Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu

Faruk Çayır

alternatif bilişim

Avrupa Birliği sivil düşün

PANDEMİ TAKİP UYGULAMALARI VE KİŞİSEL VERİLERİN İZLENMESİ RAPORU

Kasım 2020

ISBN 978-605-80007-6-6

Yazar:
Faruk Çayır

Editör:
Kazım Anıl Doğruluk

Kapak Tasarım:
Cemgazi Yoldaş

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

Bu kitap Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır.
İçeriğin sorumluluğu tamamıyla Alternatif Bilişim'e aittir ve AB'nin görüşlerini yansıtmamaktadır.

İçindekiler

SUNUŞ

Tüm dünyayı etkisi altına alan Covid-19 pandemisi, birçok soru ve sorun alanını beraberinde getirmiştir. Bu sorun alanlarından bazıları, tüm iletişim faaliyetlerinin dijital ortamlara taşınmasıyla birlikte kişisel verilerin korunmasına ilişkin kaygı ve yine dijital ortamda üretilen nefret söylemlerinin artmasıdır. Alternatif Bilişim Derneği olarak pandemiyle birlikte belirginleşen bu sorun alanlarının izlenmesinin, raporlanmasının ve paylaşılmasının farkındalık yaratmak ve bu sorunlarla mücadeleye katkı sağlamak açısından önemli bir çaba olduğuna inanıyoruz. Böylesi bir sorumlulukla, Avrupa Birliği Sivil Düşün Programı'nın Covid-19 pandemi sürecinde sivil toplum kuruluşlarına verdiği "Bizi Bağlayan Şeyler" desteği kapsamında iki konuda izleme, raporlama ve dijital okuryazarlığı geliştirmek için webinar malzemesi üretimini üstlendik. Bu kapsamda, Derneğimizin Başkanı Faruk Çayır tarafından **Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu** ve üyemiz Doç. Dr. Zeynep Özarslan'ın editörlüğünde İlden Dirini ve Gökçe Özsu tarafından **Covid-19 Pandemi Sürecinde Sosyal Medyada Nefret Söylemi Raporu**'nu hazırladık.

Covid-19 pandemi sürecinde neredeyse tüm ülkelerde geliştirilen ve gündelik yaşamın bir parçası haline gelen pandemi takip uygulamalarının kişisel verilerin korunması bağlamında izlenmesi ve değerlendirilmesi gerekmektedir. Bu nedenle ilk raporda Türkiye özelinde Hayat Eve Sığar (HES) uygulamasının kişisel verilerin korunması temelinde durumu ele alınmaktadır. Pandeminin yaygınlaşmasını önlemek üzere Türkiye'de Sağlık Bakanlığı tarafından yaşama geçirilen veri gözetimi temelli işleyen HES gibi teknolojik çözümlerin kamu erki tarafından adil, şeffaf ve hesap verilebilir şekilde yaşama sokulması gerekmektedir. İzleme raporumuzda da ortaya konduğu üzere, HES gibi teknolojik çözümler, siyasi kararın/iradenin bir çıktısıdır ve bu tür temas izleme uygulamaları, "hükümetlerin büyük bir gözetim yetkisine sahip olmasını sağlayacağı gibi; kişilerin, sağlık, cinsiyet, yaş, dil, din, ırk, etnik köken, milliyet, göçmenlik statüsü veya engellilik gibi hassas verileri işlendiğinden, toplumda ciddi bir önyargı ve ayrımcılık yaratma riski taşımaktadır."

Pandemi sürecinde, Türkiye'deki sosyal medya platformlarında dikkat çeken bir diğer olgu da nefret söyleminin çeşitli türlerinin artması ve iç içe geçmesidir. Bu nedenle ikinci raporumuzda, sosyal medya platformlarından YouTube, Instagram, Facebook ve Twitter'da nefret söylemini, bu söylem türlerini ve söylem olarak işleme/meşrulaştırılma ve doğallaştırılma mekanizmaları ele alınmaktadır. Bu raporda, özellikle Çinlilere, 65 yaş ve üzeri kişilere ve LGBTİ+ bireylere yönelik artan nefret söyleminin kullanıcı türevli içeriklerle nasıl üretilip dolaşıma sokulduğu örneklerle ortaya koyulmuştur.

Son olarak, verileştirilmiş toplum, veri gözetimi, gözetim kapitalizmi, dijital güvenlik, kişisel veri, kişisel verilerin korunması, pandemi takip uygulaması konuları üzerine uzmanlar ve akademisyenler ile görüşmeler yaparak bir webinar serisi hazırladık. Özellikle sivil toplum kuruluşları ve yurttaşlar olarak "kişisel verilerin korunması" konusunda neler yapabiliriz sorusuna, Derneğimizin YouTube kanalına yüklediğimiz bu webinarlar ile yanıt vermeyi amaçladık.

Yurttaşlara ve hak temelli çalışma yapan tüm sivil toplum kuruluşlarına veri hakkı, kişisel verilerin korunması ve sosyal medyada nefret söylemi konularında farkındalık kazandırmayı amaçladığımız bu çalışmalar, Derneğimiz web sitesinde Türkçe ve İngilizce olarak açık erişim ve açık bilim politikası kapsamında ücretsiz olarak paylaşılmaktadır.

Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi ve **Covid-19 Pandemi Sürecinde Sosyal Medyada Nefret Söylemi Raporları**'nın okurlarına ulaşması ve Dernek olarak önemsediğimiz ifade özgürlüğü, veri hakkı, şeffaflık, hesap verilebilirlik, bilgiye erişim, açık kaynak ve özgür yazılım farkındalıkların yaşama geçmesi dileğiyle,

Prof. Dr. Mutlu Binark ve Dr. Yeliz Dede Özdemir
Proje Koordinatörleri
Ankara 26 Eylül 2020

I- KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması ile ilgili olarak ülkemizde ve dünyada uzun yıllardan beri çalışmalar ve düzenlemeler yapılmaktadır. Bununla birlikte kişisel verilerin korunması, iletişim teknolojilerinin gelişimi karşısında hızla boyut değiştirmektedir. Küresel anlamda bilgi işlem hizmetlerinin yaygınlaşması ile ülkeler arasında artan veri trafiği nedeniyle kişisel veriler sosyal ve ekonomik açıdan uluslararası öneme sahip hale gelmiştir. Sosyal ağlar, bulut bilişim, büyük veri analizi, konum bazlı hizmetler ve akıllı kart gibi teknolojik gelişmeler ile küreselleşmenin getirdiği zorunluluklar başta olmak üzere pek çok etken kişisel verilere erişim, verilerin toplanması ve kullanımı yöntemlerini derinden etkileyerek değiştirmektedir. Bu nedenle, küresel anlamda ülkelerin veri koruma hukuki altyapılarını güncel teknolojik gelişmelerle uyumlaştırma yönünde adımlar atılmaya başlanmıştır.

Temel bir insan hakkı olan ifade özgürlüğü açısından kişisel verilerin korunması vazgeçilemeyecek bir haktır. Türkiye'de kişisel verilen korunması alanında ilk düzenlemelerden biri 12 Eylül 2010 referandumuyla yapılan Anayasa değişikliği ile anayasanın 20. maddesine getirilen düzenlemedir. Ancak bu düzenlemenin tek başına yeterli olmayacağı ve bu alana ilişkin özel bir kanun ile düzenleneceği yine ilgili maddede belirtilmiştir. 2010 yılında Anayasa değişikliği ile Anayasa'nın Özel Hayatın Gizliliği başlıklı 20. maddesine getirilen, "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*." düzenlemesi ile konuya açıklık getirilmeye çalışılmıştır.

Belirtmek gerekir ki, kişisel verilerin korunması konusunda 1981 yılında imzalanan 108 no'lu "Kişisel Veriler Hakkında Avrupa Konseyi Andlaşması", Türk Hukuk mevzuatı açısından önemli bir sorun teşkil etmektedir. 1981'de Avrupa Konseyi bağlamında, kısaca "108 No'lu Sözleşme" olarak bilinen "Convention for the protection of individuals with regard to automatic processing of personal data" (*Kişisel verilerin otomatik işlemden geçirilme sürecinde bireylerin korunması hakkında sözleşme*)[1] imzaya açılmış ve Türkiye tarafından da gecikmeksizin imzalanmıştır. Sözleşmenin yürürlüğe girişi ise 1986'da olmuştur. Ancak "108 no'lu Sözleşme" kişisel verilerin korunması konusunda genel ilkeleri tespitle yetinmektedir. Sözleşme'nin uygulan-

[1] Bakınız: http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm.

ması ise taraf devletlerin iç hukuklarında yapılacak düzenlemelerle mümkün olacaktır. Türkiye'de uzun yıllar kişisel verilerin korunmasına ilişkin kanuni bir düzenleme yapılmamış olsa da 2016 yılında, "6698 Sayılı Kişisel Verilerin Korunması Kanunu" yürürlüğe girmiştir. Buna rağmen gerek kanun, gerekse ikincil düzenlemelerin kâğıt üzerinde yeterli korumayı sağladığı düşünülse de kişisel verilerin işlenmesine ve aktarılmasına ilişkin istisnalar ile kişisel veri işleyen kamu kurum ve kuruluşlara ilişkin düzenlemeler yeterli veri koruma standartlarını sağlamamaktadır.

Kişisel verilerin korunması konusunda Avrupa Birliği'nde (AB) 1995 yılında yürürlüğe giren "95/46/AT sayılı AB Veri Koruma Yönergesi" kişisel verilerin korunması alanında tüm dünyada kabul gören bir çerçeve sunmaktadır. Ancak bahsetmiş olduğumuz teknolojik gelişmeler sonucunda, Avrupa Komisyonu tarafından üye ülkelerde uygulanmakta olan AB veri koruma kurallarında, Veri Koruma Yönergesinde benimsenen ilkelerin modernize edilmesi ve gelecekte vatandaşların mahremiyet hakkının garanti altına alınması amacıyla kapsamlı bir reforma gidilmesi ihtiyacı ortaya çıkmıştır.

1995 yılından itibaren AB üyesi ülkeler açısından uygulamada meydana gelen farklılıklar ve dijital dünyayla daha uyumlu hale getirilme ihtiyacı ortaya çıkan somut uyuşmazlıklar ile bu değişimi kaçınılmaz kılan siyasi açmazlar sebebiyle giderek zorunlu bir hal almıştır. Bu olayların başında, konuyla doğrudan olmasa da etkisi bakımından büyük ilgisi olan, 2013 yılında Edward Snowden tarafından ortaya çıkarılan mahremiyet ihlalleri gelmektedir. Bunun dışında ABD'de yapılan seçimlerde Cambridge Analytica Skandalı olarak bilinen olayda, Facebook'un kişilere ait verileri satması ve bu verilerin seçimlerde yönlendirme ile manipülasyon aracı olarak kullanılması, kişisel verilerinin korunmasının önemini bir kez daha ortaya koymuştur.

Snowden'ın açıklamaları Avrupa Birliği Adalet Divanı'nın (ATAD) mevcut hukuki uygulamalarında önemli bir değişimi benimsenmesine neden olmasının yanında Avrupa'da bireyin internetteki haklarının korunması konusundaki genel anlayışını da oldukça katılaştırmasına neden olmuştur. Mahkemenin bu çerçevede almış olduğu;

- Unutulma hakkı konusundaki Google-İspanya kararı,
- Mobil veya internet telefonu ile e-posta iletişimi verilerinin saklanması hususunda muhtemel bir soruşturma, araştırma ve suçun kovuşturulması amacıyla makul suç şüphesi bulunması gerektiğine ilişkin, 2006/24/EC sayılı Veri Saklama Direktifi'ni geçersiz kıldığı İrlanda Dijital Haklar kararı,
- Facebook tarafından kişisel verilerinin ABD'de tutulmasına ilişkin eşdeğer bir koruma seviyesinin bulunmaması nedeniyle Güvenli Liman Anlaşmasını

geçersiz kıldığı M.Schrems-Veri Koruma Komisyonu Kararı, kişisel verilerin korunması konusunda yeni ve kapsamlı bir reformu zorunlu kılmıştır.

Bu kapsamda, AB veri koruma kurallarında köklü bir reform olan, "Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)"[2], Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde onaylanmış, 25 Mayıs 2018 tarihinde ise yürürlüğe girmiştir.

AB'nin söz konusu düzenlemeyi, "regülasyon" yani tüzük[3] olarak düzenlemesi bağlayıcılık açısından da önemlidir. Regülasyonlar, genel olarak yürürlüğe girerek tüm üye ülkelerde yürürlük gücüne sahip olurlar. Ayrıca iç hukuka aktarılmak üzere bir onay kanununa ya da iç hukukta aynı düzenlemeleri konu alan yeni bir kanuna ihtiyaç göstermezler. Oysa yönergeler için durum farklıdır. Yönergeler üye devletleri hedef alır ve onlara belirli bir süre içinde yönergede belirtilen hususlarda ve o çerçevede iç hukukta düzenleme yapma ödevi yüklerler. İç hukukta yapılacak düzenlemenin yöntemi ise üye devletin takdirine bağlıdır. Bu açıdan, AB Genel Veri Koruma Tüzüğü üye ülkelerin düzenlemeleri ve onaylarına ihtiyaç kalmaksızın uymakla zorunlu oldukları bir düzenlemedir.

AB Genel Veri Koruma Tüzüğü[4] (GDPR), kişisel verilerin korunmasına ilişkin yeni tanımlar, yaklaşımlar ve zorunluluklar getirmektedir. Tüzüğün 3. maddesine göre,

"2. Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir kontrolör veya işleyici tarafından işlenmesine uygulanır:

a) Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya

b) Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi.

3. Bu Tüzük, Birlik içerisinde değil, ancak bir üye devletin hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde kurulu bulunan bir kontrolör tarafından kişisel verilerin işlenmesine uygulanır."

---

[2] Bakınız: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1797-1-1 .

[3] Türkçeye çevirisi bakımından anlaşılır olması için tüzük terimi kullanılacaktır.

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

Bu düzenlemede, GDPR hükümlerinin, sunucuları AB dışında yerleşik bulunan ve işleme faaliyetlerini Birlik ülkeleri dışından sürdüren bulut hizmet sağlayıcıları ile AB ülkelerindeki kişilere yönelik mal ve hizmet sağlayanlar bakımından da bağlayıcı olduğu görülmektedir. Bu açıdan Türkiye'nin Kişisel Verilerin Korunmasına yönelik yasal düzenlemelerini GDPR'a uygun hale getirmesi gerekmektedir.

Covid-19 pandemi sürecinde sıklıkla gündemde olan kişisel verilerin korunması, görüldüğü üzere 1981 yılından bu yana hukuk dünyamızdadır. Ancak Türkiye çeşitli vesile ve aşamalarla bu konuda düzenlemeler yapmış olsa da 24 Mart 2016 tarihinde TBMM'de kabul edilerek 7 Nisan 2016 tarihli, 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı "Kişisel Verilerin Korunması Kanunu"[5] tasarı aşamasında iken istisnalar ve Kişisel Verilerin Korunması Kurumu'nun yapısı hakkındaki eleştirilerin yanı sıra Genel Veri Koruma Tüzüğünde yer alan ve düzenlemesi elzem olan konular hakkındaki eleştiriler de göz ardı edilmiştir.

AB Veri Koruma Reformu kapsamında hazırlanan GDPR metninin Avrupa Parlamentosu'nda kabulü çok kısa bir süre önce onaylanmış ve 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. Türkiye'de halihazırda yürürlükte olan 6698 sayılı Kanun ise güncel kişisel veriler açısından daha fazla güvence sunan GDPR'daki düzenlemeleri değil; 95/46/AT sayılı Veri Koruma Direktifi'ni ve Avrupa Komisyonunun 108. Sayılı Sözleşmesi'ni referans almaktadır. Söz konusu metinlerin çevirisi niteliğini taşıması nedeniyle, GDPR'da yer alan birçok konuda eksik, yetersiz ve hatta kadük kaldığını söyleyebiliriz.

[5] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

II- AB GENEL VERİ KORUMA TÜZÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YENİLİKLER VE DÜZENLEMELER

AB Genel Veri Koruma Tüzüğü (GDPR), Avrupa'daki pek çok sivil toplum kuruluşunun yaratmış olduğu kamuoyu baskıyla yaşama geçmiş olup, kişisel verilerin korunması ve kişinin dijital hayattaki izlerine ilişkin pek çok yeni düzenlemeler içermektedir. 95/46 sayılı Direktif'teki ve 6698 sayılı Kanun, düzenleme bulunmayan bazı önemli gördüğümüz yenilikler ve düzenlemeleri aşağıda açıklamaya çalışacağız:

- ***Kişisel Veri Tanımı***

95/46 sayılı Direktif'teki ve 6698 sayılı Kanun'daki kişisel veri tanımına göre GDPR daha açıklayıcı ve kapsamlı bir tanım getirmeye çalışmıştır. GDPR'da kişisel veri tanımı, "*tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıdaki*" olarak kabul edilmiştir. Görüldüğü gibi konum verileri, çevrim içi tanımlayıcı gibi yeni teknolojilere uygun ve güncel veri sahibinin ortaya çıkarılmasını sağlayacak her türlü veri, kişisel veri olarak kabul edilmiştir.

- ***Profil Çıkarma***

GDPR'da 95/46 sayılı Direktif ve 6698 sayılı Kanun' da bulunmayan yeni bir tanımlama olarak "profil çıkarma" dikkati çekmektedir.

GDPR'da profil çıkarma, "*Bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi*" olarak tanımlanmıştır.

Veri sahiplerinin, kişisel verilerin otomatik karar verme mekanizmalarına bağlı olarak işlenmesi halinde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçlarına ilişkin bilgileri talep etme, kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama, profil çıkarmaya ilişkin kişisel verilerin işlenmesine herhangi bir zamanda ve kendisi ile ilgili kişisel

verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine itiraz etme ve itirazının kabul edilmemesi halinde yetkili kurula (Kişisel Verilerin Korunması Kuruluna) şikayette bulunma hakkı bulunmaktadır.

- ***Takma Ad Kullanımı***

GDPR'da, 95/46 sayılı Direktif ve 6698 sayılı Kanun'da bulunmayan başka bir yeni tanımlama da "takma adlı veri"dir. GDPR'da takma ad kullanımı, "*kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile ek bilgilerin ayrı tutulması ve teknik ve düzenlemeye ilişkin tedbirlere tabi tutulması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesi*" olarak tanımlanmıştır.

Veri kontrolörü, hem işleme yönteminin belirlenmesi, hem de işleme faaliyeti esnasında verilerin en alt düzeye indirilmesi gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ile tüzük gerekliliklerinin yerine getirilmesine yönelik gerekli güvencelerin entegre edilmesi amacıyla tasarlanan, takma ad kullanımı gibi uygun teknik ve düzenlemeye ilişkin tedbirler uygulamak ve veri sahiplerinin haklarını korumak zorundadır.

Kontrolör ile işleyicinin, gerçek kişilerin hak ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, kişisel verilerde takma ad ve şifreleme kullanımı dâhil olmak üzere uygun güvenceleri sağlaması gerekmektedir.

Takma adlı veri, kişisel veriyi anonim hale getirme olmayıp, verinin bir kimliksizleştirilmesi yöntemidir. Eğer veri sorumlusu tarafından işlenen veri, sorumlunun bir kişiyi doğrudan belirlemesine izin vermiyorsa ya da takma adlı veri oluşturuyorsa, veri sorumlusu yalnızca bu tüzüğe uyumluluk sağlamak için ilgili kişiyi belirlemek amacıyla söz konusu ek bilgileri alamaz ya da işleyemez. Tek başına kullanıldığında ve herhangi bir ek bilgi olmadan, bir bireyi tanımlayamayan ancak en fazla bireyleri tanımlamadan birbirinden ayırabilen veriler gibi veri tiplerine takma adlı veri diyebiliriz. Bu anlamda takma adlı verilere yönelik de koruma gerekmektedir.

Takma adlı veri olarak adlandırılan bu tür kişisel veriler, risk tabanlı yaklaşım ve sorumluluk açısından verilerin korunmasına yönelik iyi bir örnektir. Çünkü veri kontrolörü ile veri işleyen, verinin takma adlı veri olarak kalmasını sağlamak ve verilerin tamamen ilişkilendirilebilir hale gelmesini engellemek amacıyla gereken tüm makul önlemleri almak zorunda kalacaktır.

- ***Unutulma Hakkı***

GDPR'ın 17. maddesi kapsamında veri sahibinin kişisel verilerinin silinmesini isteme hakkı, "Unutulma Hakkı" başlığı altında düzenlenmiştir. Bu maddede, 6698 sayılı Kanun ve 95/46 sayılı Direktif'in 12. maddesinin (b) bendine nazaran, veri sahibine tanınan kişisel verilerin silinmesi hakkı kapsamının genişletildiği görülmektedir. Bu maddeye göre,

> "Veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini kontrolörden talep etme hakkı bulunur ve, aşağıdaki hallerden birinin geçerli olması durumunda, kontrolörün kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:
>
> - kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;
> - veri sahibinin, veri işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;
> - veri sahibinin, veri işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin doğrudan pazarlama ile alakalı olduğu ölçüde profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine itirazda bulunması;
> - kişisel verilerin yasa dışı biçimde işlenmiş olması;
> - kişisel verilerin doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak toplanmış olması.
>
> Kontrolörün kişisel verileri kamuya açıklamış olduğu ve kişisel verileri silmek zorunda olduğu hallerde, kontrolör, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin talep etmiş olduğu kişisel verileri işleyen kontrolörleri söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu kontrolörlerce silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dâhil olmak üzere makul adımları atmak zorundadır."

Bu maddeden de anlaşılacağı üzere veri sahipleri, verilerinin artık toplanma amacı ile ilgili olarak tutulmasının gerekli olmadığı, veri sahibin rızasının bulunmadığı yahut veri sahibinin verisinin işlenmesini istemediği veya kişisel verinin GDPR'a aykırı işlendiği durumlarda verilerinin silinmesini veya bundan sonra işlenmemesini talep edebilme hakkına sahiptir. Veri kontrolörünün, kişisel veriyi başka veri kontrolörleriyle paylaşmış veya kullanımlarına açmış olması durumunda, söz

konusu verilere ilişkin kısayol, kopya veya çoğaltılmış versiyonları silmelerinden de sorumlu olduğu görülmektedir.

Bu düzenlemeyle fiili ve hukuki anlamda, özellikle algoritmalar ile diğer otomatik veri işleme yöntemleri, verileri üzerinde denetim ve kontrolünü yitiren veri sahiplerine önemli bir hak tanınmıştır.

GDPR kapsamında kabul edilen unutulma hakkı da 6698 sayılı Kanun'da yer almamaktadır. Bununla birlikte unutulma hakkına ilişkin olarak; "cinsel taciz mağdurunun isminin kodlanmaksızın bir kitapta yayımlanmasından dolayı kişilik haklarının ihlal edildiği ve bu sebeple tazminata hükmedilen" Yargıtay 4. Hukuk Dairesi'nin 03.07.2013 tarih ve 2013/6256 esaslı kararında ve hakkında yapılan haberlerin internet ortamından silinmesi amacıyla başvuran kişinin haklı bulunduğu AYM'nin 03/03/2016 tarih ve B.2013/5653 no'lu kararı ile Türkiye'de yargı kararıyla uygulama alanı bulmuştur.[6] Yargı kararıyla da kabul edilmiş bulunan unutulma hakkı konusunda hukuki düzenlemelerde yer almaması 6698 sayılı Kanun'un yapım sürecinde de eleştirilere sebep olmuş idi. Bu sebeple AB üyesi devletler açısından büyük önem verilen unutulma hakkı konusunda Türkiye'nin de acil bir yasal düzenleme hazırlaması gerekmektedir.

Veri Taşınabilirliği Hakkı

6698 sayılı Kanun'da ve 95/46 sayılı Direktif'te yer almayıp da GDPR'da bulunan başka bir düzenleme ise veri taşınabilirliğidir. GDPR 20. maddesine göre, "veri

[6] AYM'nin 03/03/2016 tarih ve B.2013/5653 no'lu kararına göre: "Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiştir. Bununla birlikte Anayasa'nın "Devletin temel amaç ve ödevleri" başlığı altında düzenlenen 5. maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, İnternet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır." Bakınız: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653.

işleme faaliyetinin veri sahibinin usulüne uygun alınmış rızasına dayanması veyahut veri işlem faaliyetinin bir sözleşmeye dayanması, ya da veri işlemenin otomatik yollarla gerçekleşmesi halinde; veri sahibinin kendisi ile ilgili olarak bir kontrolöre sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı bulunur ve kişisel verilerin sağlandığı kontrolörün herhangi bir engellemesi olmaksızın bu verileri başka bir kontrolöre iletme hakkı bulunur."

Veri taşınabilirliği hakkı kullanılırken veri sahibinin, teknik açıdan uygulanabilir olması halinde, kişisel verilerini doğrudan bir kontrolörden diğerine iletiminin sağlama hakkı bulunur. Veri taşınabilirliği hakkının kullanımı, verilerin silinmesi talep etme (unutulma) hakkını ortadan kaldırmaz. Söz konusu hak, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması için gereken işleme faaliyetlerine uygulanmaz.

- ***Veri Kontrolörü ve Veri İşleyicisi Ayırımı, Veri İşleyenlerin Tamamının Veri İşlemeden Sorumlu Olması***

95/46 sayılı Direktif'te, "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"nin işlenmesine ilişkin kurallara uymakla yükümlü olan ve hukuka aykırı olarak yapılan iş ve işlemlerden sorumlu olan tek kişi "veri sorumlusu" (veri kontrolörü), başka bir ifadeyle veri sahipliğini elinde bulunduran kişi, olarak düzenlenmekteydi. GDPR ile kontrolör, işleyici ve alıcı olarak üçlü bir veri sahipliği/sorumluluğu düzenlemesi getirilmiştir.

Kontrolör, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kurum ve kuruluşları ya da diğer herhangi bir organdır.

İşleyici ise kontrolör adına kişisel verileri işleyen gerçek ya da tüzel kişi, kamu kurum ve kuruluşu veya diğer herhangi bir organdır.

Alıcı, üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kurum ve kuruluşu veya diğer herhangi bir organdır.

GDPR'da getirilen düzenleme ile veri sahipliğine ilişkin veri kontrolörü olmamakla birlikte bu verileri işleyen herhangi bir şirket ya da birey de, bulut hizmet sağlayıcıları gibi alt hizmet sağlayan üçüncü taraflar da dâhil olmak üzere, verinin hukuka uygun işlenmesinden sorumlu tutulacaklardır.

Bu düzenleme otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma,

saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisini uygulayanların, yani her türlü işleme faaliyetinin tüm faillerinin (kontrolör, işleyici, alıcı) söz konusu işlemeden kaynaklı her türlü veri ihlali ve hukuka aykırılıktan sorumlu olduğunu ortaya koymaktadır.

Bu hükmün uygulanmasının yansımaları oldukça geniş olacaktır. Hem veri sorumluları hem de veri sorumlusunun talebiyle veriyi işleyen üçüncü kişiler bakımından hukuki sorumluluk ortaya çıkmaktadır. Bu kapsamda GDPR hükümlerinin, sunucuları AB dışında yerleşik bulunan ve işleme faaliyetlerini Birlik ülkeleri dışından sürdüren bulut hizmet sağlayıcıları ile AB üyesi ülkelere mal ve hizmet sağlayan kuruluşlar bakımından da bağlayıcı olacaktır. Bu durumda hatalı ve hukuka aykırı işleme faaliyeti yapan bu kişi ve kuruluşlar açısından GDPR ile getirilen yüksek oranlı para cezaları bu işleyiciler için de bağlayıcıdır.

- ***Veri Sahibinin Rızası***

Veri işlemeyi hukuka uygun hale getiren veri sahibinin rızasına ilişkin 6698 sayılı Kanun ve 95/46 sayılı Direktif'te veri sahibinin "açık" rızasına vurgu yapılmaktaydı. GDPR'da ise veri sahibinin lehine olacak biçimde güçlendirilmiş bir rıza kavramı dikkat çekmektedir. GDPR'da tanımlar bölümünde veri sahibinin 'rızası', veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge olarak tanımlanmıştır.

Tüzüğün 7. maddesinde ise veri sahibinin rızasının diğer hususlarla da ilgili olan yazılı bir beyan bağlamında verilmesi durumunda, rıza talebi diğer hususlardan açık bir şekilde ayırt edilebilir, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulur. Söz konusu beyanın tüzük açısından ihlal teşkil eden hiçbir kısmı bağlayıcı değildir. Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, her şeyden önce, bir hizmetin sağlanması da dâhil olmak üzere bir sözleşmenin ifasının söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilmesi gerekmektedir.

Görüldüğü üzere, kişisel verilerin işlenmesine ilişkin rızanın özgürce, belirli ve aydınlatılmış/bir amaca ilişkin, bilinçli ve açıkça verilmiş olması gerekmektedir. Söz konusu rızanın veri işleyenin aynı amaç veya amaçlar için yürütülen tüm işleme faaliyetleri bakımından alınması gerekmektedir. Aynı şekilde rızanın elektronik

araçlarla istendiği durumlarda da bu istek sade, açık ve uğruna kullanıldığı hizmetten yararlanmayı engellemeyen bir mahiyette olmalıdır.

Diğer yandan kullanıcıların çevrimiçi sosyal ağların veya web tarayıcılarının gizlilik ayarlarına ilişkin sessiz kalmaları yahut o zamana kadar herhangi bir itirazda bulunmamış olmaları durumunda varsayılan ayarlar geçerli bir rızanın bulunmadığı anlamına gelecektir.

- ***Açık rızanın geri alınabilmesi***

Aynı şekilde GDPR 7. maddesi ile yapılan düzenlemeye göre, veri sahibinin istediği zaman rızasını geri çekme hakkı vardır. Rızanın geri çekilmesi, geri çekim işleminden önce rızaya dayalı olarak yapılan işleme faaliyetinin hukuka uygunluğunu etkilemez. Veri sahibi, rıza vermeden önce ilgili hususta bilgilendirilir. Rızanın geri çekilmesi rıza vermek kadar kolaydır. Tüzüğe göre veri sahibi, özgürce vermiş olduğu rızasını her zaman geri alma hakkına sahiptir. GDPR ile getirilen bu geniş hak ve yetki veri sahiplerine verilerinin kaderini belirleyebilme konusunda oldukça geniş bir alan sağlarken veri işleyenlere ise oldukça detaylı sorumluluklar yüklemektedir.

- ***Çocuğun Bilgi Toplumu Hizmetlerine İlişkin Rızası Açısından Geçerli Koşullar***

GDPR'ın 8. maddesi ile yeni getirilen düzenlemeye göre, veri sahibinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi durumunda, doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması halinde, söz konusu çocuğun kişisel verilerin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması hali ile verildiği veya onaylandığı ölçüde hukuka uygundur. Bu durumda veri kontrolörü mevcut teknolojiyi dikkate alarak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verildiğini veya onaylandığını doğrulamak adına makul çaba sarf etmek zorundadır.

Bu düzenlemeden de anlaşılacağı üzere, günümüz çocuklarının iletişim teknolojileri ve sosyal medya kullanımlarına yönelik ileride ortaya çıkması muhtemel bir hak ihlali gözetilmiştir. Çocukların kişisel verilerinin işlenmesinde 16 yaş sınırı gözetilmiş ve 16 yaşın altındaki çocuklar açısından velayet hakkı bulunan ebeveynden çocukların kişisel verilerinin işlenmesi için bir rıza zorunluluğu getirilmiştir.

- ***Veri Sahibinin Hakları***

GDPR 13. maddesine göre, "Bir veri sahibine ilişkin kişisel verilerin veri sahibinden toplanması durumunda, kontrolör kişisel verilerin elde edildiği anda aşağıdaki bilgilerin tamamını veri sahibine sağlar:

(a) kontrolörün ve, uygun olduğu hallerde, kontrolörün temsilcisinin kimlik ve irtibat bilgileri;
(b) uygun olduğu hallerde, veri koruma görevlisinin irtibat bilgileri;
(c) kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı;
(d) işleme faaliyetinin, veri sahibinin çocuk olması durumunda, kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatler;
(e) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;
(f) uygun olduğu hallerde, kontrolörün kişisel verileri üçüncü bir ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve Komisyon tarafından bir yeterlilik kararı verilip verilmediği, uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığına ilişkin bilgiler.

2. paragrafta atıfta bulunulan bilgilere ek olarak, kontrolör kişisel verilerin elde edildiği anda adil ve şeffaf bir işleme sağlanması için gereken aşağıdaki ek bilgileri veri sahibine sağlar:

(a) kişisel verilerin saklanacağı süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler;
(b) kontrolörden kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da silinmesini veya veri sahibi ile ilgili işleme faaliyetinin kısıtlanmasını talep etme ya da işleme faaliyetine itiraz etme hakkının yanı sıra verilerin taşınabilirliği hakkının varlığı;
(c) işleme faaliyetinin 6(1) maddesinin (a) bendine veya 9(2) maddesinin (a) bendine dayandığı hallerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğu etkilenmeden, herhangi bir zamanda rızayı geri çekme hakkının varlığı;
(d) bir denetim makamına şikayette bulunma hakkı;
(e) kişisel verilerin sağlanmasının yasal ya da sözleşmeye bağlı bir gereklilik mi yoksa bir sözleşme yapılması için gereken bir gereklilik mi olduğu ve ayrıca, veri sahibinin kişisel verileri sağlamak zorunda olup olmadığı ve söz konusu verilerin sağlanmamasının muhtemel sonuçları;

(f) profil çıkarma da dahil olmak üzere, otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.

3. Kontrolörün kişisel verileri bu verilerin toplanma amacı dışında bir amaçla işleme faaliyetine niyet ettiği hallerde, kontrolör söz konusu işleme faaliyetinden önce diğer amaca ilişkin bilgileri ve 2. paragrafta atıfta bulunulan diğer ilgili bilgileri veri sahibine sağlar.

4. Veri sahibinin hâlihazırda bu bilgilere sahip olduğu hallerde ve ölçüde, 1, 2 ve 3. paragraflar uygulanmaz."

Görüldüğü üzere GDPR, kişisel verilerin elde edildiği anda adil ve şeffaf bir işleme sağlanması için veri sahibine 6698 sayılı Kanun ve 95/46 sayılı Direktif'e göre geniş hak ve yetkiler tanımaktadır.

- ***Veri Sahibinin Haklarının Kullanımına İlişkin Şeffaf Bilgilendirme ve Bildirimde Bulunma Yükümlülüğünü Veri Kontrolörünün Yapma Zorunluluğu***

GDPR'ın 12. maddesinde kullanıcı haklarına ilişkin bilgilendirme yükümlülüğü veri kontrolörünün üzerine bırakılmıştır. Buna göre, "Kontrolör spesifik olarak bir çocuğa yönelik her türlü bilgi başta olmak üzere işleme faaliyeti ile alakalı olarak, veri sahibinden kişisel verilerin toplandığı hallerde ve veri sahibinden alınmadığı hallerde sağlanacak bilgiler atıfta bulunulan her türlü bilgi ile veri sahibinin verilerine erişim hakkı, düzeltme, kısıtlama ve silme hakkı, itiraz hakkı, profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı kapsamındaki her türlü bildirimi öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri sahibine sağlamak için gerekli tedbirleri alır. Bilgileri yazılı olarak veya uygun olduğu hallerde, elektronik yollar da dâhil olmak üzere diğer yollarla sağlar.

Kontrolör veri sahibinin haklarının kullanılmasına kolaylık sağlar."

Aynı şekilde GDPR'ın 24. maddesine göre, "Kontrolör, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, işleme faaliyetinin bu Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde

gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Bu tedbirler gözden geçirilir ve gerektiğinde, güncellenir."

Bu düzenlemeler birlikte değerlendirildiğinde, GDPR kapsamında veri kontrolörleri, kullanıcılarını bilgilendirmek ve sahip oldukları yasal haklar konusunda gerekli hatırlatmaları yapmakla yükümlü olup, aynı zamanda söz konusu yükümlülüklerini gerçekleştirdiklerini belgelemekle de sorumludur..

Tüzüğün 25. maddesine göre, "Kontrolör, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, verilerin en alt düzeye indirilmesi gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzük'ün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma ad kullanımı gibi uygun teknik ve düzenlemeye ilişkin tedbirler uygular ve veri sahiplerinin haklarını korur."

Yine bu hükümler birlikte değerlendiğinde, kullanıcılara ilişkin kişisel verilerin, kontrolörün sistemlerinde verisi saklanacak olan kişinin her ne şart altında olursa olsun mutlak suretle izninin alınmış olması gerekmektedir. Bu sistemde herkesin ücretsiz, kolay ve çabuk biçimde dilediği zaman sistemden ayrılma hakkı bulunmaktadır. Bu kuralın ihlal edilmesi durumunda veri kontrolörleri ağır tazminatlar ödemek zorunda kalacaklardır.

Aynı zamanda 25. maddeye göre, veri kontrolörü iç işleyişi ile alakalı politikalarını belirleyerek, veri işlemesine **başlangıçtan itibaren veri koruması ve tasarımdan itibaren gizlilik ve veri koruması ilkelerini karşılamaya yönelik gerekli tedbirleri almalıdır**. Bu ilkeye göre veri kontrolörü, gerek veri işleme vasıtalarının ve yönteminin belirlenmesi sırasında, gerekse veri işleme anında öngörülen veri koruma kurallarının etkili bir biçimde uygulanması için gerekli araçları kullanarak bulanıklaştırma, takma ad kullanımı, asgari veri işleme ve benzeri uygun teknik ve yapısal önlemleri almalıdır. Veri kontrolörü, kişisel verilerinin veri sahibinin herhangi bir girişimi olmaksızın belirsiz sayıda kişinin erişimine açılmamasını sağlaması gerekmektedir. Kontrolörün bu yükümlülüğü verinin toplandığı süre ile işlenmesi sırasında, kişisel verinin saklandığı ve veriye erişilebildiği müddetçe geçerlidir.

- ***Zorunlu Veri Koruma Görevlisi***

GDPR 37. Maddesine göre, "Kontrolör ve işleyici aşağıdaki durumlarda her halükarda bir veri koruma görevlisi belirler:

(a) işleme faaliyetinin kendi yargı yetkisi çerçevesinde hareket eden mahkemeler haricindeki bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi;
(b) kontrolör veya işleyicinin temel faaliyetlerinin yapıları, kapsamları ve/veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya
(c) kontrolör veya işleyicinin temel faaliyetlerinin 9 maddesi uyarınca özel kategorilerdeki verilerin ve 10. maddede atıfta bulunulan mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi."

Bu maddeden de anlaşılacağı üzere 9. maddede, "ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesinin yasaktır. Ancak istisnalara binaen işlenmesi halinde her halükarda veri işleyenin alanın yeterli uzmanlık bilgisi olan bir veri koruma görevlisi bulundurması zorunludur ve işleme faaliyetinden bu veri koruma görevlisi sorumludur."

GDPR'daki bu düzenlemeye göre, veri koruma görevlisinin iş akdiyle istihdam edilmesi de mümkün olduğu gibi veri koruma görevlisinin birden fazla şirket veya kamu kurumu adına çalışması da mümkündür.

- ***Riskli Veri İşleme Faaliyetleri Bakımından Zorunlu Veri Koruma Etki Değerlendirmesi***

GDPR'ın 35. maddesiyle özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hak ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde kontrolör, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapma zorunluluğu getirilmiştir.

Bu düzenlemede, özellikle yeni veri işleme teknolojisi ve metotlarının kullanıldığı veri işleme faaliyetlerinin, gerçek kişilerin hak ve özgürlükleri bakımından yüksek bir risk içermesinin muhtemel olduğu durumlarda, söz konusu işlemenin; kapsamı, niteliği, bağlamı ve amacı dikkate alınarak tüzük hükümlerine uyumun arttırılması amacıyla veri kontrolörü, öncelikle bir, Veri Koruma Etki Değerlendirmesi (VKED) yapılmasından sorumlu tutulmaktadır. Maddenin ikinci fıkrasında özellikle profil çıkarma dahil olmak üzere otomatik veri işleme sistemlerinin kullanılması, hassas verilerin işlenmesi veya ceza mahkûmiyeti ve suçlara ilişkin verilerin işlenmesi, kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi halinde VKED yapılması zorunludur.

Buradan da anlaşılacağı üzere, kişisel veri işleme faaliyetlerinin GDPR hükümlerine uygun olarak gerçekleştirilmesine yönelik alınacak önlemlerin belirlenmesinde söz konusu VKED sonuçlarının dikkate alınacağı ifade edilmektedir. VKED'nin özellikle büyük ölçekli işleme faaliyetlerinde gerekli olduğu vurgulanmaktadır.

Ayrıca bir VKED sonucunda, işleme faaliyetlerinin kontrolörün mevcut teknoloji ve uygulama maliyetleri açısından uygun tedbirlerle hafifletemeyeceği bir yüksek risk içerdiğinin ortaya çıkması durumunda, veri işleme faaliyetinden önce veri koruma otoritesine, Türkiye açısından denetim makamı olan Kişisel Verilerin Korunması Kurumuna danışılması gerekmektedir. Denetim makamı olan KVKK bir veri koruma etki değerlendirmesi gerekliliğine tabi olan veya olmayan işleme faaliyeti türlerine ilişkin bir liste oluşturur ve bu listeyi kamuya açıklar.

95/46 sayılı Direktif'te yer alan veri işleme faaliyetlerinin veri koruma otoritelerine bildirilmesine ilişkin genel hüküm, kişisel verilerin korunması konusunda köklü bir çözümü getirmediğinden yeni düzenleme ile ayrım gözetmeksizin tanımlanan bu genel bildirim yükümlülüğü yerine VKED'nin yapılmasının çok daha amaca uygun olacağı düşünülmektedir. VKED'de veri kontrolörü, yüksek risk olasılığını ve şiddetini değerlendirmeden önce işlemenin amaç ve kapsamı ile riskin kaynaklarını göz önünde bulundurabilecektir.

III- KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI

Sağlık verileri 6698 Sayılı Kanun kapsamında özel nitelikli kişisel verilerdir. Kanunun 6. maddesine göre,

> "(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.
>
> (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.
>
> (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.
>
> (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

Yine Kanunun 28. maddesinin (1) numaralı fıkrasının (ç) bendinde kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu, istihbari faaliyetler kapsamında işlenmesi halinde kanun hükümlerinin uygulanmayacağı düzenlenmiştir. Buradan da anlaşılacağı gibi salgın hastalıklar, koruyucu sağlık uygulamaları, doğal afetler, olağanüstü hal uygulamaları, kitle gösterileri ve benzeri nedenlerle kişisel sağlık verileri yalnızca bir kamu kurumu değil, birden fazla kamu kurum ve kuruluşu, kişisel sağlık verilerini kaydedip, işleyebileceği gibi kurumlar arası veri aktarımı da söz konusu olabilecektir.

Özel nitelikli kişisel verilerin işlenmesine ilişkin Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı ile "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" belirlenmiştir.[7] Bu önlemler şu şekilde sıralanmıştır:

[7] Bakınız: https://www.kvkk.gov.tr/Icerik/4110/2018-10.

“1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,

b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise,

a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,

b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

5- Özel nitelikli kişisel veriler aktarılacaksa

a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımının gerçekleştirilmesi,

ç) Verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır."

Özellikle sağlık verilerinin işlenmesinde 6698 sayılı Kanun'un 4. maddesinde belirtilen kişisel verilerin işlenmesinde sayılan genel (temel) ilkeler; "hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi" açıktır.

Bu konuda GDPR'ın özel (hassas) kategorilerdeki kişisel verilerin işlenmesi başlıklı 9. Maddesine göre,

g) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;

h) koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile

yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

i) özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

durumlarında hassas kategorideki kişisel verilerin işlenebilmesi, "gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler alınması" koşulu ile mümkündür.

Bu çerçevede, mevcut durum genel halk sağlığı, kamu güvenliğini ve kamu düzenini tehdit ettiğinden kişisel verilerin Sağlık Bakanlığı ve yukarıdaki madde kapsamına giren kamu kurum ve kuruluşları tarafından işlenmesinin önünde hukuki bir engel bulunmamaktadır. Ancak çeşitli aplikasyonlar ve uygulamalar vasıtasıyla Sağlık Bakanlığı gibi kamu kurum ve kuruluşlarının; sağlık verilerini toplamaları sırasında belirtilen teknik ve idari önlemleri almaları gerektiği, gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler alınması gerektiği gerçeğini ortadan kaldırmamaktadır.

IV- SALGIN SÜRECİNDE KİŞİSEL VERİLERİN KORUNMASI KURULU KARARLARI

Kişisel Verileri Koruma Kurumu (KVKK) tarafından pandemi sürecinde kişisel verilerin korunmasına ilişkin çeşitli tarihlerde aşağıdaki açıklamalar yapılmıştır:

- 27/03/2020 tarihli açıklamaya göre, "Bu istisnai zamanlarda dahi veri sorumluları ve veri işleyenlerin, ilgili kişilerin kişisel verilerinin güvenliğini sağlamaları gerekmektedir. Bu nedenle kişisel verilerin hukuka uygun olarak işlenmesi ve bu konuda alınan herhangi bir önlemin hukukun genel ilkelerine uygun olması, bu çerçevede kişilerin temel hak ve özgürlükleri açısından geri döndürülemez zararların ortaya çıkmaması önemlidir. Bu minvalde özellikle COVID-19 virüsüne karşı alınan önlemler kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri gerekli, amaçla bağlantılı, sınırlı ve ölçülü olmalıdır."[8]
- 07/04/2020 tarihli açıklamaya göre, "Uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin işlendiği görülmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanununun 5.inci maddesinde kişisel verilerin işlenme şartları, 6.ncı maddesinde ise biyometrik verilerin dâhil olduğu özel nitelikli kişisel verilerin işlenme şartları belirlenmiştir. Bu noktada, kişisel verilerin Kanunun 5.inci ve/veya 6.ncı maddesinde belirtilen şartlara uygun olarak işlenmesi gerekmektedir."[9]
- 09/04/2020 tarihli açıklamaya göre, "Kişilerin konum verilerinin sağlık durumlarıyla ilişkilendirilmek suretiyle işlenmesi sürecinde söz konusu verilerin üçüncü kişilerce ele geçirilmesi halinde ilgili kişiler bakımından ciddi zararlar ortaya çıkabileceği dikkate alınarak, ilgili kurum ve kuruluşların kişisel verilerin güvenliğini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri almaları ve bu verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde söz konusu kişisel verilerin silinmesi veya yok edilmesi unutulmamalıdır."[10]

---

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

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

[10] https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-?utm_campaign=DonanimHaber&utm_medium=referral&utm_source=DonanimHaber.

Görüleceği üzere, temas takip uygulamasının gerekli ve yeterli kontrollerden geçirilip geçirilmediği, özel (hassas) nitelikli veri olan sağlık verilerinin ve diğer kişisel verilerin korunması açısından KVKK gibi bu konuda yetkili kurumun denetimin geçirilip geçirilmediği konusunda kamuoyunu yeterince aydınlatıcı herhangi bir açıklama yapılmamıştır.

V- COVID-19 SÜRECİNDE TEMAS TAKİP UYGULAMALARI

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

Görünen o ki önümüzdeki aylar, hatta yıllar boyunca dijital izleme ve gözetim uygulamaları, yurttaşların dijital haklarını tehdit etmeye devam edecek. COVID-19'un yayılmasını kontrol etmeye yardımcı olacağı belirtilen orantısız teknolojik uygulamalar, hükümetlere ve teknoloji şirketlerine kişisel verilere erişim yetkisinde artışa neden olacak. Kişisel veriler, toplumsal alanda uygulanan güvenlik politikalarının doğal bir parçası haline gelecek.

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

Ocak ayından bu yana tüm dünyada mevcut olan kişi izleme uygulamalarının sayısında keskin bir artış olmuştur.[11] Bu uygulamaların, bireyleri ve temas ettikleri diğer bireyleri izlemek için konum verilerini kullanarak virüsün yayılmasını engellemeye yardımcı olmak amacıyla tasarlandığı iddia edilmiştir. Bu uygulamaları geliştirenlerin niyetleri iyi olsa da uygulamalar hem etkinlik hem de önemli oranda gizlilik endişelerini beraberinde getirmektedir. Birçok çalışmanın gösterdiği gibi, anonimleştirilmiş bazı veri setleri bile yeniden tanımlanma riski altındadır.[12] Ayrıca, açık gizlilik politikalarının bulunmaması ve merkezi veri depolamasının kullanılması, verilerin kötüye kullanıma karşı savunmasız olma olasılığını artıracaktır.

---

[11] Bu konuda hazırladığımız şu kitapçığa bakılabilir: Çayır, F. (2020). COVID-19 Sürecinde Temas Takip Uygulamaları ve Kişisel Verilerin Korunması. Ankara: Alternatif Bilişim Derneği. https://ekitap.alternatifbilisim.org/covid-19-temas-takip-uygulamalari/.

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

VI- KONUM VERİLERİ HAKKINDA[13]

Konum verileri, bir cihazın temel işlevlerinin parçası olarak cep telefonu operatörleri ve işletim sistemleri ile kullanıcılara dönük bir özellik olan mobil uygulamalar tarafından, aktif olarak bir ağa bağlı olmasalar bile izlenmelerine olanak tanıyan ve tanımlayıcı bilgiler yayan akıllı eşya veya oyuncaklar gibi "Nesnelerin İnterneti" (IoT) cihazları tarafından tutulabilmektedir. Devletler tarafından çeşitli vasıtalar ile bireylerin konum verilerine, yasal olarak yetki verilmiş kurum ve kuruluşlarca, gerek yasal gerekse yasal olmayan yöntemler ile erişilebilmektedir.[14] Ancak pandemi süreci kurum ve kuruluşların bu acil ve olağanüstü durumu bahane ederek ve fırsat bilerek hiçbir engel ile karşılaşmaksızın ve herhangi bir açıklama yapmaksızın, konum verilerini süresiz saklama ve kullanma yetkisine dönüşebilir.

Konum verileri veya hareketlilik verileri, cihaz ve kişilerin zaman içinde boşluklarda nasıl hareket ettikleri hakkında bilgiler içerir. En temel anlamda; bir cihazın bağlanabilirlik özelliği veya cihazlarda kablosuz içerik gönderme ve alma yeteneği, bu cihazların bulunduğu yer hakkında bilgi içermektedir. Örneğin, kablosuz servis sağlayıcıları, cihazları yerel baz istasyonları ve ağlar üzerinden sağladıkları için cihazların nerede bulunduğunu bilirler. Daha genel bir düzeyde, bir IP adresi (internet trafiği göndermek ve almak için cihazlar tarafından serbestçe ve açıkça paylaşılan bir tanımlayıcı) genellikle bir kişinin şehrini ve konumunu bilmek için yeterlidir.

Çoğu zaman konum verileri denildiğinde, GPS'i (Global Positioning System - Küresel Konumlandırma Sistemi) düşünülür. Ancak sadece GPS değil; işletim sistemleri, telefon operatörleri, uygulamalar ve diğer ağa bağlı cihazlar tarafından da kullanılan cihazların bulunduğu yerleri çıkarmanın birçok yolundan sadece biridir.

GPS, dünya üzerinde herhangi engelsiz bir görüş hattında, dört veya daha fazla uydusu ile her türlü hava koşulunda yer ve zaman bilgileri sağlayan uzay tabanlı uydu navigasyon sistemidir.[15] Akıllı telefonlar ve diğer cihazlar, herhangi bir telefon veya internet alımından bağımsız olarak GPS üzerinden konumu algılayabilir.

Baz istasyonları kullanıcılara ağ erişimi sağlarlar. Her bir istasyon eşsiz bir numaraya sahiptir. Cep telefonları kendilerine yakın istasyonlardan birine bağlanır.

---

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

[14] Türkiye'de Elektronik Haberleşme Kanunu'nun 51. Maddesine göre, trafik ve konum verileri telefon operatörleri tarafından işlenebilmektedir.

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

Bu aynı zamanda mobil operatörlerin konumumuzu yaklaşık olarak bilebilmesi anlamına gelir. Ayrıca, "Historical Traffic Search" (HTS) kayıtları olarak bilinen veride kişilerin telefonlarıyla gerçekleştirdikleri görüşmelerin arayan, aranan; arama zamanı, arama süresi, arama yeri ve sinyal alınan baz istasyonları gibi bilgileri yer alır.

Wi-Fi ağlarına bağlanma durumunda ise mobil cihazlar, yakındaki Wi-Fi ağlarını tarayarak konumlarını belirleyebilir. Yakındaki ağlar veya "erişim noktaları", örneğin komşuların Wi-Fi'ını veya kafe ve mağazalarda bulunan Wi-Fi'ı içerebilir. Bu ağlarda kablosuz yönlendiricilerin ve bilinen konumlarının benzersiz tanımlayıcıları (MAC adresleri ve SSID) büyük veritabanları mevcuttur.

Bluetooth'un kullanımındaysa, birçok uygulama, tek yönlü Bluetooth sinyalleri yayınlayan küçük radyo vericileri olan "donanımlara" olan yakınlıklarını algılamak için tasarlanmıştır. Kullanıcının Bluetooth'a erişim izni verdiği bir uygulama cihazın konumunu çıkarabilir veya yakınlığa dayalı uyarılar veya başka içerikler gönderebilir.

Her bir konum verisi elde etme yöntemi farklı bir hassasiyet seviyesi gerektirir ve farklı amaçlar için kullanılabilir. Birçok hükümet ve devlet kurumu, nüfus düzeyindeki eğilimleri ve hareketleri gözlemlemek için "anonim" veya "anonim ve toplu" konum verilerine erişmekle ilgilenmektedir. Bazı durumlarda verileri anonim hale getirmek mümkün olsa da, her bir kesin konum verisi ve veri kümesini gerçekten "anonim" hale getirmek çok zordur. İsimler yerine benzersiz tanımlayıcılar kullanılsa bile, çoğu insanın davranışları, örneğin evlerinin konumundan (cihazın açık olup olmadığı, saat kaçta açıldığı vb. bilgiler) kolayca izlenebilir. Her ne kadar konum verileri açısından benzersiz kimlik tanımlayıcı işaretler kullanılsa bile; konum verisi ile birkaç bilgi yan yana geldiğinde kişi ya da grupların kimliği rahatlıkla açığa çıkarılabilir.[16]

Bu konuda yapılan bir araştırmaya göre, basitçe anonimleştirilmiş bir veri kümesi, ad, ev adresi, telefon numarası veya diğer belirgin tanımlayıcıları içermez. Ancak, bireyin kalıpları yeterince benzersizse, verileri bir bireye geri bağlamak için dış bilgiler kullanılabilir.[17] Örneğin, benzersiz kimlik tanımlayıcı ile anonim hale dönüştürüldüğü varsayılan bir tıbbi veri tabanına ulaşabilecek kötü niyetli bir kişi, farklı bir kişinin sağlık kaydını bulmak için, konum verileri ve halka açık bir seçmen

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

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

kaydı listesi ile tıbbi veri tabanı birleştirerek istediği kişiyi başarıyla tanımlanabilir hale dönüştürebilir.

Verileri anonimleştirmeye ilişkin bu tarz zorlukların üstesinden gelmek çok zordur, ancak politika yapıcılar konuya ilişkin olarak gerek kamu erkine gerekse platform kapitalizmine aşırı ödün vermemeye çok dikkat etmeli ve konum veri kümelerini özel ve hassas veri olarak ele almalıdır.[18] Konum verilerine kimin erişebileceğini, hangi amaçlarla kullanılabileceğini öngörerek ve veri kaydının sınırlı kalmasını sağlayarak; konum verileri hakkında idari, teknik ve yasal denetimlerin arttırılması gerekmektedir. Bu konuda özellikle sivil toplum kuruluşlarının da politika yapımında etkin söz sahibi olmasına önem verilmelidir. Türkiye'de gerek kişisel verilerin korunması, konum verilerinin işaretlenmesi ve kullanılması hususunda ne yazık ki ilgili sivil toplum kuruluşlarının kamusal politika yapımına katılması için kamu erki alan açmamaktadır.

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

VII- ULUSLARASI KURULUŞLARIN TEMAS TAKİP UYGULAMALARINDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN AÇIKLAMALARI

BM Özel Raportörleri, devletlerin insan haklarını bastırmak için acil durum önlemlerini kötüye kullanmamaları konusunda açıklama yaparak, "Mevcut sağlık krizinin ciddiyetini kabul etsek ve önemli tehditlere karşılık uluslararası hukuk tarafından acil durum yetkilerinin kullanılmasına izin verildiğini kabul etsek de, Devletlere, koronavirüse yönelik acil durum müdahalelerinin orantılı, gerekli ve ayrımcı olmayan olması gerektiğini acilen hatırlatıyoruz"[19] demiştir.

BM/DESA (Ekonomik ve Sosyal İşler Dairesi Başkanlığı), hükümetleri sağlık krizi hakkında şeffaf davranarak bilgi paylaşmaya çağırarak; kamuoyu dâhil olmak üzere çeşitli paydaşları salgının yönetimine dâhil etmek; kamu-özel sektör ortaklıkları için uygun gizlilik önlemleri ile paydaş ortaklıkları ve yenilikçi dijital teknolojilerin uygulanmasını hızlandırmaya yönelik bir açıklama yayınladı.[20]

Avrupa Komisyonu, "Temas İzleme Uygulamaları Hakkında Tavsiye Metni" ile bir dizi öneride bulunmuştur. İlgili tavsiye metninde temas takip uygulamalarının kullanımı için koordineli bir yaklaşım önerilerek, anonim ve toplu mobil konum verileri yoluyla virüsün yayılmasını tahmin etmek ve modellemek için; temel ilkelere saygı ve bireylerin damgalanmaması, en az müdahaleci ama etkili araçların tercih edilmesi, teknik güvencelerin ortaya konulması, siber güvenlik önlemlerinin alınması, pandemi kontrolü sona erdiğinde alınan bu önlemlerin sona erdirilmesi, yakınlık verilerine dayanan anonim analiz ve uyarı sistemlerinin tercih edilmesi ve uygulamaların gizlilik ayarlarıyla ilgili şeffaflık sağlanması gibi tavsiyeler yer almaktadır.[21]

Avrupa Komisyonu sağlık verilerinin kullanımına ilişkin, "eHealth Network" metni yayınlayarak, AB'nin COVID-19 ile mücadelesinde izlemeyi destekleyen mobil uygulamalarda şu hususlara dikkat edilmesi önerilmiştir: Kişi izleme ve uyarı rolünün değerlendirilmesi, mevcut girişimlerin envanteri ve ulusal ölçekte kişi takibi için temel gerekliliklerin detaylandırılması, uygulamaların gönüllü, ulusal

---

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

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

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

sağlık otoritesi tarafından onaylı, kişisel verilerin güvenli bir şekilde şifrelenmesi ve gerekli olmadığı anda kaldırılması gerektiği.[22]

Avrupa Komisyonu'nun, "Veri Koruma ile İlişkili COVID-19 Salgınına Karşı Mücadeleyi Destekleyen Uygulamalar Rehberi" de geliştirilen uygulamaların AB gizliliği ve veri koruma mevzuatına, özellikle GDPR[23] ve eGizlilik Direktifine uyumu sağlamak için yerine getirmesi gereken özellikleri ve gereksinimleri açıklar.[24]

Avrupa Birliği Avrupa Veri Koruma Kurulu (EDPB), "COVID-19 Pandemisine Karşı Mücadeleyi Destekleyen Uygulamalara İlişkin Kılavuz Taslağı" yayınlayarak; Avrupa Birliği devletlerinin veri koruma otoritelerini danışmaya davet etmiş ve hesap verebilir bir şekilde uygulamalar geliştirmesini, tasarımsal ve varsayılan özellik olarak gizliliği temel alan, açık kaynak kodlu, kriz bittikten ve herhangi bir veri silindikten veya anonimleştirildikten sonra sistemin acil durumlarda dahi kullanılmaması, gönüllü, güvenli ve birlikte çalışabilir olmaları da dâhil olmak üzere kişi izleme uygulamaları için belirli önlemlerin teşvik edilmesi gerektiğini belirtmiştir. Devletlerin bu tür uygulamalar için yasal bir dayanak oluşturan ulusal yasaları yürürlüğe koymalarını, bireysel kullanıcıların konum takibinin gerekli olmadığı, sağlık yetkilileri ve bilim insanlarının bu uygulamaların temel fonksiyonel gereksinimlerini tanımlamak için sıkı bir zorunluluk testi geliştirmeleri gereğinin altı çizilmiştir. Merkezi olmayan uygulamaların daha fazla kullanılması gerektiğinin, minimum veri kaydına paralel olarak ve kişilerin sağlık otoriteleri tarafından test sonrası temaslarının tam otomatik olmayan yollarla sınırlandırılmasının, verilerin geri kullanılmaması ve zamanında silinmesinin, alınan önlemler ile uygulamayı kullananların temas kişilerinin yeniden tanımlanmasını önlenmesi gerektiğinin de altı çizilmiştir.[25]

EDPB'nin, "COVID-19 Salgını Bağlamında Kişisel Verilerin İşlenmesi Hakkında Bildiri" metni ise konum verilerinin kullanımı, istihdam, temel ilkeler ve işlemenin yasallığı hakkında kapsamlı bir kitapçıktır.[26]

---

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

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

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

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

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

AB Temel Haklar Ajansı'nın, "AB'deki Coronavirus Salgınında Temel Haklara İlişkin Bülteni"nin 4. bölümünde ise işveren ile medya kurumlarının veri koruma yetkilileri tarafından pandemi sırasında gizlilik ve veri koruma haklarının nasıl sağlanacağına ilişkin bilgiler verilmekte, özellikle veri işleme ana hatlarıyla açıklanmaktadır.[27]

Avrupa Komisyonu Başkanı Ursula von der Leyen ve Avrupa Konseyi Başkanı Charles Michel, 15 Nisan'da COVID-19 sınırlama önlemlerini kaldırmaya yönelik ortak bir "Avrupa Yol Haritası" imzaladı.[28] Ortak deklarasyona göre veri gizliliğine saygı gösteren mobil uygulamaların kullanımı ile kişi takip ve uyarı uygulaması için bir çerçeve oluşturmak amaçlanmıştır. Enfeksiyon zincirlerini kesintiye uğratmaya ve daha fazla bulaşma riskini azaltmaya yardımcı olabildikleri için temas takip uygulamaları artan test kapasiteleri de dâhil olmak üzere diğer önlemleri tamamladıkları sürece üye devletlerin oluşturduğu stratejilerde önemli bir unsurdur. Mobil uygulamaların gönüllü olmaları ve ulusal sağlık otoritelerinin sistem tasarımına dahil edilmesi önerilmektedir. Önerilen güvenceler ise verilerin anonimleştirilmesi ve toplanması, kullanıcıların izlenmesi ve yönetişim korumaları gibi bir dizi teknik güvencelerin bir karışımıdır. COVID-19 krizi sona erdiğinde şeffaf ve sona erme süresi belirli olan uygulama ile kaydedilen verilerin silinmesi ve uygulamaların devre dışı bırakılması gereklidir. Belgeye göre, bu uygulamalara duyulan güven ve gizlilik ve veri korumaya saygıları, başarıları ve etkililikleri için çok önemlidir.

Derneğimizin de üye olduğu, EDRI'nin (Avrupa Dijital Haklar Örgütü) yapmış olduğu açıklamaya göre,

"Devletler pandemi ile mücadelede dijital gözetim teknolojilerini kullanırken insan haklarına saygı göstermelidir. Üzerinde anlaşmaya varılmamış dijital gözetim gücündeki bir artış cep telefonu konum verilerine erişim elde etmek, gizliliği, ifade özgürlüğünü ve örgütlenme özgürlüğü haklarını ihlal edebilecek ve kamu makamlarına olan güveni azaltabilecek şekilde tehdit edebileceği gibi herhangi bir halk sağlığı müdahalesinin etkinliğini de baltalayabilir. Bu önlemler aynı zamanda ayrımcılık riski taşır ve zaten ötekileştirilmiş topluluklara orantısız bir şekilde zarar verebilir."[29]

---

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

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

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

Access Now, COVID-19 kişi izleme uygulamalarının kullanımında gizlilik ve halk sağlığı için yapılması ve yapılmaması gerekenlere dair bir dizi öneri hazırlamıştır.[30] CCC (Chaos Computer Club) tarafından yapılan açıklama ile kişi izleme uygulamalarına ilişkin asgari 10 gereksinim sıralanmış ve Prensip olarak bir "Corona Uygulaması" kavramı, toplanabilecek temas ve sağlık verileri nedeniyle büyük bir risk içerir. Aynı zamanda son yıllarda kripto ve gizlilik toplulukları tarafından geliştirilen "tasarım gereği gizlilik" ilkesine bağlı kalarak bu teknolojilerin yardımıyla, bir gizlilik felaketi yaratmadan temas takip uygulamalarının potansiyelini ortaya çıkarmak da mümkündür. Sadece bu nedenle, "mahremiyeti ihlal eden ve hatta tehlikeye atan tüm kavramların kesinlikle reddedilmesi" gerektiği belirtilmiştir.[31] Privacy International tarafından farklı ülkeler tarafından uygulanan COVID-19 uygulamalarına ilişkin bir bilgilendirme listesi hazırlanmaya başlanmıştır.[32] Privacy International tarafından yapılan açıklamaya göre, "Bu tür uygulamaların başlangıç noktası yalnızca sağlığa yardımcı olmaktır. Uygulamalar pandemiye mücadelede halk sağlığını korumanın küçük bir parçasıdır. Herhangi bir önlem insana öncelik vermeli ve verileri en aza indirmelidir. İnsanların, verilerinin ve cihazlarının güvenli olduğuna emin olmaları ve bu küresel salgının sonunda verilerin yok edilmesi gereklidir."[33]

Avrupa Özgür Yazılım Vakfı'nın (FSFE) açıklamasına göre, "Özgür Yazılımlar, eksiksiz bir veri korumasını ve uyumlu bir kullanımı doğrulamak için yeterli şeffaflık sunar, böylece güvenli bir sistem kurulabilir. Güvenli bir ortamda küresel kod geliştirme iş birliğini mümkün kılan yalnızca Özgür Yazılımlardır. Herhangi bir sahipli çözüm kaçınılmaz olarak sayısız izole edilmiş veri sızıntısına yol açacak ve böylece enerji ve zaman israfına neden olacaktır. Özgür Yazılım lisansları evrensel bir iş birliğinin yanı sıra herhangi bir yetki alanında yazılım kodlarının paylaşılmasına izin verir".[34] Electronic Frontier Foundation (EFF) tarafından yapılan açıklamaya göre, "EFF uzun zamandır hükümetlerin ve şirketlerin konum verileri, sağlık verileri ve kişisel ilişkilerimizin dijital gözetimine karşı ve büyük veri sistemlerinin hayatımızı açık kitaplara dönüştürmesine karşı mücadele ediyor. Bu tür veri işleme genellikle gizliliğimizi ihlal eder, özgür konuşmamızı ve ilişkilendirmemizi engeller ve azınlıklara farklı yükler getirir. Halk sağlığı yetkilileri COVID-19'u içermek için

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

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

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

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

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

çalışırken büyük verilerin bir miktar kullanımı garanti edilebilir. Ancak, halk sağlığı uzmanları tarafından belirlendiği üzere tıbbi olarak gerekli olmalıdır; kişisel verilerin işlenmesi gerçek yeni ihtiyaçlar ile orantılı olmalıdır. İnsanlar uyrukları veya diğer demografik faktörler nedeniyle incelenmemelidir ve herhangi bir yeni hükümet yetkisinin, hastalık bulunduğunda sona ermesi gerekir."[35]

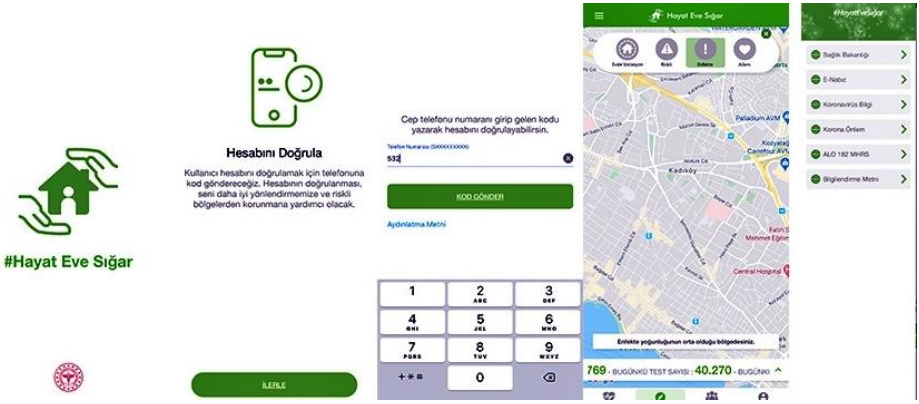
[35] https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis.

VIII- TÜRKİYE'DEKİ HAYAT EVE SIĞAR PANDEMİ TEMAS TAKİP UYGULAMASI

Sağlık Bakanlığı, COVID-19 pandemisi nedeniyle üç farklı uygulamayı yaşama geçirdi. Bu uygulamalardan Korona Virüs Kontrolü Uygulaması (19 Mart 2020) ve Pandemi İzolasyon Takip Projesi (09 Nisan 2020) uygulamaları; Hayat Eve Sığar (18 Nisan 2020) uygulaması adı altında birleştirildi. Hayat Eve Sığar uygulaması 4 Haziran 2020 tarihinden itibaren kullanıma açılan şehirlerarası ulaşım hizmetlerinde kullanılmak üzere HES (Hayat Eve Sığar) Kodu eklenmiştir.

Hayat Eve Sığar uygulaması Sağlık Bakanlığı'nın, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve GSM operatörleri (Türkcell, Türk Telekom, Vodafone) iş birliğiyle yaşama geçirdiği bir uygulamadır. Cep telefonu abonelerinin konum verilerine göre bulundukları konumu değiştirip, değiştirmedikleri izlenmektedir.

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



Uygulama;

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

Uygulama;

- Evde izolasyon altında bulunması gereken kişilerin, evlerini terk ettiğinde kısa mesaj servisi aracılığıyla uyarılması,

- Bu kişilerle anında iletişime geçilerek, izolasyon altında bulunmaları gereken yere dönmelerinin istenmesi,
- Yapılan uyarıya uymayan ve ihlale devam edenlerin durumlarının ilgili emniyet birimleriyle paylaşılarak gerekli idari önlem ve yaptırımların uygulanması,
- Yol kontrolü yapan emniyet ekiplerinin, kişinin bilgilerini sorgulayarak izolasyon ihlali yapıp yapmadığını öğrenebilmesi şeklinde gerçekleşmektedir.

Uygulama içeriğinde;

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

HES Kodu Uygulaması

HES kodu, Covid-19 pandemi sürecinde tüm vatandaşlar açısından iç hat uçuşlarda, tren ve otobüs yolculukları için zorunlu hale getirilmiştir. HES aplikasyonuna eklenen HES kodu denilen QR kodu, Hayat Eve Sığar aplikasyonu, e-devlet üzerinden ya da SMS yöntemi ile alınabilir.

HES kodunu uygulama üzerinden almak için: Hayat Eve Sığar uygulaması üzerinden “HES Kodu İşlemleri” bölümüne girilir. “HES Kodu Oluştur” butonuna tıklanır. Kod kullanım süresi seçilir ve kod oluşturulur.

HES Kodunu e-devlet üzerinden almak için: e-devlet şifresi ile giriş yapılıp HES kodu bölümünden; üretme, silme, sorgulama ve detaylarını görüntüleme işlemleri yapılabilir.

HES kodunu SMS ile almak için: HES yazıp aralarında boşluk bırakılarak sırasıyla T.C. Kimlik Numarası, T.C. Kimlik Seri Numarasının son 4 hanesi ve paylaşım süresi (gün sayısı olarak) yazılır ve 2023’e SMS olarak atılır.

Üretilen HES kodları kurum ya da kişilerle doğrudan veya mobil uygulama üzerinden paylaşılabilir. Kurum ya da kişiler, paylaştığınız HES kodlarını sorgulayarak Covid-19 açısından herhangi bir risk taşıyıp taşımadığınızı sorgulayabilirler. Aynı şekilde kullanıcılar paylaşılan HES kodlarını uygulama üzerinden sorgulayıp kişilerin risk durumlarını görebilir.

HES kodu alındıktan sonra seyahat edilecek seyahat firması ile HES kodunun paylaşılması gerekmektedir. Paylaşılan firma ya da kurum HES kodu ile kişinin sağlık durumunu sorgular. Paylaşılan HES kodları üzerinden tüm yolcuların Covid-19 riski taşıyıp taşımadığı sorgulanabilecek ve riskli kişilerin seyahati engellenebilecektir.

HES kodu belirli bir süre boyunca geçerlidir. HES kodunun seyahat bitiş tarihinden itibaren en az 7 gün daha geçerli olması, seyahat firmaları tarafından istenilmekte, aksi durumda rezervasyonlar onaylanmamaktadır.

Uygulamanın Aydınlatma Metnine göre[36],

Veri Sorumlusunun Kimliği; Bu uygulamada işlenen kişisel veriler bakımından veri sorumlusu T.C. Sağlık Bakanlığıdır.

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

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

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

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

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

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

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

Kişisel Verilerin Aktarımı: İzolasyon altında bulunmanız gereken bölgeyi terk etmeniz halinde bu uygulama ile elde edilen kimlik, iletişim ve konum verileriniz, kamu sağlığının korunması ve salgının yayılmasını önleme amaçlarıyla İçişleri Bakanlığı ve kolluk kuvvetleri ile paylaşılmaktadır.

IX- HAYAT EVE SIĞAR UYGULAMASININ KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN İNCELENMESİ VE ÖNERİLER

Temas takip uygulamaları toplanabilecek konum ve sağlık verileri nedeniyle büyük bir risk içermektedir. Tek başına konum verilerinin dahi üç ya da daha fazla veri ile eşleştirilmesi halinde kişilerin ya da toplulukların kimliğinin açığa çıkarılabileceği unutulmamalıdır. Ancak bazı asgari teknolojiler ve ilkeler göz önüne alınarak bir gizlilik ya da kişisel veri sızıntısı felaketine yol açmadan temas takip uygulamalarının geliştirilmesi de mümkündür. Bu anlamda teknik olarak önerilen ve uluslararası bazı metinlerden belirtilen ilkelerden aşağıda bahsedeceğiz. Bu ilkeler ve öneriler gerek Avrupa Komisyonu tarafından yayınlanan Sağlık Verilerinin Kullanımına İlişkin eHealth Network Metni, EDPB'nin COVID-19 Pandemisine Karşı Mücadeleyi Destekleyen Uygulamalara İlişkin Kılavuz Taslağı gibi resmi metinlerde ve gerekse de EFF, EDRI, CCC gibi sivil toplum kuruluşlarının metinlerinde yer almıştır. İlgili metinler baz alınarak, buradaki tartışmalar geliştirilmiştir.

1. Anlam ve Amaç:

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

2. Gönüllülük ve Onay:

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

saygı duyan güvenilir bir teknolojiye dayalı şekilde gönüllü olarak kullanılması ile mümkündür.

3. Şeffaflık:

Temas ve konum izleme uygulamalarının, düzenli olarak kullanıcıların uygulamadaki etkinlikleri hakkında kullanıcıları bilgilendirmesi gereklidir. Uygulamalar sağlam güvenlik programları ile şifrelenmeli, üçüncü taraf denetimleri ve sızma testlerini içermelidir. Devletler ve hükümetler, uygulamaya ilişkin politikalarını ve eğitim materyallerini yayınlamalı, aynı zamanda her bir temas izleme programının kullanımı ile ilgili istatistikleri ve diğer bilgileri mümkün olan en ayrıntılı şekilde, düzenli olarak yayınlamalıdır. Uygulamalar teknik güvenlik açısından, teknoloji ve gizlilik konusunda bilgili, bu alanda çalışan odalar ve sivil toplum örgütleri ile bağımsız denetçiler tarafından test edilmiş ve belgelendirilmiş olmalıdır. Her bir programın etkinliği ve kötüye kullanımı konusunda bağımsız uzmanlar tarafından yapılan denetim sonuçlarını düzenli olarak yürütülmeli ve yayınlamalıdır.

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

4. Önyargı ve Ayrımcılığa Maruz Kalmama:

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

5. Veri Minimizasyonu:

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

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

6. Kullanım Süresi ve Kaydedilen Verilerin Kullanımının Sınırlanması:

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

7. Kullanıcı Verilerini Kaydeden Merkezi Sistemlerin Kullanılması:

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

Google, Apple gibi şirketler de dahil olmak üzere hiçbir merkezi otoriteye güvenilmemelidir. Temas takip ve irtibat uygulamalarının şeffaflığı ve geliştirilebilirliği açısından Özgür Yazılım (Free Software) olması gereklidir. Özgür Yazılımlar, eksiksiz bir veri koruması ve uyumlu bir kullanımı doğrulamak için yeterli şeffaflık sunar. Böylece güvenli bir sistem kurulabilir. Güvenli bir ortamda küresel kod geliştirme iş birliği Özgür Yazılım vasıtasıyla mümkün kılınabilir. Herhangi bir şirket ya da merkezi otorite tarafından sunulan çözüm önerileri kaçınılmaz olarak sayısız veri sızıntısına yol açacaktır. Özgür Yazılım lisansları evrensel bir iş birliğinin yanı sıra herhangi bir yetki alanında yazılım kodlarının paylaşılmasına da izin verir.[37] Böylelikle bir ülkede geliştirilen çözümler başka bir ülkede yeniden kullanılabilir, benimsenebilir. Böylece kolektif bir yapı ortaya çıkacaktır.

8. Gizlilik İlkesine Göre Tasarım:

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

9. Anonimlik:

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

Ayrıca kullanıcılar için her ne kadar benzersiz kullanıcı kimlikleri oluşturulduğu belirtilse de bu durum tam olarak ve her zaman anonimliğin sağlandığı anlamına gelmez.

---

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

Anonimlik kavramı, verilerinizin hiçbir zaman bir kişi ile ilişkilendirilecek şekilde geri döndürülememesi anlamına gelmektedir. Uygulama ve sistemler tarafından atanmış olan kullanıcı kimlikleri ile diğer verileriniz eşleştiğinde, verilerinizi takma adlı veri haline dönüşür, yani tam anlamıyla anonim hale gelmez. Herhangi bir kişisel veri toplamadan veya kullanıcı kimliği türetmeden de temas takip uygulaması kullanmak mümkündür. Bu nedenle de merkezi sistemler tarafından kullanıcılar için kimlikler türetmek uygun değildir.

X- HAYAT EVE SIĞAR UYGULAMASINA ASGARİ GİZLİLİK İLKELERİ VE TEKNOLJİLERİ AÇISINDAN BAKIŞ

Sağlık Bakanlığı tarafından COVID-19 pandemisi nedeniyle uygulamaya konan *Hayat Eve Sığar* (18 Nisan 2020) uygulaması 10 milyondan fazla kişi tarafından mobil cihazlara yüklenmiştir.

Hayat Eve Sığar Uygulaması;

Bluetooth, GPS ve GSM operatörlerinden (Turkcell, Türk Telekom, Vodafone) alınan baz istasyonu bilgilerini kullanmaktadır. Bu uygulama ile T.C. Kimlik Numarası, baba adı ve doğum tarihi bilgileri, konum verileri, MERNİS adres bilgileri, sağlık verileri, telefon numarası bilgileri işlenmektedir. Bu uygulama yüklendiğinde telefonu vasıtasıyla iletişim (baz istasyonu) verileri, rehberde kayıtlı kişiler, kamera, fotoğraf ve video, konum, yaklaşık konum (ağ tabanlı), kesin konum bilgileri (GPS ve Ağ Tabanlı), kablosuz bağlantı bilgileri, tam ağ erişimi bilgileri, Bluetooth cihazlarla eşleşme ve Bluetooth ayarları, ağ bağlantıları, Google hizmet yapılandırması bilgilerine erişebilir. Kişisel veriler Sağlık Bakanlığı tarafından işlenmekte olup, veri sorumlusu Sağlık Bakanlığı'dır. Ayrıca İçişleri Bakanlığı ve kolluk kuvvetleri ile de veriler paylaşılmakta olup, veri paylaşımı yapılan tüm bu kurumlar da aynı zamanda veri sorumlusudur. Dolayısıyla verilerin toplanması ve eşleştirilmesinde merkezi sistem benimsenmiş, hatta birden fazla merkezi veri tabanı ile veri alış-verişi yapılmasına izin verilmiştir. Uygulama aracılığıyla veri minimizasyonuna aykırı olarak halk sağlığı amacıyla alakalı olmayan birçok kişisel veri toplanmakta ve işlenmektedir.

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

Kullanımının COVID-19 testi pozitif ve tanı konulan kişiler ve tanı konulanlarla yakın teması olanlar kişiler açısından zorunlu olduğu Sağlık Bakanlığı tarafından açıklanmıştır. Ayrıca teşhis ve tanı konulmayan kişiler tarafından uygulamanın Google Play veya Apple mağazalarından indirilmesi mümkündür. Uygulamanın kurulum aşamasında ilk istenilen telefon numarası verisinin Sağlık Bakanlığı paylaşılması ile birlikte uygulama, telefon operatörü bilgilerinize ulaşacağından ad, soyad, adres ve diğer abonelik bilgilerine onay vermemiş olsanız dahi erişecektir. Dolayısıyla uygulama etik olarak tasarım gereği gizlilik ilkesine uygun olmadığı gibi, kullanıcıların üçüncü kişiler tarafından belirlenebilirliği açısından her kullanıcıya anonim veya geçici bir kimlik türetip türetmediğinin tespiti mümkün değildir.

En son eklenen HES kodu ile birlikte kullanıcıların sağlık verileri özel seyahat firmaları ile paylaşılmaktadır. Hatta kullanıcılar sağlık verilerini özel kişiler ile de paylaşabilmektedir. Uygulamaya eklenen HES kodu ile kişilere ait hassas (özel) nitelikteki sağlık verilerinin paylaşılması veri minimizasyonu ilkesine aykırı olup, uygulamanın açıklanan anlam ve amacı ile çelişmektedir.

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

XI- SONUÇ

Akıllı telefonlara sahip milyarlarca insanın genellikle bu cihazlarda işletim sistemleri ve çeşitli uygulamalar kullandığını düşünürsek, insanlara ulaşmak ve cihazlarından kapsamlı veriler çekmek mümkündür. Akıllı telefonların hâlihazırdaki donanımları (chip, işlemci ve antenler) ile işletim sistemleri (genellikle Apple iOS ve Google Android), uygulama mağazaları (Apple App Store ve Google Play), platformlar (analiz şirketleri ve sosyal medya şirketleri) ve uygulamalar tarafından enformasyonel kapitalizminin ve platform ekonomisinin veriye değer katma politikası gereği sürekli bir izleme ve gözetim hali hazırda uygulanmaktadır. Facebook, Google, Apple vb. büyük teknoloji şirketleri ile analiz şirketleri yıllardır çok ayrıntılı ve toplu olarak konum verilerini biriktirmektedir. Platformlar için tüm veriler ticari değer taşımakta ve platform ekonomisinin temel kaynağını üreterek değer yaratmaktadır. Devletler istedikleri takdirde Google ve Apple'dan, WeChat'ten konum verilerini elde etmektedir. Verileştirilmiş bir toplumsal ekonomik ve siyasal yaşama doğru hızla ilerliyoruz.

Anlık veri takibi yapılabilen, teknik olarak desteklenen "temas takip" uygulamaları hızlı ve etkili çözüm üretmek amacıyla COVID-19 virüsünün yayılmasını önlemeye yönelik bir araç olarak düşünülmektedir. Bu uygulamaların enfeksiyon zincirlerinin hızlı izlenmesi ve virüs etkileşiminin kesilmesine olanak sağlayacağı düşünülmektedir. Genel olarak bu uygulamalar enfekte olmuş kişilerin ve temas ettiği kişilerin daha hızlı uyarılmasına, böylece kendilerini daha hızlı karantinaya alabilmelerine olanak sağlayabilir. Bu durum ise enfeksiyonun yayılmasını önleyebilir niteliktedir. Ancak bu durumda dahi herhangi bir korona temas izleme uygulaması ne kendimizi ne de temas ettiğimiz kişileri korumaya yönelik değildir. Önemle belirtmek gerekir ki, bu uygulamaların kullanılması ne COVID-19 pandemisinin sona ermesini ne de küresel ölçekte yaşanan halk sağlığı krizine çözüm üretilmesini sağlamayacaktır. Bu uygulamalar hükümetler tarafından gerekli sosyal güvenlik önlemleri alınmadan ve yeterli sağlık olanakları eşit olarak sağlanmadan, yurttaşların işlerini kaybetme gibi ekonomik kaygılar ortadan kaldırılmadan; pandeminin sona erdirilmesini sağlamaz. Dolayısıyla asıl bu toplumsal ve ekonomik önlemler alınmadan, yalnızca teknolojik çözümler ve uygulamalar vasıtası ile halk sağlığı krizine çözüm üretilebilmesi mümkün değildir. Dolayısıyla, teknolojik çözümleri kamu erki nasıl yaşama hızla geçiriyorsa, asıl olan toplumsal ve ekonomik önlemleri adil, şeffaf ve hesap verebilir şekilde yaşama sokmasıdır. Bu nedenle, teknolojik çözümlerin siyasi karar/irade olduğunu bir kere daha somutlar.

Bu anlamda teknolojik önlemler ve temas takip uygulamaları açısından hükümetler tarafından belirtilen önlemlere ve vaatlere güvenmek yeterli değildir. Temas

izleme uygulamaları hükümetlerin büyük bir gözetim yetkisine sahip olmasını sağlayacağı gibi; kişilerin sağlık, cinsiyet, yaş, dil, din, ırk, etnik köken, milliyet, göçmenlik statüsü veya engellilik gibi hassas verileri işlendiğinden toplumda ciddi bir önyargı ve ayrımcılık yaratma riski taşır. Uluslararası sözleşmeler ve T.C. Anayasası ile tanınan temel hak ve hürriyetlere ilişkin güvenceler halk sağlığı gerekçe gösterilerek bertaraf edilmemelidir. Özel hayatın gizliliği, kişisel verilerin korunması ve ifade özgürlüğü gibi hakların kullanımın engellenmesine ilişkin geniş kapsamlı istisnalar ve gözetimi derinleştirecek teknolojik uygulamalar kullanılmamalıdır.

2016 yılında Sağlık Bakanlığı'nın 33 hastanesine yapılan siber saldırı sonucu bir milyona yakın hasta verisinin çalınmış, bu saldırılar sonucunda kişilerin yalnızca sağlık bilgileri değil, diğer kişisel bilgileri de üçüncü kişiler tarafından elde edilmiştir.[38] 2018 yılında sonuçlanan bir dava sonucu sağlık verileri de dahil olmak üzere birçok kişisel verinin Sosyal Güvenlik Kurumu tarafından üçüncü bir şirkete ihale ile satıldığı ortaya çıkmıştır.[39] Yine 2019 yılı yerel seçimlerinde kişilerin sağlık verilerinin politik amaçlarla kullanılmasına Sağlık Bakanlığı'nın sessiz kalması[40], Türkiye'de Sağlık Bakanlığı ile diğer kurumların şeffaf ve güvenilir bir şekilde kişisel verileri depolayamadığını ortaya koymaktadır.

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

---

[38] https://onedio.com/haber/devlet-hastanelerine-siber-saldiri-binlerce-hastanin-kayitlari-sizdi--711565.

[39] https://www.sozcu.com.tr/2018/ekonomi/skandal-sgk-hasta-bilgilerini-65-bin-tlye-satti-2225264/.

[40] https://turk-internet.com/kisitli-secmen-verileri-konusu-anayasal-koruma-altindaki-bir-hakkin-ihlalidir-ve-suctur/.

ISBN 978-605-80007-6-6