenen bir olayda 200 bin maskeye Almanya’ya getirilirken ABD tarafından el konulduğunu iddia edilmiştir. Çin’de imal edilen ve Tayland üzerinden Almanya’ya gönderilecek olan maskelere Bangkok Havalimanı’nda el konulduğunu ileri sürülürken ABD’li üretici firma 3M bahsi geçen siparişin varlığını inkar etmiştir.<sup>21</sup> Öte yandan Almanya’nın Şubat ortasında teslim alması gereken 6 milyon FFP2 özellikli maskenin ise Kenya’da kaybolduğu ileri sürülmüş, bunların akıbetine dair ise kesin açıklama yapılamamıştır.<sup>22</sup> Almanya ise komşuları İsviçre ve Avusturya’ya maske satışını kısıtlayarak sipariş edilen maskelerin bu ülkelere ulaşmasını engellemiş, neticesinde İsviçre ve Avusturya ile Almanya arasında gerilim yükselmiştir. İki ülke tarafından Almanya, Avrupa’daki birliğe uymayan tavırlar göstermekle suçlanmıştır.

Bundan kısa süre önce ise Fransa benzer bir suçlama yöneltmiş, ülkeye gelecek maskelerin ABD’ye gittiğini iddia etmiş, ABD ise diplomatik kanallar aracılığıyla iddiaları yalanlamıştır. Bununla birlikte N95 özellikli maske üretiminin üçte ikisi ABD dışında olan 3M’in tıbbi ekipman ihracına getirilen kısıtlamalar, kısıtlama öncesi alınan siparişlere dair böylesi süreçlerin yüksek ihtimal olduğu değerlendirmesine yol açabilmektedir.<sup>23</sup> Fransa ve İspanya’dan gelen diğer suçlayıcı açıklamalar ise ABD firmalarının hem talep büyüklüğü hem de üç kata varan fiyat teklifleri dolayısıyla pek çok ülkenin önüne geçerek maske teminini dolaylı yoldan engellediğini ifade etmektedir.<sup>24</sup> Bu iklimde BM tarafından New York için gönderilen 250 bin hibe maske<sup>25</sup> ise muhtemeldir ki salgın sonrası uluslararası örgütlere dair başlayacak olan tar-

tışmanın önemli maddelerinden biri olacaktır. Hem devletler arasında hem sınır aşan organize suç yapılanmalarının birbirlerinden ve devletlerden maske, solunum cihazı ve tıbbi teknoloji elde etmeye dair illegal girişimlerin, DSÖ tarafından hastalığın 2021 hatta 2022’ye kadar etkinliğini sürdürebileceği yönündeki açıklamalar nedeniyle hareketle artması beklenebilir. Bu durum özellikle ekipman ve teknoloji üretim ve

CIA ve ABD Ulusal Tıbbi İstihbarat Servisi olan NCMI’nın kasım ayında Çin’de ortaya çıkan bir salgın ile ilgili uydu görüntülerini ve bilgisayar frekanslarını analiz ederek bir rapor hazırladığı öne sürülmüştür. Ocak ayı başına kadar ise brifingler ile Beyaz Saray’ın raporun çeşitli analizleri doğrultusunda bilgilendirildiği iddia edilmektedir.

transfer noktalarında da güvenliği oldukça kritik hale getirmiş durumdadır. Cerrahi maskeler gibi nispeten daha kolay ve daha fazla ülke tarafından üretilebilecek materyalin ötesinde, özellikle N95 maskeler, solunum cihazları ve hastalığın tedavisine dair bilimsel gelişmeler gibi konularda önümüzdeki iki yıl içerisinde benzer operasyonel hamlelerin olması mümkündür.

İstihbarat servisleri COVID-19 salgınının öncesinde ve devamında salgının yayılmasını

önlemek amacıyla önemli roller üstlenmiştir. Salgının ortaya çıkmasının akabinde istihbarat servislerinin etkinlikleri, çalışma sistemleri ve

Konuyla ilgili sıkı tedbirlerin alındığı İran’da parlamento üyesi Hassan Norouzi korana virüs hakkında sahte haber yayınlayanların 1 ila 3 yıl hapis cezasına çarptırılacağını söylemesi, İran’da yayınlanan vaka ve ölüm sayıları hakkındaki bilgilerin doğruluğunun tartışılmasına neden olmaktadır.

kapasiteleri yeniden gündeme gelmiştir. Salgının yayıldığı ülkelerdeki istihbarat servislerinin veri toplama ve hükümetleri bu veriler üzerinden oluşabilecek tehditlere karşı uyarma kabiliyetleri ülkelerin salgın ile mücadelelerinde önemli roller oynamaktadır.

CIA ve ABD Ulusal Tıbbi İstihbarat Servisi olan NCMI’nın Kasım ayında Çin’de ortaya çıkan bir salgın ile ilgili uydu görüntülerini ve bilgisayar frekanslarını analiz ederek bir rapor hazırladığı öne sürülmüştür. Ocak ayı başına kadar ise brifingler ile Beyaz Saray’ın raporun çeşitli analizleri doğrultusunda bilgilendirildiği iddia edilmektedir.<sup>26</sup> Ocak ve Şubat aylarına kadar ise COVID-19 salgını ile ilgili detaylı istihbarat raporları olmasına rağmen, Trump yönetimi bunları ciddiye almamış, Ocak ayı sonlarına doğru Çin’in salgınla olan mücadelesini öven sözler sarf etmiştir.<sup>27</sup> Nitekim salgının ABD’ye

ulaşması ve binlerce insanın hayatını kaybetmesine neden olması üzerine Trump’ın salgını ve kendisine verilen istihbarat raporlarını ciddiye almaması ABD tarihindeki en kötü ve tehlikeli politika başarısızlık olarak tartışılmaya başlanmıştır.

İngiltere’de ise COVID-19 salgını sonrasında istihbarat servislerinin bilgi ileme ve veri toplama kapasitelerinin yetersiz görülmesi, salgına dair ön bir bilginin hükümete iletilmemesi büyük tartışmalara yol açarken, MI5 ve MI6’ye tahsis edilen 3 milyar sterlinin üzerindeki bütçeleri sorgulanmaya başlamıştır. Bununla birlikte MI5 ve MI6 gibi servislerin içerisinde herhangi bir salgın durumunda konuyla ilgili çalışabilecek yeterli kapasitedeki uzman bulunmaması, buna ek olarak COVID-19 krizine karşı hükümetin alacağı kararları hızlandıracak istihbari bilgi eksikliği İngiltere’nin istihbarat altyapısının zaafiyeti olarak değerlendirilmektedir.<sup>28</sup>

İran’da COVID-19 salgınının hızla yayılmasının akabindeyse yönetim salgını tamamen politik ve güvenlik eksenli olarak ele almış ve Devrim Muhafızları ve istihbarat servisi MOIS tarafından vakalara dair bilgiler gizlenmeye başlamıştır. İstihbarat birimleri sağlık personelinin hangi bilgileri açıklayacağına dair yetkiyi ellerinde tutmakta ve bu bilgilerin halka, medyaya ve uluslararası topluma ifşa edilmesini yasaklamış durumdadırlar. Konuyla ilgili sıkı tedbirlerin alındığı İran’da parlamento üyesi Hassan Norouzi korana virüs hakkında sahte haber yayınlayanların 1 ila 3 yıl hapis cezasına çarptırılacağını söylemesi, İran’da yayınlanan vaka ve ölüm sayıları hakkındaki bilgilerin doğruluğunun tartışılmasına neden olmaktadır.<sup>29</sup>

Salgın sürecinde ise istihbarat servislerinin yürüttüğü çalışmalar genel itibariyle vaka ve ölüm oranlarına dair bilgilerin gizlenmesi ve dijital platformlar başta olmak üzere uluslararası sistemde yürüttükleri propaganda savaşı olarak değerlendirilmektedir. Çin’in salgının başlan-



gıç tarihini gizlemesi ve ülke içerisinde vaka ve ölüme dair istatistiksel bilgilerin paylaşılmamasına dair yürüttüğü baskı rejimi, İspanya’da huzur evlerinde salgından dolayı hayatını kaybedenleri ve İtalya’nın hastane dışında ölen kişileri salgın ile ilişkilendirmemesi,<sup>30</sup> ABD’de ise, evsizlerin salgın karşısında savunmasız kaldığı ve New York, Florida gibi eyaletler dışında hükümetin genel bir yardım kampanyasının olmadığı bir ortamda, virüsten dolayı hayatını kaybeden birçok evsiz kayıtlara geçmemiştir.<sup>31</sup> Vakaların ve ölümlerin saklanması arkasında ise ülkelerin iç ve dış politikalarının yanı sıra ekonomik ve ticari kaygılar ve vatandaşlarının tepkilerini en az seviyeye indirme amacı yatmaktadır. Dolayısıyla, salgından etkilenen birçok ülkenin istihbarat servisleri ve hükümetleri vakalar ile ilgili bilgileri gizlerken Çin’in salgının başlangıç tarihi hakkında yanlış bilgi verdiği, vakaların Çin hükümeti tarafından gizlendiği, salgının Çin’in tedbirsiz davranması nedeniyle tüm dünyaya yayıldığı gibi konularda propaganda faaliyetleri yürütmektedirler. Trump’ın salgının başlangıcından itibaren virüsü “Çin Virüsü” olarak isimlendirmesi, Macron’un son dönemlerde

Çin’in virüs ile ilgili bilgileri eksik verdiği dair söylemleri bu açıdan değerlendirilebilir.

## Sonuç

COVID-19 salgını dünyada sağlık sistemi ile birlikte güvenlik alanında da yeni tartışmaların ortaya çıkmasına neden olmuştur. Bir taraftan birçok ülkede hayata geçirilen ve yaygınlaştırılmaya çalışılan dijital uygulamaları ve web sitelerini salgının yayılım hızını düşürmek ve enfekte olan kişilerin izolasyonunu sağlamak adına önemli bir adım olarak değerlendirmek mümkündür. Diğer taraftan ise bu dijital mücadele, milyonlarca kişinin kimlik bilgilerinin ve hareketlerinin izlenmesi ve aynı zamanda da yapay zeka uygulamaları ve yüz tanıma sistemleriyle entegre çalışmaları ile ortaya çıkabilecek insan hakları ihlallerini ve veri güvenliği sorunlarını gündeme getirmektedir. Dijitalleşmenin COVID-19 sürecinde kazandığı bu boyut bir yandan verilerin devlet-dışı silahlı aktörler, sınır aşan suç yapılanmaları ve diğer devletler tarafından ele geçirilmesi riskini, diğer yandan ise ülke sınırları dahilinde hak ihlallerinin artması riskini beraberinde getirmekte, bu da güven-

“  
Dijitalleşmenin COVID-19 sürecinde kazandığı bu boyut bir yandan verilerin devlet-dışı silahlı aktörler, sınır aşan suç yapılanmaları ve diğer devletler tarafından ele geçirilmesi riskini, diğer yandan ise ülke sınırları dahilinde hak ihlallerinin artması riskini beraberinde getirmekte, bu da güvenlik-özgürlük ikilemine dair en önemli sorulardan birini oluşturmaktadır.”

lik-özgürlük ikilemine dair en önemli sorulardan birini oluşturmaktadır.

İstihbarat servisleri ve devletlerin güvenlik

aygıtı içerisindeki farklı yapılar tarafından ülke içinde ve dışında güvenliği sağlamak ve salgınla mücadeleyi desteklemek amacıyla özellikle ekipman ve teknoloji transferi bağlamında gerçekleştirilen operasyonlar giderek görünürlük kazanmakta ve artmaktadır. COVID-19 salgını sonrası hem istihbarat servislerinin araç ve planlamalarında hem de operasyonel çabalarının kapsam ve yönteminde değişimlerin yaşanması muhtemeldir. Salgın ile ilgili verilen toplanması ve sınıflandırılması, ekipman tedariki ve teknoloji transferi bağlamında istihbarat servislerinin sahada daha aktif bir rol alacağı değerlendirilebilir. Bunlarla birlikte hem devletlerin sağlık ve insan güvenliği ile ilgili kurumlarının hem de bilgi-iletişim firmalarının daha fazla öne çıkacağı, bu alanlara yapılan yatırımın artacağı ve bu aktörler arası işbirliğinin teşvik edileceği bir döneme doğru ilerlendiğini değerlendirmek mümkündür. İstihbarat servisleri tarafından elde edilen verilerin işlenerek raporlanması ve bu raporların ülkelerin politikalarına dönüşmesi salgının durdurulmasından ziyade diğer devletlerin sahip oldukları teknolojik imkanlar, ilaç endüstrisindeki kapasiteler, sağlık sistemlerinin gelişim düzeyleri gibi alanlara hakim olunma-



sı bağlamında değerlendirilmektedir. Nitekim mevcut salgına dair üretilecek aşı ya da ilacın istihbarat servisleri tarafından yakın takibi gerçekleştirilecektir, bu yöndeki olası gelişmeler neticesinde servislerin sürecin kendi ülkeleri tarafından tamamlanması için oldukça önemli rolleri olabilecektir. Bununla birlikte hem ulusal hem bölgesel ve küresel ölçekte işbirliği mekanizmalarının sağlık başlığını daha fazla önceleyeceğini, bu konuda mevcut yapılardan başarısız sınav verenlerin sorgulanacağını, ileriye dönük sağlık odaklı yeni uluslararası yapılanmalara gidilebileceğini ya da mevcutlara yeni araçlar eklenebileceğini de öngörmek mümkündür.

Ulusal düzlemde özellikle insani güvenlik ve daha dar bağlamda sağlıkla ilgili kurum, kuruluş ve bakanlıkların öneminin artacağı, bunlar altında salgın hastalıklara yönelik daha kapsamlı, profesyonel ve uzmanlaşmış yapılar teşkil edileceği değerlendirilebilir ki bu kuruluşlar hem mevcut hastalıkla mücadele hem de ileriye dönük benzer durumlarda ulusal düzeydeki etkinlikleri dolayısıyla ana aktör olmaya devam edeceklerdir. Özel şirketler ve üniversitelerin

ise özellikle dijital mücadelede yukarıda bahsi geçen ülke örneklerinden hareketle böylesi bir mücadelenin olmazsa olmaz parçaları olduğu, hem mücadelenin dizaynı ve araçların ortaya konması ve geliştirilmesi, hem de toplanan verilerin diğer aktörlere karşı muhafaza edilmesi noktasında yazılım firmalarının ve üniversitelerin ilgili programlarının resmi kurumlarla birlikte çalışma pratiğinin daha fazla gelişeceği bir süreci beklemek, bunun sağlanabilmesi için de gerekli imkanların bu yapılara da sunulması gereğinin altını çizmek mümkündür. Bu alanlardaki olası başarısızlıklar COVID-19 sonrasındaki ekonomik ve sosyal iklimde daha içe kapanık ve birbirleriyle ilişkilerini gözden geçiren devletleri, ittifak sistemlerine, ikili ilişkilere ve uluslararası örgütlere dair önemli bir sorgulama sürecini, yasadışı yapılara ve devlet-dışı aktörlere açılan daha geniş alanları ve radikal hareketler için daha elverişli beşeri kaynakları beraberinde getirebilecektir. Dünyanın büyük ölçüde hazırlıksız yakalandığı oldukça bütüncül ve uluslararası güvenliği doğrudan ilgilendiren bir tehditle karşı karşıya kalmış olması neticesinde mücadelenin de hem ulusal hem bölgesel hem küresel ölçekte verilmesi gerekmektedir.

## Kaynakça

“Coronavirus: Israel’s spy agency Mossad admits to stealing face masks overseas amid global PPE shortage, The New Arab, 14/4/2020.

“Coronavirus: US accused of ‘piracy’ over mask ‘confiscation’”, BBC, 4/4/2020.

“Covid-19: Thousands download coronavirus tracking app in Austria”, The Star, 2/4/2020.

“Free Japanese-language medical app offers advice about coronavirus”, The Japanese Times, 23/2/2020.

“US firm denies German ‘piracy’ claims over vanished face masks”, DW, 4/4/2020; “Berlin accuses US of ‘piracy’ over face masks”, Politico, 4/3/2020.

“US hijacking mask shipments in rush for coronavirus protection”, The Guardian, 3/4/2020.

“World risks permanent surveillance with coronavirus controls”, DW, 2/4/2020.

“China launches Coronavirus ‘close contact detector’”, BBC, 11/2/2020.

“Intelligence services, armies wage ‘war’ over masks amid COVID-19 outbreak”, Daily Sabah, 27/3/2020.

“Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights”, Human Rights Watch, 2/4/2020.

Amanda Shendruk, “South Koreans are using smartphone apps to avoid the novel coronavirus, Quartz, 29/2/2020.

Ben Caspit, “Mossad, Netanyahu’s secret weapon against the coronavirus”, 1/4/2020.

Bhaswati Guha Majumder, “Free medical app with 120 doctors in Japan comes to rescue of users on Coronavirus scare “, IBT, 24/2/2020.

Caroline Kelly, “Washington Post: US Intelligence warned trump in january and february as he dismissed coronavirus threat”, CNN, 21/3/2020.

Cindi Cook, “Coronavirus: 2K face masks stolen from French hospital”, Anadolu Agency, 4/3/2020.

Connor Perrett, “People are stealing masks and other sterile supplies from hospitals and research facilities amid a global shortage”, Business Insider, 7/3/2020.

Helen Davidson, “China’s Coronavirus health code apps raise concerns over privacy”, The Guardian, 1/4/2020.

Israel Salas-Rodriguez, “UN donates 250K face masks to NYC health care workers”, New York Post, 28/3/2020.

Janosch Delcker and Stephen Brown, “Europe shares code for new Coronavirus warning app”, Politico, 1/4/2020.

Jennifer Valentino-DeVries, “Translating a surveillance tool into a virus tracker for democracies”, The New York Times, 19/3/2020.

Josh Margolin and James Gordon Meek, “Intelligence Report warned of coronavirus crisis as early as november: sources”, ABC News, 9/4/2020.

Judah Ari Gross, “Netanyahu sparks privacy scare with move to track corona patients’ phones”, The Times of Israel, 15/3/2020.n

Ken Dilanian, “spying on coronavirus: a little-known U.S. intel outfit has its most important mission yet”, NBC News, 13/3/2020.

Laura Romero, “For American’s Homeless Staying Home During Coronavirus Outbreak Is Not An Option”, ABC News, 25 /03/2020.

Lucy Williamson, “Coronavirus: The Grim crisis in Europe’s care homes”, BBC, 31/3/ 2020.

Majid Rafizadeh, “How Iran is cracking down on the truth on coronavirus”, Arab News, 19/3/2020.

Mark Zastrow, “South Korea is reporting intimate details of COVID-19 cases: has it helped?”, Nature, 18/3/2020.

Matt Kennard, “British security services have ignored global health pandemics The UK’s biggest threat” Daily Maverick, 24/3/2020.

Maya Wang “China: Fighting COVID-19 with automated tyranny, HRW, 1/4/2020.

Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, 2020.

Paul Mozur, Raymond Zhong ve Aaron Krolik, “In Coronavirus fight, China gives citizens a color code, with red flags”, The New York Times, 1/3/2020.

San Dabbagh, “UK spy agencies urge china rethink once covid-19 crisis is over”, The Guardian, 14/4/2020.

Steven Feldstein, “Beware the implications of coronavirus surveillance”, Carnegie Endowment, 31/3/2020.

Stuart Winer, “Healty Minister Launches Phone App to Help Prevent Spread of Coronavirus”, The Times of Israel, 23/3/2020.

Toi Staff , “Mossad said to bring in 100.000 virus tests, but usefulness of kits doubted”, The Times of Israel, 16/3/2020.

Tova Cohen, “1.5 million Israelis using voluntary coronavirus monitoring app”, Reuters, 1/4/2020

## Sonnot

- 1 Helen Davidson, “China’s Coronavirus health code apps raise concerns over privacy”, The Guardian, 1/4/2020.
- 2 Maya Wang, “China: Fighting COVID-19 with automated tyranny”, HRW, 1/4/2020.
- 3 “China launches Coronavirus ‘close contact detector’”, BBC, 11/2/2020.
- 4 Paul Mozur, Raymond Zhong ve Aaron Krolik, “In Coronavirus fight, China gives citizens a color code, with red flags”, The New York Times, 1/3/2020.
- 5 Tova Cohen, “1.5 million Israelis using voluntary coronavirus monitoring app”, Reuters, 1/4/2020; Judah Ari Gross, “Netanyahu sparks privacy scare with move to track corona patients’ phones”, The Times of Israel, 15/3/2020.
- 6 Stuart Winer, “Healthy Minister Launches Phone App to Help Prevent Spread of Coronavirus”, The Times of Israel, 23/3/2020.
- 7 Janosch Delcker and Stephen Brown, “Europe shares code for new Coronavirus warning app”, Politico, 1/4/2020.
- 8 Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, 2020.
- 9 Ken Dilanian, “spying on coronavirus: a little-known U.S. intel outfit has its most important mission yet”, NBC News, 13/3/2020.
- 10 Jennifer Valentino-DeVries, “Translating a surveillance tool into a virus tracker for democracies”, The New York Times, 19/3/2020.
- 11 Mark Zastrow, “South Korea is reporting intimate details of COVID-19 cases: has it helped?”, Nature, 18/3/2020; Amanda Shendruk, “South Koreans are using smartphone apps to avoid the novel coronavirus”, Quartz, 29/2/2020.
- 12 “Covid-19: Thousands download coronavirus tracking app in Austria”, The Star, 2/4/2020.
- 13 “World risks permanent surveillance with coronavirus controls”, DW, 2/4/2020.
- 14 Steven Feldstein, “Beware the implications of coronavirus surveillance”, Carnegie Endowment, 31/3/2020.
- 15 “Free Japanese-language medical app offers advice about coronavirus”, The Japanese Times, 23/2/2020. Bhaswati Guha Majumder, “Free medical app with 120 doctors in Japan comes to rescue of users on Coronavirus scare”, IBT, 24/2/2020.
- 16 “Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights”, Human Rights Watch, 2/4/2020.
- 17 San Dabbagh, “UK spy agencies urge china rethink once covid-19 crisis is over”, The Guardian, 14/4/2020.
- 18 Toi Staff, “Mossad said to bring in 100.000 virus tests, but usefulness of kits doubted”, The Times of Israel, 16/3/2020.
- 19 “Coronavirus: Israel’s spy agency Mossad admits to stealing face masks overseas amid global PPE shortage”, The New Arab, 14/4/2020; Ben Caspit, “Mossad, Netanyahu’s secret weapon against the coronavirus”, 1/4/2020.
- 20 Connor Perrett, “People are stealing masks and other sterile supplies from hospitals and research facilities amid a global shortage”, Business Insider, 7/3/2020; Cindi Cook, “Coronavirus: 2K face masks stolen from French hospital”, Anadolu Agency, 4/3/2020.
- 21 “US firm denies German ‘piracy’ claims over vanished face masks”, DW, 4/4/2020; “Berlin accuses US of ‘piracy’ over face masks”, Politico, 4/3/2020.
- 22 “Intelligence services, armies wage ‘war’ over masks amid COVID-19 outbreak”, Daily Sabah, 27/3/2020.
- 23 “US hijacking mask shipments in rush for coronavirus protection”, The Guardian, 3/4/2020.
- 24 “Coronavirus: US accused of ‘piracy’ over mask ‘confiscation’”, BBC, 4/4/2020.

- 25 Israel Salas-Rodriguez, “UN donates 250K face masks to NYC health care workers”, New York Post, 28/3/2020.
- 26 Josh Margolin and James Gordon Meek, “Intelligence Report warned of coronavirus crisis as early as november: sources”, ABC News, 9/4/2020.
- 27 Caroline Kelly, “Washington Post: US Intelligence warned trump in january and february as he dismissed coronavirus threat”, CNN, 21/3/2020.
- 28 Matt Kennard, “British security services have ignored global health pandemics The UK’s biggest threat” Daily Maverick, 24/3/2020.
- 29 Majid Rafizadeh, “How Iran is cracking down on the truth on coronavirus”, Arab News, 19/3/2020.
- 30 Lucy Williamson, “Coronavirus: The Grim crisis in Europe’s care homes”, BBC, 31/3/ 2020
- 31 Laura Romero, “For American’s Homeless Staying Home During Coronavirus Outbreak Is Not An Option”, ABC News. 25/3/2020.



📍 Mustafa Kemal Mah. 2128. Sok.  
No:3 Çankaya/Ankara

☎ +90 (850) 888 15 20  
📠 +90 (312) 430 39 48

✉ info@orsam.org.tr  
🌐 www.orsam.org.tr

📺 info@orsam.org.tr  
📺 info@orsam.org.tr