Polisin Sanal Devriye Yetkisini İptal Eden Anayasa Mahkemesi Kararının Değerlendirilmesi

Dr. Mehmet Bedii Kaya

İnternet ortamı dinamik bir alandır ve bu yönüyle suçla mücadele konusunda bünyesinde kendine özgü sorunlar barındırmaktadır. Bu dinamizm, usul açısından da muhtelif görev ve yetki sorunlarını beraberinde getirmektedir. Trafik verisinin kaydedilmesi, bu verilerin idari makamlar ve kolluk kuvvetleriyle paylaşımı, Türk hukukunda hukuki tartışmalara konu olmuştur.

Bu çalışma kapsamında, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun "Adli görev ve yetkiler" başlıklı ek madde 6'ya eklenen hükmü ile polise tanınan sanal devriye yetkisi ve bu yetkiyi iptal eden Anayasa Mahkemesi kararı kısaca değerlendirilecektir.

I. İnternetin izlenmesi ve trafik bilgisinin işlenmesi

Türk hukukunda, İnternet ortamının izlenmesi ve bu ortamdaki suçla mücadele edilmesi konusu ilk olarak 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile normatif dayanak kazanmıştır. İzleme, mevzuattaki tanımıyla İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesidir. 5651 sayılı Kanun kapsamındaki suçlar bağlamında Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından gerçekleştirilmektedir. BTK, çocukların İnternet ortamında korunması amacıyla katalog olarak belirlenen suçlara ilişkin olarak İnternet ağını izlemekte, erişim, yer ve içerik sağlayıcılarından trafik bilgilerine ilişkin talepte bulunabilmekte ve bazı durumlarda re'sen, bazı durumlarda ise talep üzerine hukuka aykırı içeriğe erişimi engellemektedir.

Erişimin engellenmesi, geçici bir hukuki tedbirdir. İçeriğin kaldırılması veya konusu suç teşkil eden içeriği oluşturan kişinin tespiti için müstakil bir süreç işletilmesi gerekmektedir. 5651 sayılı Kanunun temel mücadele noktası erişim, yer, toplu kullanım ve içerik sağlayıcılar üzerinden suçla mücadeledir. Bu mücadelenin en temel verisi ise erişim, toplu kullanım ve yer sağlayıcıları nezdinde tutulan trafik bilgisidir.

İstanbul Bilgi Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku Ana Bilim Dalı Öğretim Üyesi
E-posta: **mehmet@mbkaya.com** Web: **www.mbkaya.com**

Trafik bilgisine ilişkin temel gelişmeleri kronolojik olarak belirtmek gerekirse:

2007: Trafik bilgisinin tanımlanması

Trafik bilgisi 5651 sayılı Kanundaki ilk düzenlendiği halde "*İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerler*" olarak tanımlanmışken, 2014 yılında "*Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgiler*" olarak revize edilmiş ve varsa abone kimlik bilgilerinin de işlenmesinin önü açılmıştır.

2014: Trafik bilgisinin üçüncü kişilere aktarılmasının düzenlenmesi

Trafik bilgisi hangi koşullarda elde edilecek ve hangi amaçlarla kullanılacaktır? 2014 yılında 5651 sayılı Kanunun 3. maddesine eklenen dördüncü fıkrayla, trafik bilgisinin ancak bir suç soruşturması ve/veya kovuşturması kapsamında mahkemelerce talep edilmesi hâlinde (kapatılan) TİB tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınarak verileceği hüküm altına alınmıştır. Aynı yıl yapılan başka bir değişikle ise trafik bilgisinin TİB tarafından ilgili işletmecilerden temin edileceği ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verileceği düzenlenmiştir. Lakin, bu hüküm Anayasa Mahkemesi'nin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile iptal edilmiştir.

2015: TİB'e veri talebine ilişkin özel yetki tanınması

2014 yılında 5651 sayılı Kanunun içerik sağlayıcılara ilişkin 4., yer sağlayıcılara ilişkin 5. ve erişim sağlayıcılara ilişkin 6. maddesine (kapatılan) TİB'in talep ettiği bilgileri talep edilen şekilde TİB'e teslim etmekle ve TİB tarafından bildirilen tedbirleri almakla yükümlüdür şeklinde yeni bir hüküm eklenmiştir. Bu hükümler de Anayasa Mahkemesinin önüne götürülmüştür. Anayasa Mahkemesinin 8.12.2015 tarihli ve E 2014/87, K 2015/112 sayılı kararı ile bu söz konusu ilave hükümlerin iptaline karar verilmiştir.

2016: BTK'ya siber güvenlik ve siber caydırıcılıkla ilgili yetki verilmesi

5651 sayılı Kanunun 'İdari yapı ve görevler' başlıklı 10. maddesi BTK'ya ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, gerekli tedbirlerin aldırılması konusunda faaliyet yürütme ve ihtiyaç duyulan çalışmaları yapma yetkisi tanımaktadır.

2016 yılında 671 sayılı KHK'nın 25. maddesiyle 5809 sayılı Elektronik Haberleşme Kanununun 60. maddesine onuncu fıkra eklenmiş ve BTK'ya, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma yetkisi tanınmıştır. Aynı hükme eklenen on birinci fıkraya göre ise, BTK görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilecek ve değerlendirmesini yapabilecek; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilecek, bunlarla irtibat kurabilecek ve bu kapsamda diğer gerekli önlemleri alabilecek veya aldırabilecektir. Keza, gerçek kişiler ile özel hukuk tüzel kişilerin, BTK'nın bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamayacakları hüküm altına alınmıştır.

BTK'ya bu şekilde bir yetki veren hükümlerin iptali için Anayasa Mahkemesi nezdinde iptal davası açılmıştır. Konunun esasını inceleyen Anayasa Mahkemesi, 24.07.2019 tarihli ve E. 2017/16, K. 2019/64 sayılı kararıyla hükmü Anayasaya aykırı görmemiştir.

Anayasa Mahkemesine göre:

"***59.*** *Bilgi çağı olarak da adlandırılan çağımızda bilgi ve iletişim teknolojisinde büyük ilerlemeler yaşanmakta ve bu gelişmeler toplumu kuşatmaktadır. Bu ilerlemeye koşut olarak siber saldırı ve tehditlerin de artarak devam ettiği görülmektedir. Bu durum siber güvenlik ihtiyacının ortaya çıkmasına neden olmaktadır. Bireylerin güven içinde yaşamalarının sağlanmasında devlete yüklenen ödevler arasında şüphesiz siber güvenliğin sağlanması da yer almaktadır. Dolayısıyla siber güvenliğin sağlanmasının kamu güvenliğinin korunmasına yönelik olduğu anlaşılmaktadır.*

60. *Hedeflenen amacın gerçekleştirilmesi için kurallarla Kuruma ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve değerlendirmesini yapabilme, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu*

kapsamda diğer gerekli önlemleri alabilme ya da aldırabilme yetkisinin verilmesi ile Kurum tarafından istenen her türlü bilgi ve belge talebinin ilgilisi tarafından gecikmeksizin yerine getirilmesi hükme bağlanmıştır. Siber güvenliğin sağlanması amacıyla getirilen sınırlamanın anılan amaca ulaşmak bakımından gerekli ve elverişli olmadığı söylenemez. Kurumun bilgi temini yetkisinin siber güvenliğin sağlanması göreviyle sınırlı olduğu ve kişisel bilgilerin gizliliğini ve işletmecilerin ticari sırlarını korumakla yükümlü kılınması dolayısıyla bu yetkisini keyfi olarak kullanmasını önleyecek güvencelerin de sağlanmış olduğu dikkate alındığında kuralların getirdiği sınırlamanın orantısız olduğu da söylenemez."

2016: Trafik verisinin saklanma süresine ilişkin değişiklikler

5651 sayılı Kanunun 5. maddesinin üçüncü fıkrasına göre yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Keza, 6. maddenin birinci fıkrasına göre erişim sağlayıcı, sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

Öte yandan, trafik bilgilerinin saklanma sürelerine ilişkin 2016 yılında önemli bir değişiklik yapılmıştır. Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliğinin 2009 yılında yürürlüğe giren halinde, trafik bilgilerinin muhafaza edilmesi 19. maddesinin birinci fıkrasının (f) bendinde "Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, kullanıcı sayısı, kimlik bilgileri ve görüşme süreleri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini, bir yıl süreyle muhafaza etmekle yükümlüdür." şeklinde düzenlenmiş iken, bu hüküm 2016 yılında revize edilmiş ve trafik bilgilerinin muhafaza edilmesine yönelik düzenleme, "Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, taraflara ilişkin IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, kullanıcı sayısı ve abone kimlik bilgileri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini iki yıl süreyle; kullanıcı bilgilerini ise ilgili mevzuatta belirtilen zamanaşımı süresi boyunca muhafaza etmekle yükümlüdür." şeklinde değiştirilmiştir. Bu şekilde, erişim sağlayıcıların trafik bilgilerini saklama yükümlülüğü 1 yıldan 2 yıla çıkarılmıştır.

5651 sayılı Kanunun 6. Maddesi, trafik bilgilerinin altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklanacağı öngörülmüştür. Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliğindeki ilgili değişikliğin tarihinin diğer hükümlere göre (Uygulama ve Faaliyet Belgesi Yönetmeliklerinde yer alan) yeni tarihli olması ve özel olarak bu alanı düzenlemiş olması sebebiyle öncelikli uygulanması hukukun genel ilkesidir. Bu bağlamda erişim sağlayıcıların trafik bilgilerini 2 yıl boyunca saklama yükümlülüğü bulunmaktadır.

Öte yandan, 5651 sayılı Kanunun 5. maddesine 2014 yılında 6518 sayılı Kanunun 88. maddesiyle eklenen üçüncü fıkrası uyarınca yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Uygulama yönetmeliklerinde bu kanuni değişikliği yansıtacak güncellemeler henüz yapılmamıştır.

2017: Polise sanal devriye yetkisi tanınması

İnternet ortamında siber suçlarla mücadele için bir diğer önemli gelişme ise 2017 yılında gerçekleşmiştir. 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun "Adli görev ve yetkiler" başlıklı ek madde 6'ya eklenen hükmüyle polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkili kılınmıştır. Erişim sağlayıcılarının, yer sağlayıcılarının ve içerik sağlayıcılarının talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildireceği hüküm altına alınmıştır.

Polise verilen bu yetkinin de Anayasaya aykırı olduğu iddiasıyla iptal davası açılmıştır. Anayasa Mahkemesi, 19.02.2020 tarih, E. 2018/91 ve K. 2020/10 sayılı kararıyla polise sanal devriye yetkisi veren hükmü Anayasaya aykırı bularak iptal etmiştir.

III. Anayasa Mahkemesi'nin iptal kararının değerlendirilmesi

Anayasa Mahkemesi, 19.02.2020 tarih, E. 2018/91 ve K. 2020/10 sayılı kararıyla polise sanal devriye yetkisi veren hükmü Anayasaya aykırı bularak iptal etmiştir. Anayasa Mahkemesine göre:

"***101.*** *Buna göre sanal ortamda işlenen suçlar da dahil olmak üzere suç soruşturmasını yapacak yetkili Cumhuriyet başsavcılığının belirlenmesi ve bu konuya ilişkin uyuşmazlıkların çözümü yargı makamlarının görevi kapsamında kalmaktadır. Kanun'da yargı mercilerine, anılan görevin yerine*

getirilmesini sağlayabilecek bilgiler de dahil olmak üzere suç soruşturmasıyla ilgili bilgilere erişme yetkisinin de tanındığı görülmektedir. Dolayısıyla yalnızca yetkili Cumhuriyet başsavcılığının belirlenmesi amacıyla kolluğa, kişisel verilerin korunmasını isteme hakkını sınırlamak suretiyle kuralda belirtilen yetkiyi tanımanın zorunlu bir toplumsal ihtiyaca karşılık gelmediği ve bu yönüyle dava konusu kuralla getirilen sınırlamanın demokratik toplum düzeninin gereklerine uygun olmadığı sonucuna ulaşılmıştır.

***102.** Öte yandan kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın zorunlu bir toplumsal ihtiyaca karşılık geldiği hâllerde de Anayasa'ya uygun bir sınırlamanın varlığının kabulü için Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan söz konusu hakkın gerektirdiği özel güvencelerin kişilere sağlanmış olması gerekir. Dava konusu kuralla öngörülen yetkili Cumhuriyet başsavcılığının belirlenmesi için yapılan sınırlamanın zorunlu bir toplumsal ihtiyaca karşılık gelmediği sonucuna varıldığından bu özel güvenceler yönünden ayrıca inceleme yapılmasına gerek görülmemiştir.*"

Anayasa Mahkemesi'nin doyurucu bir gerekçe ortaya koyduğunu söylemek zordur. Basit bir metodolojiyle konuya yaklaşmıştır: trafik bilgisinin temini için zorunlu bir toplumsal ihtiyaç yoktur. İlk koşul sağlanmadığı için, kişisel verilerin korunmasına yönelik kişilere özel güvencelerin sağlanıp sağlanmadığı konusuna ilişkin Mahkeme ayrıca inceleme yapmamıştır.

Esasında, dünyada siber güvenlik tehditleri artmakta, şekil ve nitelik değiştirmekte, bu tehditlerin etkilediği alanlar farklılaşmaktadır. Bu gelişim ve değişime bağlı olarak da bilişim suçları çok farklı şekilde işlenmekte; bilişim suçlarına konu fiil ve eylemler geniş bir spektruma yayılmaktadır. Trafik bilgileri suçla mücadele için önemli veriler içermektedir. Trafik bilgilerinin en önemlisi olan IP adresi kişiyi değil, internet ağına bağlanan cihazı işaret eder. Dolayısıyla, cihazı kimin kullandığının tespiti ayrıca her somut olaydaki bulgulara ve verilere göre tespit edilmesi gereken bir husustur. Sanal devriye hükmü incelendiğinde, yetkinin konuyla sınırlandığı görülmektedir: yetkili Cumhuriyet başsavcılığının tespiti. Şu hâlde, bilişim suçlarıyla mücadelede özellikle olası yetki sorunlarını bertaraf etmek ve suçla daha etkin ve hızlı şekilde mücadele etmek amacıyla getirilen hükmün zorunlu bir toplumsal ihtiyaca karşılık gelmediği söylenemez.

Doğrudan bilişim suçları veya dolaylı bilişim suçları işlenerek kişilerin mal ve can güvenliği tehlikeye atılmaktadır. Türkiye'nin de taraf olduğu ve iç hukukuna aktardığı Avrupa Konseyi Siber Suçlar Sözleşmesi uyarınca Türkiye başta çocuk pornografisi olmak üzere çeşitli bilişim suçu için

mücadele için uluslararası iş birliği içerisindedir. Siber Suçlar Sözleşmesi, taraf devletlerin trafik verisinin süratli şekilde korunması ve kısmen açıklanması ve trafik verilerinin gerçek zamanlı toplanmasına ilişkin kurallar koymakta ve her bir taraf devlet nezdinde kurulan 7/24 esasına dayalı göre çalışan birimler aracılığıyla siber suçlarla hızlı ve etkin şekilde mücadele edilmesini sağlamaktadır.

Siber dünyadaki en önemli tehdit ise çocukların cinsel istismarıdır. Çocukların cinsel istismarının önlenmesi küresel ölçekte güncel bir sorundur. Öyle ki, devletlerin iç hukuk farklılıklarından dolayı çocuklara yönelik yaklaşımlarının değişmesi sebebiyle, çocukların etkin bir şekilde korunması amacıyla çeşitli uluslararası sözleşmeler akdedilmiştir. Suçluların başka bilişim sistemlerini istismar etmesi, izlerini kaybettirmek için farklı ölçekte şifreleme sistemleri kullanması sebebiyle bu alanda mücadele için günler değil bazen saatler ve hatta dakikalara önemli hale gelmektedir. Özellikle çocukların cinsel istismarının önlenmesi gibi soruşturulmasında ve kovuşturulmasında üstün kamusal yararın olduğu alanlar için polise sanal devriye yetkisi tanınması zorunlu bir toplumsal ihtiyaca karşılık gelmektedir.

Peki, polise tanınan sanal devriye hükmüyle Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan söz konusu hakkın gerektirdiği özel güvenceler kişilere sağlanmış mıdır? Esasında polis ve yargı makamlarının kişisel verileri işlemesi ve muhafazası konusunda mevzuat dağınıktır; farklı veri türlerine ilişkin muhtelif hükümler bulunmaktadır.**[1]** Kişisel verilerin en etkin şekilde korunması, işlenmesi ve aktarılmasını düzenleyen, konunun bilgi güvenliği, idari ve teknik tedbirleri tanımlayan bir çerçeveye ihtiyaç bulunmaktadır.

Mukayeseli hukuktan örnek vermek gerekirse; Avrupa Birliği'nin Genel Veri Koruma Tüzüğünün tamamlayıcısı, Polis ve Yargı Direktifi olarak da anılan "*AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/680 sayılı, Konsey'in 2008/977/JHA Çerçeve Kararını yürürlükten kaldıran, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair Direktif*" isimli düzenlemedir.**[2]**

Kolluk ve adli makamların görevlerini yerine getirirken muhtelif nitelikte ve boyutta kişisel verileri işlemesi kaçınılmazdır. Bu veri işleme sırasında denge nasıl sağlanacaktır? AB Polis ve Yargı Direktifi politika temelli koruma, sözleşme temelli koruma, risk temelli koruma,

mahremiyet temelli koruma, güvenlik temelli koruma ve en önemlisi işlem kaydı temelli koruma ilkeleriyle hesap verebilirlik ve denetimi sağlamaktadır.

Direktifin temel ilkeleri ise şöyledir:

- Maksimum kayıt süreleri ve veriyi muhafaza için periyodik denetim yapılmalıdır.
- Gözden geçirme kayıt altına alınmalı ve işlemler gerekçelendirilmelidir.
- Veri kalitesi temin edilmelidir.
- Mahremiyet temelli koruma sağlanmalıdır.
- Mevcut ve gelecek veri tabanlarının periyodik gözden geçirmeyi otomatik sağlaması ve yaşam süresinin sonunda verilerin otomatik silinmesini temin etmelidir.
- Veri kayıt süreleri değişik veri sahibi kategorilerine göre ayrı ayrı belirlenmelidir.

Bu şekilde de hem kişisel verilerin etkin şekilde işlenmesi hem de bir ihlal durumunda ilgili kişilerin korunması, ilgili hesap verme mekanizmalarının işletilmesi mümkün hale gelmektedir.

Türk hukukunda henüz kapsamlı bir şebeke ve bilgi güvenliği düzenlemesinin olmaması da kişisel verilerin istisna alanlarda işlenmesi durumunda uygulanacak teknik ve idari tedbirlere ilişkin belirsizlik yaratmaktadır.

Anayasa Mahkemesinin polise sanal devriye yetkisi veren hükmü zorunlu bir toplumsal ihtiyaca karşılık gelmediği ve haliyle demokratik toplum düzeninin gerekliliklerine aykırı olduğu gerekçesiyle iptali görüşüne katılmamakla birlikte, Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan söz konusu hakkın gerektirdiği özel güvencelerin kişilere tam manasıyla sağlanmış olduğunu söylemek de yukarıda izah edilen gerekçelerle pek mümkün değildir. Nihayetinde, Kişisel Verilerin Korunması Kanununun 28. maddesinde yer alan kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi istisnası, kişisel verilerin bu alanlarda hiçbir korumaya sahip olmadığı manasına gelmemektedir. Bu alanın istisna tutulmasının sebebi, alana özgü veri işleme usulleri dikkate alınarak kendine özgü kurallarla düzenlenmesine ilişkin ihtiyaçtır.

Belirtmek gerekir ki, 6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkındaki Kanun ile kurulan Kolluk Gözetim Komisyonu da kişisel verilerin etkin şekilde korunması, bilgi güvenliği yükümlülüklerinin temini, kişisel verilerin korunmasına ilişkin teknik ve idari yükümlülüklerin

yerine getirilmesi, ilgili kişilerin haklarının korunması için gereken etkinliğin sağlanmasını temin edecek nitelik bir idari yapı değildir.

Anayasa Mahkemesi'nin BTK'nın siber güvenlik ve caydırıcılığa ilişkin bilgi ve belge talep yetkisini iptal etmemesindeki aslında en temel sebep, elektronik haberleşme alanında kişisel verilerin korunmasına ilişkin hem belirli hem de etkin bir yasal çerçevenin varlığıdır. 5809 sayılı Elektronik Haberleşme Kanunu, elektronik haberleşme alanında kişisel verilerin korunmasına ilişkin öncü bir düzenlemedir. Anayasa Mahkemesi'nin 24.07.2019 tarihli ve E. 2017/16, K. 2019/64 sayılı kararındaki tespitini tekrarlamak gerekirse: "*Kurumun bilgi temini yetkisinin siber güvenliğin sağlanması göreviyle sınırlı olduğu ve kişisel bilgilerin gizliliğini ve işletmecilerin ticari sırlarını korumakla yükümlü kılınması dolayısıyla bu yetkisini keyfi olarak kullanmasını önleyecek güvencelerin de sağlanmış olduğu dikkate alındığında kuralların getirdiği sınırlamanın orantısız olduğu da söylenemez.*"

Türkiye'de, kişisel verilerin kolluk veya yargı makamları tarafından işlendiği durumlarda da uygulanacak genel bir kanuna ihtiyaç vardır. Nasıl ki AB Polis ve Yargı Direktifi, AB Genel Veri Koruma Tüzüğünü tamamlıyor, çıkartılacak özel düzenleme de 6698 sayılı Kişisel Verilerin Korunması Kanununu tamamlayacaktır. Bu şekilde, Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan kişisel verilerin korunması hakkının gerektirdiği özel güvencelerin kişilere sağlanmış olması mümkün olacaktır.

Özetle, Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan kişisel verilerin korunmasını talep hakkının gerektirdiği özel güvencelerin kişilere sağlanmış olması kaydıyla polise sanal devriye yapma yetkisi verilmesi zorunlu bir toplumsal ihtiyaca karşılık gelmektedir.

Referanslar

[1] Bu konudaki genel mevzuat için bkz. **https://www.mbkaya.com/hukuk/abpolisveyargidirektifi.pdf**

[2] AB Polis ve Yargı Direktifinin Türkçe tercümesi için bkz. **https://www.mbkaya.com/hukuk/law-enforcement-directive-turkce.pdf**