ANAYASA MAHKEMESİ KARARI

Anayasa Mahkemesi Başkanlığından:

GENEL KURUL
KARAR

BESTAMİ EROĞLU BAŞVURUSU

Başvuru Numarası : **2018/23077**
Karar Tarihi : **17/9/2020**

Başkan : Zühtü ARSLAN
Başkanvekili : Hasan Tahsin GÖKCAN
Başkanvekili : Kadir ÖZKAYA
Üyeler : Serdar ÖZGÜLDÜR
Burhan ÜSTÜN
Engin YILDIRIM
Hicabi DURSUN
Celal Mümtaz AKINCI
Muammer TOPAL
M. Emin KUZ
Rıdvan GÜLEÇ
Recai AKYEL
Yusuf Şevki HAKYEMEZ
Yıldız SEFERİNOĞLU
Selahaddin MENTEŞ
Basri BAĞCI
Raportörler : Şermin BİRTANE
Ayhan KILIÇ
Başvurucu : Bestami EROĞLU
Vekili : Av. Metin POLAT

I. BAŞVURUNUN KONUSU

1. Başvuru; tutuklama tedbirinin hukuki olmaması nedeniyle kişi hürriyeti ve güvenliği hakkının, ByLock haberleşmesi ve kişisel verilerin yasal olmayan şekilde elde edilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ve geçmişteki ByLock kullanımı dolayısıyla cezalandırılma nedeniyle de suç ve cezaların kanuniliği ilkesinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 26/7/2018 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmiştir.

7. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmamıştır.

8. İkinci Bölüm tarafından 9/9/2020 tarihinde yapılan toplantıda, niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:

10. Başvurucu 1978 doğumlu olup inceleme tarihi itibarıyla Kayseri 1 No.lu T Tipi Kapalı Ceza İnfaz Kurumunda hükümlü olarak bulunmaktadır. Başvurucu, bireysel başvuruya konu olayların geçtiği tarihte öğretmen olarak görev yapmaktadır. Başvurucu, terör örgütleriyle veya Millî Güvenlik Kurulunca devletin millî güvenliğine karşı faaliyette bulunduğuna karar verilen yapı, oluşum veya gruplarla irtibatı olduğu gerekçesiyle 15/8/2016 tarihli ve 672 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname ile kamu görevinden çıkarılmıştır.

A. Genel Bilgiler

11. Türkiye 15 Temmuz 2016 tarihinde askerî bir darbe teşebbüsüyle karşı karşıya kalmış, bu nedenle 21/7/2016 tarihinde ülke genelinde olağanüstü hâl ilan edilmesine karar verilmiş ve olağanüstü hâl 19/7/2018 tarihinde -yeniden uzatılmayarak- son bulmuştur. Kamu makamları ve yargı organları -olgusal temellere dayanarak- bu teşebbüsün arkasında Fetullahçı Terör Örgütü/Paralel Devlet Yapılanmasının (FETÖ/PDY) olduğunu değerlendirmiştir (darbe teşebbüsü ve arkasındaki yapılanmaya ilişkin ayrıntılı bilgi için bkz. *Aydın Yavuz ve diğerleri* [GK], B. No: 2016/22169, 20/6/2017, §§ 12-25). Darbe teşebbüsü sırasında ve sonrasında ülke genelinde darbe girişimiyle bağlantılı ya da doğrudan darbe girişimiyle bağlantılı olmasa bile FETÖ/PDY'nin kamu kurumlarındaki örgütlenmesinin yanı sıra eğitim, sağlık, ticaret, sivil toplum ve medya gibi farklı alanlardaki yapılanmasına yönelik olarak Cumhuriyet başsavcılıkları tarafından soruşturmalar yürütülmüş; çok sayıda kişi hakkında gözaltı ve tutuklama tedbirleri uygulanmıştır (*Aydın Yavuz ve diğerleri*, § 51; *Mehmet Hasan Altan (2)* [GK], B. No: 2016/23672, 11/1/2018, § 12).

12. Yargı organları birçok kararda FETÖ/PDY'nin devletin anayasal kurumlarını ele geçirmeyi, sonrasında devleti, toplumu ve fertleri kendi ideolojisi doğrultusunda yeniden şekillendirmeyi, oligarşik özellikler taşıyan bir zümre eliyle ekonomiyi, toplumsal ve siyasal gücü yönetmeyi amaçlayan, bu doğrultuda mevcut idari sisteme paralel şekilde örgütlenen bir terör örgütü olduğunu kabul etmiştir. Yargı organları kararlarında ayrıca FETÖ/PDY'nin gizlilik, hücre tipi yapılanma, her kurumda örgütlenmiş olma, kendisine kutsallık atfetme, itaat ve teslimiyet temelinde hareket etme gibi birçok özelliğinin bulunduğunu, bu örgütün diğerlerine nazaran çok daha zor ve karmaşık bir yapı olduğunu ortaya koymuştur (FETÖ/PDY'nin genel özellikleri için bkz. *Aydın Yavuz ve diğerleri*, § 26; yargı organlarındaki örgütlenme biçimi için bkz. *Selçuk Özdemir* [GK], B. No: 2016/49158, 26/7/2017, § 22; *Alparslan Altan* [GK], B. No: 2016/15586, 11/1/2018, § 11).

13. Örgütlenme şekli olarak gizliliği esas alan FETÖ/PDY'nin üyelerine telkin ettiği yöntemler, istihbarata karşı koyma olarak nitelendirilebilecek düzeyde güvenlik önlemleridir. Bu bağlamda FETÖ/PDY'nin kurucusu ve lideri olan Fetullah Gülen'in örgüt mensuplarına *"Hizmet bir namaz ise tedbir onun abdestidir. Tedbirsiz hizmet abdestsiz namaz gibidir."* şeklinde talimat verdiği ifade edilmiştir. Gizliliği sağlamak üzere örgüt tarafından başvurulan yöntemler arasında -diğer pek çok terör örgütünde olduğu üzere- *kod adı* kullanmak da yer almaktadır. Soruşturma ve kovuşturma makamlarının tespitlerine göre FETÖ/PDY'nin deşifre olmamak için bir *tedbir* olarak iletişimde başvurduğu temel yöntem yüz yüze görüşme, bunun mümkün olmadığı durumlarda ise kripto programlar üzerinden iletişimdir. Örgüt liderinin *"Telefonla görüşme yapanlar hizmete ihanet etmiş olur."* şeklindeki talimatı nedeniyle telefonla olağan usulde örgütsel görüşme yapılması yasaktır (bu konuda detaylı bilgi için bkz. Yargıtay 9. Ceza Dairesinin -ilk derece mahkemesi sıfatıyla- 28/3/2019 tarihli ve E.2018/12, K.2019/45 sayılı kararı). Bu nedenle örgütsel iletişimde kullanılmak üzere güçlü kriptolu programlar geliştirilmiştir (*Ferhat Kara* [GK], B. No: 2018/15231, 4/6/2020, § 22).

B. ByLock Programına İlişkin Açıklamalar

14. FETÖ/PDY'nin örgütsel haberleşme için oluşturduğu ve örgüt mensuplarınca kullanılan iletişim yöntemlerinden birinin ByLock uygulaması olduğu özellikle darbe teşebbüsünden sonra örgütle bağlantılı soruşturma ve kovuşturmalarda tespit edilmiştir (*Ferhat Kara*, § 23). ByLock haberleşme programıyla ilgili kavramsal açıklamalara, programın tespiti, adli makamlara ulaştırılması ve adli sürece, yüklenmesine ve iletişimde kullanılmasına, genel ve örgütsel özelliklerine, yaygın uygulamalardan ayrılan yönlerine, ByLock verilerinin niteliği, anlamlandırılması ve kişilerle eşleştirilmesine ilişkin arka plan bilgisinin detaylarına *Ferhat Kara* kararında yer verilmiştir (*Ferhat Kara*, §§ 23-67).

C. ByLock Programının Tespiti, Adli Makamlara Ulaştırılması ve Adli Süreç

15. Millî İstihbarat Teşkilatı (MİT) tarafından 1/1/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 4. ve 6. maddeleri uyarınca yürütülen çalışmalar kapsamında ana sunucusu yurt dışında bulunan *ByLock (ByLock: Chat and Talk)* adlı bir mobil uygulama ve bu uygulamanın iletişim kurduğu sunucular ayrıntılı teknik çalışmalara tabi tutulmuştur. MİT'e özgü teknik istihbarat usul, araç ve yöntemleri kullanılmak suretiyle yapılan bu çalışma sonucunda, FETÖ/PDY'nin kullandığı değerlendirilen bu programla ilgili olarak birtakım veriler elde edilmiştir (*Ferhat Kara*, § 25).

16. MİT, ByLock programıyla ilgili olarak temin edilen dijital verileri içeren sabit diski ve uygulamaya bağlantı sağlayan ByLock abone listesinin bulunduğu flash bellek ile düzenlediği ByLock Uygulaması Teknik Raporu'nu Ankara Cumhuriyet Başsavcılığına teslim etmiştir (*Ferhat Kara*, § 26)

17. Bunun akabinde Ankara Cumhuriyet Başsavcılığı, Ankara 4. Sulh Ceza Hâkimliğinden söz konusu (dijital) materyal üzerinde 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesi uyarınca inceleme, kopyalama, çözümleme işlemi yapılmasına karar verilmesi talebinde bulunmuştur. İlgili yazıda; anılan madde gereğince bir adet *Sony marka HD-B1 model, üzerinde bBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24f0d69ede96 yazılı hard disk* ve bir adet *Kingston marka data traveler, uç kısmında DTIG4/8GB 04570-700.A00LF5V 0S7455704 yazılı flash bellek* üzerinde inceleme yapılmasına, iki kopya çıkarılmasına ve kopya üzerindeki kayıtların çözümlenerek metin hâline getirilmesine karar verilmesi istenmiştir (*Ferhat Kara*, § 27).

18. Ankara 4. Sulh Ceza Hâkimliği tarafından 5271 sayılı Kanun'un 134. maddesi uyarınca talep kabul edilmiş ve *"dijital materyaller üzerinde inceleme yapılması, kopya çıkarılması ve kopya üzerinde bilirkişi incelemesi yapılarak metin haline getirilmesi için bir kopyasının Ankara Cumhuriyet Başsavcılığına gönderilmesine"* karar verilmiştir. Anılan karar doğrultusunda görevlendirilen iki uzman bilirkişi tarafından hâkim huzurunda kamera kaydı da yapılmak suretiyle söz konusu hard disk ve flash bellek üzerinde imaj alma-kopyalama işlemi yapılmıştır (*Ferhat Kara*, § 28).

19. Ankara Cumhuriyet Başsavcılığınca Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına (EGM-KOM Daire Başkanlığı) gönderilen bir yazıyla Ankara 4. Sulh Ceza Hâkimliğince verilen inceleme, kopyalama ve çözümleme kararına istinaden gerekli araştırma ve soruşturma işlemlerinin yapılması, ulaşılan tespitleri içerir bir rapor düzenlenmesi talimatı verilmiştir (*Ferhat Kara*, § 29).

20. EGM-KOM Daire Başkanlığınca teslim alınan verilerin (ByLock verilerini içeren hard disk ve abone listesinin bulunduğu flash bellek) incelenmesi ve rapor hazırlanması amacıyla EGM-KOM, Terörle Mücadele (TEM), İstihbarat ve Siber Suçlarla Mücadele Daire Başkanlıkları tarafından görevlendirilen personelden oluşan bir çalışma grubu oluşturulmuştur. Bu kapsamda ByLock verilerinin dışarı aktarılması için arayüz programı kullanılmış ve bu sayede ByLock verileri incelenmeye başlanmıştır (*Ferhat Kara*, § 30).

21. Bu arada Yargıtay 16. Ceza Dairesince yürütülen bir yargılamaya esas olmak üzere EGM-KOM Daire Başkanlığından ByLock'un teknik özelliklerine dair bilgi istenmiştir. EGM-KOM Daire Başkanlığı tarafından bir rapor hazırlanarak anılan Daireye gönderilmiştir. Söz konusu raporda; ByLock iletişim sisteminin mahiyeti ve diğer özellikleri hakkında ayrıntılı bilgiler verildikten sonra anılan uygulamadaki kullanıcı sayısı, arkadaş grubu, mesaj ve e-posta içeriklerine dair açıklamalarda bulunulmuştur (*Ferhat Kara*, § 31).

22. Sonraki süreçte Ankara Cumhuriyet Başsavcılığı tarafından ByLock IP adreslerine bağlandığı belirtilenlere ilişkin listede yer alan abonelerin ByLock IP adreslerine kaç defa bağlandığına dair raporlar (CGNAT verileri) Bilgi Teknolojileri ve İletişim Kurumundan (BTK) talep edilmiştir (*Ferhat Kara*, § 32).

23. Bu arada MİT tarafından detaylı çalışma yapılarak güncellenen abone listesinin yeni hâli tekrar Ankara Cumhuriyet Başsavcılığına gönderilmiştir. Başsavcılığın talebi üzerine Ankara 5. Sulh Ceza Hâkimliğince MİT tarafından gönderilen *data traveler G4 marka, DTİG4/8GB 04570-760B00LF 5V 0S 7575458 seri numaralı TAİWAN ibaresi bulunan dijital materyal* üzerinde 5271 sayılı Kanun'un 134. maddesi gereğince inceleme yapılmasına, kopya çıkarılmasına (imaj alma), bu kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir. Bu karar doğrultusunda söz konusu materyalin imaj alma (kopyalama) işlemi Cumhuriyet savcısı ve görevlendirilen iki adli bilişim görevlisinin huzurunda video kamera eşliğinde gerçekleştirilmiştir (*Ferhat Kara*, § 33).

24. Sonrasında Ankara Cumhuriyet Başsavcılığı tarafından abone listesi BTK'ya bildirilmiş ve ByLock sunucusuna bağlanan *güncellenmiş numaraların* abonelerine ait şahıs *kimlik bilgilerinin* tespiti için BTK'dan bilgi istenmiştir (*Ferhat Kara*, § 34).

25. Bağlantı yapılan GSM numaralarına ait abonelik bilgileri ve ADSL numaralarına ait abonelik bilgileri de farklı tarihlerde BTK'dan alınarak Ankara Cumhuriyet Başsavcılığına iletilmiştir. Devamında KOM Daire Başkanlığınca Ankara Cumhuriyet Başsavcılığından teslim alınan abonelik bilgilerinden yararlanılarak yeni *"user ID_list"* (kullanıcı listesi) tablosu oluşturulmuştur (*Ferhat Kara*, § 35).

26. Ankara Cumhuriyet Başsavcılığınca EGM-KOM Daire Başkanlığına verilen talimat üzerine BTK tarafından gönderilen 123.111 GSM numarasına ait CGNAT verilerinin (ByLock sunucusuna ait IP adreslerine hangi tarihte kaç defa bağlanıldığı bilgisi) -il Cumhuriyet başsavcılıklarına gönderilmek üzere- il KOM birimlerine dağıtılmasına başlanmıştır. VPN programı kullanılarak yapılan bağlantıların Türkiye IP'si almaması sebebiyle gerçekte ByLock kullanıcısı olan kişilerin VPN programı kullanarak ByLock sunucusunun IP'lerine yaptıkları bağlantılara dair CGNAT kayıtlarına erişilememiştir. CGNAT kayıtlarına ulaşılanlar, ByLock sunucusuna ait hedef IP'lerine Türkiye IP'lerinden VPN kullanmaksızın yapılan ya da Türkiye'den VPN ile bağlantı devam ederken VPN'nin devre dışı kalması sonucunda yeniden Türkiye IP'si alınması nedeniyle tespit edilebilen bağlantılara aittir (*Ferhat Kara*, § 36).

27. Bu arada internet üzerinde yayımlanan *Morbeyin* isimli adres ve uygulamaları kullananların arka plandaki kodlar vasıtasıyla doğrudan ByLock IP'sine bağlandıklarına ve ByLock dökümü bulunmayan (gerçekte ByLock kullanıcısı olmayan) bazı kişilerin haksız yere cezalandırıldığına dair kamuoyunda paylaşılan iddia ve haberlerle ilgili olarak Ankara Cumhuriyet Başsavcılığı tarafından soruşturma başlatılmış ve bu kapsamda Siber Suçlarla Mücadele Daire Başkanlığı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve BTK görevlilerinden oluşan inceleme grubu oluşturulmuştur. Başsavcılığın yaptığı soruşturmada FETÖ/PDY'nin ileride delil olması ihtimaline karşı gerçek ByLock kullanıcılarının açığa çıkmasını önlemek, ilgisiz kişileri bu programa yönlendirmek ve bu suretle delilin güvenilirlik derecesini düşürmek amacıyla 2014 yılında *Morbeyin* isimli bir yazılım yaptırdığı, kullanıcının kıble pusulası, namaz vakti, dua dinleme, Kur'an okuma ve çeşitli sözlük uygulamalarına girmesi hâlinde bu programın tesiriyle bilgisi ve iradesi dışında cihazının bir iki saniye kadar ByLock sunucusunun IP'lerine bağlandığının göründüğü tespit edilmiştir. Bu konuda gerçekleştirilen detaylı inceleme neticesinde bağlantı ve veri parametreleri bakımından benzer özellikler taşıyan 11.480 GSM numarasının kullanıcısının iradeleri dışında ByLock sunucusu IP'lerine yönlendirilmiş olduğu belirlenmiştir. Bunlar listelerden çıkarılmıştır (*Ferhat Kara*, § 37).

D. Başvurucuya İlişkin Süreç

28. Kayseri Cumhuriyet Başsavcılığı (Başsavcılık) tarafından başvurucunun da aralarında bulunduğu Millî Eğitim Bakanlığı personeli hakkında FETÖ/PDY'ye üye olma suçunu işledikleri isnadıyla soruşturma başlatılmıştır.

29. Soruşturma kapsamında Başsavcılığın 5/9/2016 tarihli talebi üzerine Kayseri 3. Sulh Ceza Hâkimliğince 5271 sayılı Kanun'un 116., 127. ve 134. maddeleri uyarınca başvurucunun da aralarında bulunduğu şüphelilerin ikametgâhlarında 6/9/2016 tarihinde arama yapılmasına, bulunan cep telefonu, bilgisayar, hard disk, hafıza kartları, sim kartları vb. kayıt tutma özelliği bulunan her türlü dijital materyale el konulmasına, ele geçirilecek kayıtlardan kopya alınmasına, kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir.

30. Başvurucu, Kayseri 3. Sulh Ceza Hâkimliğinin 8/9/2016 tarihli kararı ile tutuklanmıştır.

31. Kayseri Cumhuriyet Başsavcılığının 26/10/2016 tarihli yazısıyla, 5271 sayılı Kanun'un 135. maddesi uyarınca başvurucunun da aralarında bulunduğu şüphelilerin telefon numaralarının 1/10/2013 ile 1/10/2016 tarihleri arasında iletişim kayıtları ve hangi baz istasyonlarından servis aldığının tespitine karar verilmesi talep edilmiştir. Kayseri 1. Sulh Ceza Hâkimliğinin 2/11/2016 tarihli kararı ile talep doğrultusunda karar verilmiştir.

32. Başsavcılık tarafından 27/12/2016 tarihli iddianame ile Kayseri 2. Ağır Ceza Mahkemesinde (Mahkeme) kamu davası açılmıştır. İddianamede FETÖ/PDY'ye ilişkin açıklamalara yer verildikten sonra başvurucunun durumu değerlendirilmiştir. İddianamede başvurucunun örgütün haberleşme aracı olan ByLock programının kullanıcısı olduğu tespitine yer verilmiştir. Söz konusu haberleşme programının örgüt üyesi olmayanlar tarafından kullanılmasının mümkün olmadığının vurgulandığı iddianamede, başvurucunun terör örgütüne üye olma suçunu işlediği kanaati ifade edilmiştir. İddianamede başvurucunun ByLock isimli şifreli haberleşme programını adına kayıtlı 533....2 GSM numarası ile kullandığının tespit edildiği belirtilmiştir. İddianamede ayrıca başvurucunun Bank Asyada hesabının bulunmasına, 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname ile kapatılan *Aktif Eğitim-Sen* isimli sendika ile Silopi Eğitimciler ve Girişimci İş Adamları Derneğinin üyesi olmasına ve başvurucunun sohbet imamı olduğunu beyan eden O.D. isimli bir tanığın ifadesine dayanılmıştır.

33. Mahkeme başvurucunun ByLock kullanıp kullanmadığı, kullanmış ise hangi telefon hattı ve IMEI numaralı telefonda kullandığı hususunda bilgi verilmesini KOM'dan ve Kayseri İl Emniyet Müdürlüğünden istemiştir. Kayseri Siber Suçlar İle Mücadele Şube Müdürlüğünce 18/2/2017 tarihinde başvurucuya ait dijital materyallere dair inceleme raporu ve ekinde bir adet DVD mahkeme dosyasına sunulmuştur.

34. Kayseri İl Emniyet Müdürlüğü KOM Şube Müdürlüğünce 6/2/2017 tarihinde *Yeni ByLock CBS Sorgu Sonucu Raporu* sunulmuş ve başvurucuya ait telefonun hat numarası ve IMEI numarası bilgilerine göre başvurucunun telefonuna ByLock haberleşme programını yükleyerek *(4397) ID kullanıcı numarasıyla* kullandığının anlaşıldığı belirtilmiştir. Ayrıca Ankara Cumhuriyet Başsavcılığının 2016/180056 sayılı soruşturma dosyasından elde edilen bilgi kapsamında başvurucuya ait ByLock kullanımını gösteren ByLock Tespit ve Değerlendirme Tutanağı sunulmuştur. Söz konusu tutanakta, başvurucu adına kayıtlı olan

GSM hattı kullanılarak ByLock sunucusuna yapılan bağlantı sonucunda ByLock iletişim sistemi içinde oluşturulan verilere ilişkin bilgiler yer almaktadır. Buna göre ByLock Tespit ve Değerlendirme Tutanağı'nda; kullanıcı bilgilerinin yanı sıra kullanıma ilişkin istatistiksel verilere, kullanıcıyı ekleyenlerin ve kullanıcının eklediği kişilere, kullanıcının kurduğu ve katıldığı gruplar ile bunların kişi listesine, kullanıcıya bağlı kişi ve mail listesi ile yazışmalara, mail bilgisi ve arama kayıtları ile log tablolarına dair bilgiler bulunmaktadır.

35. Başvurucu hakkındaki yargılama iki celsede tamamlanmıştır. 9/3/2017 tarihli ilk duruşmada Mahkeme bir tanığı dinlemiştir. Tanık O.D. başvurucunun sohbet imamı olduğunu, sohbetlerde Fetullah Gülen'in vaazlarını dinlediklerini beyan etmiştir. Başvurucu ise suçlamaları ve tanık beyanını kabul etmediğini, ByLock programını kullanmadığını, 7-8 yıldır aynı telefon hattını kullandığını, bu hatla ByLock programını ne zaman ne şekilde indirdiğini bilmediğini, HTS kayıtlarında inceleme yapıldığı takdirde ByLock kullanmadığının anlaşılacağını belirtmiştir. Başvurucu müdafii; HTS kayıtları, IP çakışması, ByLock içeriklerini gösteren belgelerin getirtilmesini talep ettiğini belirtmiştir.

36. 14/3/2017 tarihinde yapılan ikinci duruşmada Mahkeme, başvurucunun silahlı terör örgütüne üye olma suçundan 7 yıl 6 ay hapis cezası ile cezalandırılmasına karar vermiştir. Kararın gerekçesinde hem FETÖ/PDY'nin kuruluşu, amaçları ve yapılanmasıyla ilgili hem de ByLock iletişim programına, bu programa dair verilerin hukuka uygun delil olduğuna ve programın örgütün kullanımına sunulmuş, örgütsel amaçlarla kullanılan bir program olduğuna dair açıklamalara yer verilmiştir. Başvurucunun sıradan bir vatandaşın temin edip kullanma imkânı olmayan ve sadece FETÖ/PDY mensuplarınca haberleşme amacıyla kullanıldığı bilinen ByLock isimli programını kullanmak, FETÖ/PDY ile irtibat ve iltisakı olması nedeniyle 667 sayılı KHK'yla kapatılan Aktif Eğitim Sen ile Silopi Eğitimciler ve Girişimci İş Adamları Derneğine üye olmak, FETÖ/PDY tarafından düzenlenen toplantılara katılmak, bu toplantılarda imamlık yapmak, Bank Asyaya gelirinin çok üzerinde para yatırarak Bank Asyayı desteklemek suretiyle örgütün hiyerarşik yapısına dâhil olduğu, böylelikle üzerine atılı terör örgütüne üye olma suçunu işlediği belirtilmiştir.

37. Başvurucu anılan karara karşı istinaf başvurusunda bulunmuştur. İstinaf dilekçesinde ceza normunun geçmişe yürütülmesi, telefona ByLock programının yüklenmiş olmasının suç kapsamında yorumlanması sebebiyle suç ve cezaların kanuniliği ilkesinin, ceza kanununun geniş yorumlanması sebebiyle de kıyas yasağının ihlal edildiğini ileri sürmüştür. Başvurucu, kanuni olmayan delillere dayanılarak suç isnat edilmesinin belirlilik ilkesine aykırı olduğunu, mahkûmiyet hükmünün varsayıma dayandığını belirtmiş; ByLock delilinin hukuka aykırı olarak elde edildiğini iddia etmiştir.

38. Ankara Bölge Adliye Mahkemesi 4. Ceza Dairesi (Bölge Adliye Mahkemesi) başvurucunun kullandığı GSM hattının ve bu hatlarda kullanılan IMEI numaralarının 1/1/2014-15/7/2016 tarihi aralığını kapsayacak şekilde HTS kayıtları ile 12/7/2014-15/7/2016 tarihi aralığını kapsayacak şekilde ByLock'un belirlenen IP numaralarına bağlantı yaptığı tarih, saat ve baz istasyonu gösterir HTS kayıtlarını BTK Başkanlığından ve başvurucunun kullandığı GSM hatları ile Bylock programı üzerinden yaptığı iletişim içeriklerinin tespitini Emniyet Genel Müdürlüğü KOM Daire Başkanlığından talep etmiştir. Bölge Adliye Mahkemesi başvurucunun GSM hattı ve bu hattın kullanıldığı cihazlarla ByLock programına erişime ilişkin olarak BTK Başkanlığı ve Emniyet Genel Müdürlüğü KOM Daire Başkanlığından getirtilen kayıtlar üzerinde adli bilişim konusunda uzman bilirkişiden rapor aldırmıştır. Adli bilişim uzmanınca hazırlanan 29/6/2017 tarihli bilirkişi raporunda, başvurucunun adına kayıtlı olan ve kullandığı 0533....2 numaralı GSM hattı ile 11/8/2014 ve

9/5/2015 tarihleri arasında 99 farklı günde ByLock sunucuları/sistemlerine ait 46.166.160.137, 46.166.164.176, 46.166.164.177 ve 46.166.164.181 No.lu IP numaraları ile iletişim kurduğu, belirtilen IP numarası üzerinden belirtilen tarih aralığında ByLock sistemine 119.451 kez erişim sağladığı belirtilmiştir.

39. Bölge Adliye Mahkemesi 19/10/2017 tarihinde istinaf istemini esastan reddetmiştir. Mahkeme kararında ByLock delilinin hukuka aykırı şekilde elde edildiğine ilişkin iddialar da değerlendirilmiştir. Kararda, Anayasa'nın 22. maddesinin son fıkrasında yer alan *"İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."* hükmü uyarınca MİT'in istisna kurumlardan kabul edildiği, ayrıca ByLock delilinin elde edilmesinde MİT'in 2937 sayılı Kanun'un 6. maddesinin (d) ve (g) bentleri ile 4. maddesinin (i) bendi kapsamında verilen yetkileri kullandığının açık olduğu ifade edilmiştir. Kararda ByLock iletişim sisteminin FETÖ/PDY mensuplarının kullanmaları amacıyla oluşturulan ve münhasıran bu örgütün mensupları tarafından kullanılan bir ağ olduğu, bu nedenle örgüt talimatı ile bu ağa dâhil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti hâlinde kişinin örgütle bağlantısını gösteren delil sayılacağı belirtilmiştir. Bunun yanı sıra somut olayda sadece FETÖ/PDY mensuplarının kullanması amacıyla oluşturulan ve münhasıran bu suç örgüt mensupları tarafından kullanıldığı tespit edilen ByLock iletişim sistemine, bu özelliğini bilerek dâhil olan ve birçok kez kullanan başvurucunun inkâra dayanan savunmalarına itibar edilmeyerek dosya içinde bulunan diğer delillerle birlikte FETÖ/PDY'ye üye olduğu sonucuna ulaşan ilk derece mahkemesinin değerlendirmesinde isabetsizlik olmadığı belirtilmiştir.

40. Başvurucu temyiz başvurusunda bulunmuş, Yargıtay 16. Ceza Dairesi 4/6/2018 tarihinde Mahkemenin mahkûmiyet kararına yönelik istinaf istemini reddeden Bölge Adliye Mahkemesi kararını onamıştır. Nihai karar başvurucu müdafiine 25/7/2018 tarihinde tebliğ edilmiştir.

41. Başvurucu 26/7/2018 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

1. İlgili Mevzuat

42. 5271 sayılı Kanun'un *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* kenar başlıklı 134. maddesinin olay tarihinde yürürlükte bulunan hâli şöyledir:

> *"(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

43. 5271 sayılı Kanun'un *"İletişimin tespiti, dinlenmesi ve kayda alınması"* kenar başlıklı 135. maddesinin olay tarihinde yürürlükte olan hâlinin ilgili kısmı şöyledir:

"(1) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...) dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır.

...

(8) Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

...

16. (Ek: 2/12/2014-6572/42 md.) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),"

44. 5271 sayılı Kanun'un *"Cumhuriyet savcısının görev ve yetkileri"* kenar başlıklı 161. maddesinin ilgili kısmı şöyledir:

"(1) Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir; yukarıdaki maddede yazılı sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. ..

...

(4) Diğer kamu görevlileri de, yürütülmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri, talep eden Cumhuriyet savcısına vakit geçirmeksizin temin etmekle yükümlüdür."

45. 2937 sayılı Kanun'un 4. maddesinin olay tarihinde yürürlükte bulunan hâlinin ilgili kısmı şöyledir:

"Milli İstihbarat Teşkilatının görevleri şunlardır:

a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

...

i) Dış istihbarat, milli savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak."

46. 2937 sayılı Kanun'un 6. maddesinin ilgili kısmı şöyledir:

"Milli İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

a) Yerli ve yabancı her türlü kurum ve kuruluş, tüm örgüt veya oluşumlar ve kişilerle doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.

b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

...

d) Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir.

...

g) Telekomünikasyon kanallarından geçen dış istihbarat, milli savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir."

47. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun *"Genel ilkeler"* kenar başlıklı 4. maddesi şöyledir:

"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

48. 6698 sayılı Kanun'un *"İstisnalar"* kenar başlıklı 28. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

...

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

..."

49. 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun BTK'nın görev ve yetkilerini düzenleyen *"Kurumun görev ve yetkileri"* kenar başlıklı 6. maddesinin birinci fıkrasının ilgili kısmı şöyledir:

"c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

...

ı) Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak,

..."

50. 5809 sayılı Kanun'un *"Kişisel verilerin işlenmesi ve gizliliğin korunması"* kenar başlıklı 51. maddesinin ilgili kısmı şöyledir:

"(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

...

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir..."

51. 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in (Yönetmelik) *"Kişisel verilerin işlenmesine ilişkin ilkeler"* kenar başlıklı 4. maddesinin (1) numaralı fıkrası şöyledir:

> *"Kişisel verilerin;*
>
> *a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,*
>
> *b) İlgili kişinin rızasına dayalı olarak işlenmesi,*
>
> *c) Elde edilme amacıyla bağlantılı, yeterli ve orantılı olması,*
>
> *ç) Doğru olması ve gerektiğinde güncellenmesi,*
>
> *d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi esastır."*

52. Yönetmelik'in *"Haberleşmenin gizliliği"* kenar başlıklı 7. maddesinin (1) numaralı fıkrası şöyledir:

> *"Elektronik haberleşme ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve gözetimi yasaktır."*

53. Yönetmelik'in *"Trafik verisinin bildirilmesi"* kenar başlıklı 10. maddesi şöyledir:

> *"Trafik verisi, arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü, tüketici şikâyetlerinin değerlendirilmesi ve denetim faaliyetlerinin gerçekleştirilmesi amacıyla yazılı olarak talep edilmesi halinde kanunların yetkili kıldığı mercilere verilir."*

54. Yönetmelik'in *"İşletmecilerin veri saklama süreleri"* kenar başlıklı 14. maddesinin (2) numaralı fıkrası şöyledir:

> *"Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler, ilgili süreç tamamlanıncaya kadar saklanır."*

2. İlgili Yargı Kararları

55. Anayasa Mahkemesi 5809 sayılı Kanun'un 51. maddesinin (2) numaralı fıkrasında yer alan *"...ilgili mevzuatın ve..."*, (6) numaralı fıkrasında yer alan *"...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..."* ve (8) numaralı fıkrasının ikinci cümlesinde yer alan *"...ilgili mevzuatın ve..."* ibareleri ile (13) numaralı fıkrasının Anayasa'ya aykırılık iddiasını incelemiş; söz konusu düzenlemelerin Anayasa'nın kişisel verilerin korunmasını isteme hakkını güvence altına alan 20. maddesine aykırı olmadığına karar vermiştir (AYM E.2015/61, K.2016/172, 2/11/2016). Anayasa Mahkemesinin söz konusu kararının ilgili kısmı şöyledir:

"191. Anayasa'nın 20. maddesinin üçüncü fıkrasında, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu; bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtildikten sonra kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla düzenleneceği hüküm altına alınmıştır. Böylece kişisel verilerin korunması hakkı anayasal güvenceye bağlanmıştır.

192. Kişisel verilerin korunması hakkı, insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Anayasa'nın 20. maddesinin üçüncü fıkrası uyarınca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Türkiye'nin taraf olduğu 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Ancak bu sınırlamalar, Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı gibi hak ve özgürlüklerin özlerine de dokunamaz.

193. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri ve bilgilerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hâle getirilebilir.

194. Kanun'un 51. maddesinin (2) numaralı fıkrasında, elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin esas olduğu ifade edildikten sonra, dava konusu kuralla 'ilgili mevzuatın' öngördüğü durumlar istisna tutularak, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır. Böylece, kişisel verilerin işlenmesi kural olarak yasaklanmış olmakla beraber ilgili mevzuatın öngördüğü durumlarda haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi mümkün kılınmıştır.

195. Anayasa'nın 20. maddesinin üçüncü fıkrasında, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin rızasıyla işlenebilmesine olanak tanınmış, Anayasa Mahkemesinin yukarıda anılan 9.4.2014 tarihli ve E.2013/122, K.2014/74 sayılı kararında da bu husus teyit edilerek kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği ifade edilmiştir. Anayasa'nın 20. maddesinin açık hükmü ve Anayasa Mahkemesinin anılan kararı gözetildiğinde, kanunla bir belirleme ve sınırlama yapılmaksızın yürütmenin düzenleyici işlemleriyle haberleşmeye ilişkin kişisel verilerin işlenmesine anayasal açıdan olanak bulunmamaktadır. Bu bağlamda, elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda yer alan 'ilgili mevzuat' ibaresiyle de kişisel verilerin işlenmesiyle ilgili düzenlemeler öngören diğer kanun hükümlerinin kastedildiği anlaşılmaktadır. Nitekim, kuralın gerekçesinde de Anayasa'nın 20. maddesi uyarınca kişisel verilerin işlenmesi konusunun kanunla düzenlenmesi gerektiğinden elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğine yönelik hususlara ilişkin olarak yeni bir kanun tasarısı

hazırlandığı ifade edilmiştir. Ayrıca kişisel verilerin korunması konusunda çerçeve kanun niteliği taşıyan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinin (1) numaralı fıkrasında da, kişisel verilerin ancak kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hüküm altına alınmıştır.

196. Dolayısıyla, kuralda yer alan 'ilgili mevzuat' kavramı, elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesiyle ilgili yasal düzenlemeleri ifade ettiğinden, dava konusu kuralda, kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenlenmesini öngören Anayasa'nın 20. maddesine aykırı bir yön bulunmamaktadır.

197. Günümüzde, milli güvenlik, istihbarat, suçla mücadele gibi çok farklı nedenlerle kişisel verilerin işlenmesine ihtiyaç duyulabilmektedir. Ayrıca zaman içerisinde gelişen teknolojiyle birlikte bu konuda yeni kanuni düzenlemeler yapılması da gerekebilir. Bu nedenle, haberleşmeye ilişkin kişisel verilerin hangi durumlarda işlenebileceğinin kanunla tek tek sayılmak suretiyle belirlenmesi mümkün değildir. Dava konusu kuralda da genel bir belirleme yapılarak haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğu hüküm altına alındıktan sonra, elektronik haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanıyan ilgili kanun hükümleri saklı tutulmuştur.

198. Diğer taraftan, dava konusu kuralla, konuyla ilgili kanunlarda haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanınmakla birlikte bu konuda kanun koyucunun sınırsız bir takdir yetkisi bulunmamaktadır. Nitekim, 5809 sayılı Kanun'un 51. maddesinin (1) numaralı fıkrasında, kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulması gerektiği belirtilmiş, Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde de, benzer ilkelere yer verilerek kişisel verilerin işlenmesinde gözetilmesi gereken hususlar ayrıntılı bir şekilde düzenlenmiştir. Dolayısıyla, dava konusu kuralın kişisel verilerin işlenmesi noktasında kanun koyucuya sınırsız bir takdir hakkı verdiği söylenemez.

199. Bu itibarla, ilgili kanunların öngördüğü durumlarda, haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda belirsizlik bulunmadığı gibi, kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçüsüz şekilde sınırlandıran bir husus bulunmamaktadır.

200. Açıklanan nedenlerle kural, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir."

56. Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararında *ByLock iletişim sistemindeki veri tespitlerinin hangi koruma tedbiri kapsamında incelenmesi gerektiğine* ilişkin olarak yapılan açıklamalar şöyledir:

"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri, CMK'nun 134. maddesinde düzenlenmiştir. Bu koruma tedbiri, CMK'nun 116 ve 134. maddeleri arasında düzenlenen 'arama' ve 'elkoyma' koruma tedbirlerinin özel bir görünümünü oluşturmaktadır.

...

Bilgisayar kütüklerinin sadece hard disk şeklinde anlaşılmaması gerekir. Bilgisayar kütükleri, internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP no'larını ve diğer erişim bilgilerini depoladıkları veri tabanlarını da ifade etmekte[dir] ...

Nitekim Adli ve Önleme Aramaları Yönetmeliğinin 'bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' başlıklı 17. maddesinin yedekleme işlemini düzenleyen üçüncü fıkrası; yedekleme işleminin, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanacağını düzenlemiştir. Yönetmelikte yer alan "Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır' ibaresi ile olay yerindeki bilgisayarların yanı sıra uzak bilgisayar kütüklerine de erişim sağlanabilecektir.

...

... [İ]nternet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından, bu iletişim kayıtları hakkında CMK'nun 134. maddesinin birinci fıkrası gereğince arama, kopyalama ve elkoyma koruma tedbirleri uygulanabilir..."

B. Uluslararası Hukuk

1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

57. Birleşmiş Milletler Genel Kurulunun 10/12/1948 tarihli ve 217 (111) sayılı kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi şöyledir:

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfî karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalamaz. Herkesin bu karışmalara ve tecavüzlere karşı kanun ile korunmağa hakkı vardır."

58. Birleşmiş Milletler Genel Kurulu tarafından kişisel verilerin korunması konusunda kabul edilen 14/12/1990 tarihli ve 45/95 sayılı *"Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler"*de şu temel ilkelere yer verilmiştir:

"1- İşlemenin hukuka uygun ve adil olması ilkesi: Kişilerin hakkındaki veriler hukuka aykırı veya adil olmayan şekilde toplanmamalı veya işlenmemelidir. Ayrıca Birleşmiş Milletler Şartı'ndaki ilkelere aykırı amaçlarla kullanılmamalıdır.

2- Doğruluk ilkesi: Kişisel verileri tutmakla sorumlu makamlar bu bilgilerin doğru tutulmasını güvence altına almalıdır.

3- Belirli ve meşru amaçlar için işleme ilkesi: Bir kaydın tutulması ve kullanımı meşru ve belirli bir amaca dayalı olmalıdır. Bütün kişisel veriler amaç ile ilgili ve onu gerçekleştirmeye elverişli olacak şekilde toplanmalı ve kaydedilmelidir. Bu kişisel verilerin hiçbiri, ilgili kişinin rızası dışında, belirtilenlerle uyuşmayan amaçlar için kullanılamaz veya ifşa edilemez. Kişisel verilen saklanma süresi, belirtilen amaçlara ulaşılmasını sağlayacak süreyi aşamaz.

4- İlgili kişilerin erişmesi ilkesi: Kimlik kanıtı sunan herkes kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve gereksiz bir gecikme veya masraf olmadan anlaşılır biçimde elde etme hakkına sahiptir. Ayrıca bu bilgilerin kanuna aykırı, gereksiz veya yanlış olması durumunda uygun düzeltmelerin yapılmasını veya silinmesini talep etme hakkına sahiptir. Devletler buna uygun bir çözüm yolu sağlamak durumundadır. Herhangi bir düzeltme maliyeti dosyadan sorumlu kişi tarafından karşılanmalıdır. Bu ilke hükümlerinin uyruk veya ikametine bakılmaksızın herkes için uygulanması arzu edilir.

5- Ayrımcılığın önlenmesi ilkesi: (6) numaralı ilkede kısıtlı olarak öngörülen hâller söz konusu olduğunda ırk veya etnik köken, renk, cinsel yaşam, siyasi görüş, dini, felsefi ve diğer inançların yanı sıra dernek veya sendika üyeliği bilgileri de dahil olmak üzere kanuna aykırı veya keyfi olarak ayrımcılığa yol açabilmesi muhtemel veriler toplanmamalıdır.

6- Üstün amaçlar için istisna koyabilme ilkesi: Ulusal güvenlik, genel sağlık ve ahlakı korumak veya özellikle zulüm gören kişilerin ve diğerlerinin hak ve özgürlüklerinin korunması amacıyla (1) ila (4) numaralı ilkelerden ayrılabilmek mümkün olabilir. Ancak bu tür istisnalar, sınırlarının açıkça belirlendiği ve uygun tedbirlerin ortaya konulduğu iç hukuk sistemine göre yürürlüğe konan bir kanun veya eşdeğer bir düzenlemede açıkça belirtilmiş olmalıdır.

7- Güvenlik ilkesi: Veri dosyaları, kaza ile kaybetme veya yok etme gibi doğal afetler, hileli verilerin yanlış kullanılması ya da bilgisayar virüsleri gibi insan odaklı tehlikelere karşı uygun tedbirlerle korunmalıdır.

8- Denetleme ve yaptırım ilkesi: Her ülkenin kanunu, yerel hukuk sistemine uygun olarak yukarıda belirtilen ilkelere uyulmasından sorumlu makamı belirler. Bu makam tarafsızlık, veri işleme ve oluşturmadan sorumlu kişilere karşı bağımsızlık ve teknik yeterlilik teminatı sunmalıdır. Yukarıda belirtilen ilkeleri uygulayan ulusal kanun hükümlerinin ihlali durumunda cezai veya diğer idari yaptırımlar uygun bireysel çözümlerle birlikte öngörülmüş olmalıdır.

9- Sınır ötesi veri transferi ilkesi: Sınır ötesi bir veri akışı ile ilgili olarak iki veya daha fazla ülkenin mevzuatı mahremiyetin korunması için karşılaştırılabilir güvenceler sunduğu takdirde veri dolaşımı mümkün kılınabilir."

2. Avrupa Birliği Genel Veri Koruma Tüzüğü

59. 27/4/2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün *"Tanımlar"* kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Bu Tüzük'ün amaçları doğrultusunda, aşağıdaki tanımlar geçerlidir:

Kişisel veri, belirli veya belirlenebilir bir gerçek kişi hakkındaki her bilgiyi ifade eder (veri sahibi); belirlenebilir bir gerçek kişi ad, kimlik, yer bilgisi, online kimlik veya kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliği gibi belirleyici bir özellikle doğrudan veya dolaylı olarak belirlenebilen kişidir.

İşleme, kişisel veri veya kişisel veri dizisinin otomatik veya başka bir şekilde toplanması, kaydedilmesi, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, kullanılması, iletim yoluyla açıklanması, yayılması veya erişilebilir hâle getirilmesi, sıralanması veya kombine edilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi yollarla herhangi bir işlem veya işlem dizisine tabi tutulması anlamına gelir."

60. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün *"Kişisel verilerin işlenmesi ile ilgili ilkeler"* kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kişisel veri;

Veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir (hukuka uygunluk, adillik ve şeffaflık),

Belirlenmiş, açık ve meşru amaçlar için toplanmış olmalı ve bu amaçlara uygun olmayan bir şekilde işlenmemelidir. Kamu yararı, bilimsel ve tarihsel amaçlar ya da arşivleme amacıyla yapılacak diğer işlemler madde 89/1 uyarınca başlangıç amaçlarıyla uyumsuz kabul edilmeyecektir (amaç sınırlaması)

Yeterli, ilgili ve işlendiği amaçlar için gerekli olanlarla sınırlı işlenmelidir (verilerin en az seviyeye indirilmesi)

Doğru ve gerektiğinde güncel tutulmalı; hatalı olan kişisel verinin işlenme amacına bakılmaksızın gecikmeden silinmesini veya düzeltilmesini sağlamak için makul her adım atılmalıdır (doğruluk).

İşlenme amacı için gerekenden daha uzun olmayan bir süre boyunca veri konularının tanımlanmasına izin veren bir formda tutulmalıdır. Kişisel veriler, veri sahibinin hak ve özgürlüklerini korumak için bu Tüzüğün öngördüğü uygun teknik ve yapısal tedbirler alınmak kaydıyla Tüzüğün 89/1. maddesi uyarınca sadece kamu yararına, bilimsel veya tarihi araştırma amaçlarına ya da istatistiki amaçlara yönelik olarak arşivleme amacıyla daha uzun bir süre saklanabilir (saklama süresinin sınırlandırılması).

Yetkisiz veya kanun dışı işlemeye ve kazara kayıp, imha ve hasara karşı uygun teknik veya yapısal tedbirler alınarak kişisel verilerin güvenli bir biçimde işlenmesi sağlanmalıdır (bütünlük ve gizlilik)."

61. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün *"Kısıtlamalar"* kenar başlıklı 23. maddesinin ilgili kısmı şöyledir:

"Veri sorumlusunun veya işleyenin tabi olduğu Birlik veya Üye Devlet hukuku, 12. ila 22. (bunlara karşılık geldiği sürece 5. madde) ve 34. maddelerdeki yükümlülükleri ve hakların kapsamını, temel hak ve özgürlüklerin özüne saygı gösterdiğinde ve demokratik bir toplumda korunmak için gerekli ve orantılı bir tedbir olduğu takdirde aşağıdaki hallerde kanun yoluyla sınırlayabilir:

Ulusal güvenlik,

Savunma,

Kamu güvenliği,

Kamu güvenliğine yönelik tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması veya cezaların infazı.

Birliğin veya Üye Devletin genel olarak kamu yararına olan diğer önemli hedeflerin, özellikle para, bütçe, önemli bir vergilendirme, kamu sağlığı veya sosyal güvenlik dahil olmak üzere önemli bir ekonomik veya mali çıkar amacıyla,

Yargı bağımsızlığının ve yargısal işlemlerin (sürecin) korunması,

Regüle edilmiş meslekler için etik ihlallerin önlenmesi, tespiti, soruşturulması ve kovuşturulması,

(a) ila (e) ve (g) maddelerinde atıfta bulunulan hallerde resmi otoritenin kullanımına zaman zaman bağlı olsa bile izleme, inceleme veya düzenleyici işlevin yerine getirilmesi,

Veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması,

Medeni hukuk hak ve alacaklarının icrası,

Özellikle 1. paragrafta atıfta bulunulan herhangi bir hukuki tedbir öngören kanun en azından uygun olduğu hallerde şu belirli hükümleri içermelidir:

İşleme veya işleme kategorilerinin amaçları,

Kişisel veri kategorileri,

Tanınan kısıtlamaların boyutu,

Keyfi veya hukuk dışı erişimin ya da aktarımın önlenmesine dair güvenceler,

Sorumlunun veya sorumlu kategorilerinin belirlenmesi,

Depolama dönemleri ve işlemenin niteliği, kapsamı ve amaçları veya işleme kategorileri dikkate alınarak uygulanabilir güvenceler,

Veri sahibinin hakları ve özgürlüklerine getirilen riskler,

Veri sahibinin, amacına halel getirmediği sürece kısıtlama hakkında bilgilendirilmesi."

3. Avrupa İnsan Hakları Sözleşmesi

62. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) *"Özel ve aile hayatına saygı hakkı"* kenar başlıklı 8. maddesinin ilgili kısmı şöyledir:

"(1) Herkes .... yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

4. Avrupa Konseyi Siber Suç Sözleşmesi

63. Türkiye Cumhuriyeti tarafından 10/11/2010 tarihinde imzalanan ve Türkiye Büyük Millet Meclisi tarafından onaylanması uygun bulunarak 2/5/2014 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi'nin *"Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması"* kenar başlıklı 32. maddesi şöyledir:

"Bir taraf, diğer tarafın izni olmaksızın; a) Halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine bunların coğrafi konumuna bakılmaksızın erişilebilir; veya b) Kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişebilir veya bunları temin edebilir."

5. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

64. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin *"Tanımlar"* kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"Bu Sözleşmenin amaçları bakımından:

a "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder.

...

c "Otomatik işlem"den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/ veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."

65. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin *"Verilerin niteliği"* kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;

b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;

c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;

d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;

e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır."

66. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin *"İstisnalar ve kısıtlamalar"* kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması."

6. Avrupa İnsan Hakları Mahkemesi İçtihadı

a. Olağan Hukuk Yollarının Tüketilmesi Kuralı Yönünden

67. Avrupa İnsan Hakları Mahkemesi (AİHM) *Hambardzumyan/Ermenistan* (B. No: 43478/11, 5/12/2019) kararında ceza soruşturması kapsamında başvurulan gizli dinleme tedbirinin haberleşme hürriyetini ihlal ettiği iddiasının ceza yargılamasının sonuçlanmasından sonra bireysel başvuruya konu edilmesini başvuru süresi açısından tartışmıştır (*Hambardzumyan/Ermenistan*, §§ 39-55). Başvuruya konu olayda başvurucu, bir ıslahevinin kadınlarla ilgili bölümünün başkan yardımcısı olarak çalışmakta iken ıslahevinde kalan bir mahkûmun başvurucunun kendisinden rüşvet istediği ihbarında bulunması üzerine başvurucunun görüntülü ve sesli izleme altına alınmasına, telefonlarının dinlenmesine 3/2/2010 tarihinde hâkim tarafından karar verilmiştir. Bu suretle elde edilen delillere istinaden başvurucu hakkında ceza davası açılmıştır. Başvurucunun avukatı 12/5/2010 tarihinde 3/2/2010 tarihli karardan haberdar olmuştur. Başvurucu gerek ceza mahkemesinde gerekse temyizde gizli dinleme ve izleme kararının hukuka aykırı olduğunu ileri sürmüş, derece mahkemeleri de başvurucunun bu iddiasını esastan tartışmıştır. Başvurucu 9/11/2010 tarihinde 9 yıl hapis cezasına mahkûm olmuş, ceza 28/4/2011 tarihinde kesinleşmiştir (*Hambardzumyan/Ermenistan*, §§ 5-22).

68. Başvurucu ceza yargılamasının kesinleşmesinden sonra AİHM'e yaptığı bireysel başvuruda gizli izleme tedbiri sebebiyle Sözleşme'nin 8. maddesinin ihlal edildiğini öne sürmüştür (*Hambardzumyan/Ermenistan*, § 35). Hükûmet başvurucunun tedbirden haberdar olduğu 12/5/2010 tarihinden itibaren altı ay içinde bireysel başvuruda bulunması gerektiği itirazında bulunmuş, ceza yargılamasında delilin hukuka aykırılığının ileri sürülmesinin 8. madde bağlamında etkili bir yol olamayacağını belirtmiştir (*Hambardzumyan/Ermenistan*, § 37). AİHM sadece etkili olan hukuk yollarının tüketilmesinin zorunlu olduğunu belirtmiş (*Hambardzumyan/Ermenistan*, § 40), etkili bir başvuru yolunun bulunmadığı veya var olan yolun etkisiz olduğu kanaatine varıldığı hâllerde başvuru süresinin kural olarak şikâyet edilen fiilin/işlemin gerçekleştiği tarihten itibaren işlemeye başlayacağını ifade etmiştir (*Hambardzumyan/Ermenistan*, § 41).

69. AİHM başvurucunun suçluluğu hakkında karar veren mahkemenin Sözleşme'nin 8. maddesiyle ilgili şikâyet için etkili bir giderim sağlamaya muktedir olmadığını vurgulamıştır. AİHM'e göre ceza mahkemeleri delilin kabul edilebilirliğiyle ilgili sorunları incelemeye yetkili olsalar da başvurucunun özel hayatına ve haberleşmesine saygı hakkına yapılan müdahalenin kanuni dayanağının bulunup bulunmadığı ya da demokratik toplumda gerekli olup olmadığı şikâyetinin incelenmesi ceza mahkemelerinin yetki alanının dışındadır. Ayrıca bu mahkemeler bu şikâyetle ilgili olarak uygun giderim sağlama niteliğini de haiz değildir (*Hambardzumyan/Ermenistan*, § 43). Bu sebeple gizli izleme meselesinin başvurucu aleyhine açılan ceza davasının esasını inceleyen mahkemelerde ileri sürülmesi Sözleşme'nin 8. maddesiyle ilgili şikâyetler için etkili yol olarak görülemez (*Hambardzumyan/Ermenistan*, § 44).

70. Daha sonra AİHM etkili olmadığını tespit ettiği ceza davasından sonra başvuru yapılmış olmasının altı ay kuralıyla bağdaşıp bağdaşmadığını incelemiştir. AİHM başvurucunun gizli izleme kararından soruşturmanın son evrelerinde -dinleme sonucu elde edilen delillerin onun aleyhine olan suçlamanın dayanağı olarak gösterildiği iddianameden kısa bir süre sonra- dosyaya erişim imkânının sağlandığından haberdar olduğunun altını çizmiştir. AİHM olayın arka planı gözetildiğinde başvurucunun bu şikâyetini ceza mahkemesi önünde dile getirmesinin gayrimakul olmadığını kabul etmiştir. AİHM'e göre

derece mahkemelerinin gerçekte başvurucunun bu şikâyetini incelemiş olması bu sonucu desteklemektedir. Derece mahkemeleri, izleme tedbirinin hukukiliği iddiasıyla ilgili olarak yaptıkları incelemede Sözleşme şikâyetinin esasıyla ilgili değerlendirmelerde bulunmuştur. Bu koşullarda başvurucu, şikâyetini -hatalı olarak- etkili olduğunu düşündüğü bir hukuk yolunda derece mahkemelerinin dikkatine sunmuş olması sebebiyle suçlanamaz (*Hambardzumyan/Ermenistan*, § 52).

71. AİHM sonuç olarak Sözleşme'nin kurduğu koruma mekanizmasının insan haklarını güvence altına alan ulusal hukuk sistemine nazaran ikincil nitelikte olduğu ilkesine saygı gösteren başvurucunun ihlalin ulusal hukuk sistemi içinde düzeltilmesi fırsatını derece mahkemelerine vermek için Sözleşme şikâyetini aleyhine yöneltilen suçlamayla ilgili olarak karar veren ceza mahkemesinde öne sürmüş olmasının mantıksız olmadığını vurgulamış ve hükûmetin süre aşımı itirazını reddetmiştir (*Hambardzumyan/Ermenistan*, §§ 53, 54).

b. Kişisel Verilerin Korunmasını İsteme Hakkı Yönünden

72. AİHM, devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (*Leander/İsveç*, B. No: 9248/81, 26/3/1987, § 59).

73. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması özel hayata saygı hakkına müdahale oluşturur (*Leander/İsviçre*, § 48; *Kopp/İsviçre*, B. No: 23224/94, 25/3/1998, § 53; *Amann/İsviçre* [BD], B. No: 27798/95, 16/2/2000, § 69; *Rotaru/Romanya* [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44, 46).

74. AİHM'e göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel verilerin Sözleşme'nin 8. maddesinde öngörülen unsurlardan birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (*S. ve Marper/Birleşik Krallık* [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

75. AİHM'e göre kişisel verilerin korunması, Sözleşme'nin 8. maddesinde öngörülen özel hayata saygı hakkından kişinin yararlanması konusunda büyük öneme sahiptir. İç hukuk kişisel verilerin bu maddede öngörülen güvencelere uygun olmayan şekilde kullanımını engellemek için gerekli güvenceleri sağlamalıdır. Bu tür güvencelerin bulunmasının gerekliliği; otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda, özellikle de bu verilerin polis tarafından kullanılması hâlinde daha fazla hissedilmektedir. İç hukuk, bu verilerin saklanma amaçlarına uygun ve aşırılıktan uzak olmalarını sağlamalı; verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç hukuk, aynı zamanda kişisel verilerin uygun olmayan şekillerde, keyfî ve yetki aşımı yapılarak kullanılmalarına karşı uygun güvenceler de

içermelidir (*S.ve Marper/Birleşik Krallık*, § 103; *M.M./Birleşik Krallık*, B. No: 24029/07, 13/11/2012, § 195).

c. Haberleşme Hürriyeti Yönünden

76. AİHM kararlarında gizli tedbirlere ilişkin kanun hükümlerinin barındırması gereken asgari unsurlar sıralanmıştır. Bu kapsamda izleme kararı verilmesine yol açabilecek suçların niteliği, iletişimleri izlenecek kişi kategorisi, izleme sürelerinin sınırları, elde edilen verilerin incelenme, değerlendirilme ve saklanmalarına ilişkin esaslar, verilerin başkalarıyla paylaşılmasına ilişkin önlemler ve elde edilen verilerin ortadan kaldırılmasına ilişkin koşulların kanunda açık bir şekilde düzenlenmesi gereklidir (*the Association for European Integration and Human Rights ve Ekimdzhiev/Bulgaristan*, B. No: 62540/00, 28/6/2007, §§ 76, 77).

77. AİHM somut olaya tam olarak benzemeyen ancak ortaya konulan ilkeler bakımından dikkate değer olan *Weber ve Saravia/Almanya* ((k.k.), B. No: 53934/00, 29/6/2006) kararında Almanya İstihbarat Teşkilatına mail, posta ve iletişime müdahale yetkisi tanıyan 1968 tarihli Kanun'da 1994 yılında yapılan değişikliği haberleşme hürriyeti yönünden incelemiştir. Söz konusu kanun stratejik izleme olarak tabir edilen yöntemlerle iletişimi kayıt altına alma ve bu yolla temin ettiği bilgileri yetkili makamlara aktarma yetkisini Alman İstihbarat Teşkilatına tanımaktadır. Anılan Kanun'a göre stratejik izlemenin amacı, Federal Almanya Cumhuriyeti'nin karşılaşabileceği, ülkesine yönelik silahlı saldırı, uluslararası terörist saldırılar ile öteki bazı ağır suçlar gibi ciddi tehlikeleri tespit etmek ve önlemek için iletişimin tespiti ve dinlenmesi yoluyla bilgi toplamaktır. Belli bir kişinin iletişimine müdahale olarak tanımlanan bireysel izleme ise izlenen kişinin işlediğinden veya planladığından şüphelenilen belli ağır suçları önleme veya soruşturma hedefine yöneliktir (*Weber ve Saravia/Almanya* §§ 3-13).

78. Başvurucular söz konusu Kanun'un başka ülkelerin egemenliklerine yasa dışı olarak müdahale edilmesini öngörmesi sebebiyle kanunilik kriterini sağlamadığını ileri sürmüşlerdir. AİHM söz konusu Kanun'un uluslararası kablosuz iletişim şebekelerini izleme yetkisi verdiğini, bunun da sabit telefon hatlarını değil uydu ve radyo ağlarını etkilediğini belirtmiştir. AİHM'e göre yabancı ülkelerden emilen sinyaller Alman topraklarında yerleşik tesislerden izlenmekte ve toplanan veriler Almanya'da kullanılmaktadır. Bu çerçevede başvurucular, Alman otoritelerinin stratejik izleme yöntemini uygulamak suretiyle yabancı devletlerin uluslararası hukukla korunan toprak egemenliklerini ihlal edecek şekilde davrandıklarını gösteren delil ibraz etme yükümlülüklerini yerine getirememişlerdir (*Weber ve Saravia/Almanya*, § 88).

79. Başvurucular Kanun'un öngörülebilir olmadığından da şikâyet etmişlerdir. AİHM'e göre gizli dinleme tedbirinin kendine özgü bağlamındaki öngörülebilirlik, kişinin davranışlarını ayarlayabilmesi amacıyla otoritelerin onun iletişimine ne zaman müdahale edebileceğini öngörmesi gerektiği anlamına gelmemektedir. Ancak özellikle idari otoritelere tanınan yetkinin gizli bir şekilde kullanıldığı hâllerde keyfîlik ihtimali bariz hâle gelmektedir. Bu yüzden özellikle kullanıma açık olan teknolojinin gün geçtikçe daha karmaşık hâle geldiği bu süreçte telefon konuşmalarını dinlemeye ilişkin kuralların açık olması önemlidir. Ulusal hukukun vatandaşların hangi durumlarda kamu otoritelerinin bu tedbiri uygulamaya yetkili olduğunu bilmelerine imkân sağlayacak ölçüde açık olması gerekir. Öte yandan kanun, yetkili otoritelere tanınan takdirin kapsamını ve keyfî müdahalelere karşı koruma sağlamak için nasıl uygulanacağını bireye yeterli açıklıkta göstermelidir (*Weber ve Saravia/Almanya*, §§ 93, 94).

80. AİHM, devletin gizli izleme tedbiri yoluyla ulusal güvenliğini sağlamadaki menfaati ile başvuruculaların özel hayatına saygı hakkına yapılan bu ciddi müdahale arasında denge kurulması bağlamında ulusal otoritelerin ne tür araçları seçecekleri hususunda nispeten geniş bir takdir yetkisine sahip olduklarına işaret etmiştir (*Weber ve Saravia/Almanya*, § 106).

81. AİHM elde edilen bilginin başka kurumlara verilmesine ve kullanılmasına ilişkin olarak ise Alman Anayasa Mahkemesinin iptal kararından sonra yapılan değişikliklerle bunların çok sıkı koşullara bağlandığını belirtmiş, özellikle söz konusu bilginin aktarılması için bunun zorunlu olması gerektiğine ve Alman Anayasa Mahkemesinin bu bilginin elde edilme amacı dışında kullanılmayacağına dair kararına işaret etmiştir (*Weber ve Saravia/Almanya*, §§ 121, 122). AİHM bu bilgilerin Anayasayı Koruma Ofisi ile diğer otoritelere aktarılması ve bunlar tarafından kullanılmasını da incelemiştir. AİHM izlenen kişiler aleyhine ceza soruşturması başlatılmasına imkân sağlamak amacıyla, öncesinde herhangi bir suç şüphesi olmaksızın uygulanan gizli izleme tedbiri ile elde edilen kişisel verilerin transferinin bu kişilerin haberleşmenin gizliliği hakkına yapılan nispeten ciddi bir müdahale olduğunu kabul etmiştir. Bununla birlikte AİHM, stratejik gözetleme yoluyla elde edilen bilginin transferinin sadece kanunda belirtilen ve nispeten ciddi mahiyet taşıyan suçların önlenmesi ve soruşturulması amacıyla sınırlı olduğunu not etmiştir. Ayrıca Alman Anayasa Mahkemesi, iptal kararıyla buna ilişkin güvenceleri sıkılaştırmıştır. Öte yandan bilginin aktarılması kararı, İstihbarat Teşkilatının transfer koşullarının oluşup oluşmadığını değerlendirme konusunda eğitimli olan personeli tarafından verilmektedir. Tüm bu koşulları gözeten AİHM, gözetlemenin konusu olan kişilerin haberleşmenin gizliliği hakkına yapılan müdahalenin gerek suç bakımından makul sınırlamalar getirilmiş olmasıyla gerekse kötüye kullanmaya karşı uygun denetim mekanizmalarının getirilmesiyle dengelendiği sonucuna ulaşmıştır (*Weber ve Saravia/Almanya*, §§ 125-129).

82. AİHM bilginin imha edilmesini de incelemiştir. AİHM kişisel verilerin kanunda öngörülen amaçlar çerçevesinde arşivlenmesine artık ihtiyaç kalmadığının anlaşıldığı anda imhasının ve imha koşullarının oluşup oluşmadığının görece kısa aralıklarla değerlendirilmesinin öngörülmesinin haberleşmenin gizliliğine yapılan müdahalenin etkisinin kaçınılmaz seviyeye kadar azaltılmasında önemli bir unsur oluşturduğuna dikkat çekmiştir. AİHM ayrıca Federal Anayasa Mahkemesinin yargısal süreçler için hâlen ihtiyaç duyulan bilgilerin hemen imha edilemeyeceğine ve kanun kapsamında oluşturulan bağımsız komisyonun denetim yetkisinin imhası da dâhil olmak üzere bilginin kullanılmasına ilişkin bütün süreci kapsadığına karar verdiğine işaret etmiştir (*Weber ve Saravia/Almanya*, § 131).

83. AİHM devletin stratejik gözetleme yetkisinin kötüye kullanılmasına karşı etkili ve yeterli güvencelerin olduğu kanaatine varmış; somut olayda haberleşmenin gizliliğine ulusal güvenliğin sağlanması, suç işlenmesinin önlenmesi amaçlarıyla müdahale edilmesinin demokratik toplumda gereklilik kriterini karşıladığını belirtmiştir. AİHM sonuç olarak başvuruyu açıkça dayanaktan yoksun olması sebebiyle kabul edilemez bulmuştur (*Weber ve Saravia/Almanya*, §§ 137, 138).

V. İNCELEME VE GEREKÇE

84. Mahkemenin 17/9/2020 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Kişi Hürriyeti ve Güvenliği Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

85. Başvurucu, ByLock programını kullandığı gerekçesiyle tutuklanmasının Anayasa'nın 15. ve 19. maddelerine aykırı olduğunu belirterek kişi hürriyeti ve güvenliği hakkının ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

86. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 47. maddesinin (5) numaralı ve İçtüzük'ün 64. maddesinin (1) numaralı fıkraları uyarınca bireysel başvurunun başvuru yollarının tüketildiği, başvuru yolu öngörülmemişse ihlalin öğrenildiği tarihten itibaren otuz gün içinde yapılması gerekmektedir.

87. Bir suç isnadına bağlı olarak tutuklulukla ilgili şikâyetleri içeren bireysel başvurunun hükümle birlikte verilen tutukluluğun devamı kararı sonrasında yapılması hâlinde tutukluluğun devamı kararına itiraz edilmemiş ise kararın verildiğinin öğrenildiği tarihten itibaren, itiraz edilmiş ise itiraz merciince verilen kararın öğrenildiği tarihten itibaren otuz gün içinde yapılması gerekmektedir (*Fırat İşgören*, B. No: 2014/6425, 17/11/2016, § 34).

88. Somut olayda başvurucunun ilk derece mahkemesince hükümle -14/3/2017 tarihli mahkûmiyet kararıyla- birlikte verilen tutukluluğun devamı kararına itiraz ettiğine yönelik bir bilgi ve/veya belge bulunmamaktadır. Bu nedenle başvurunun ilk derece mahkemesinin nihai kararının tefhimle öğrenildiği 14/3/2017 tarihinden itibaren otuz gün içinde yapılması gerekmektedir. Buna göre 26/7/2018 tarihinde yapılan bireysel başvuruda süre aşımı olduğu sonucuna varılmıştır.

89. Açıklanan gerekçelerle başvurunun bu kısmının *süre aşımı* nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkı Kapsamında Kişisel Verilerin Korunmasını İsteme Hakkının ve Haberleşme Hürriyetinin İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

90. Başvurucu, haberleşme araçları ve içeriğinin gizli olması gerektiğini belirtmiş; ByLock haberleşmesinin 5271 sayılı Kanun'un 134. ve 135. maddelerine uyulmadan ele geçirildiğini, ByLock uygulamasının ele geçirilmesi ve kişisel verilerinin ortaya çıkarılışındaki hukuksuzluk nedeniyle kişisel verilerin korunmasını isteme hakkının ve haberleşmenin gizliliğinin ihlal edildiğini iddia etmiştir. Başvurucu bu nedenlerle özel hayata saygı ile kişisel verilerin korunmasını isteme hakları ve haberleşme hürriyetinin ihlal edildiğini ileri sürmüştür.

91. Bakanlık görüşünde; Yargıtay 16. Ceza Dairesinin (E.2015/3, K.2017/3; E.2017/1443, K.2017/4758 sayılı) ve Yargıtay Ceza Genel Kurulunun (E.2017/16.MD-956, K.2017/370 sayılı) kararları ile Anayasa Mahkemesinin *Aydın Yavuz ve diğerleri* kararındaki ByLock iletişim sistemine dair inceleme ve tespitlerin bulunduğu kısımlara yer verilmiştir. Bu kararlara atıfla ByLock iletişim sisteminin kullanımı sonucunda oluşan verilerin tespitinin 5271 sayılı Kanun'un 135. maddesinin birinci fıkrası veya 2937 sayılı Kanun'un 6. maddesinin ikinci fıkrası kapsamında olmayıp 5271 sayılı Kanun'un *"Bilgisayarlarda,*

bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" kenar başlıklı 134. maddesinin birinci fıkrası kapsamında olduğu belirtilmiştir. Bu sebeple 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (i) bendi ile 6. maddesinin birinci fıkrasının (d) ve (g) bentlerine uygun şekilde MİT tarafından elde edilen ByLock'a ilişkin dijital materyaller hakkında Ankara Cumhuriyet Başsavcılığının talebi üzerine 5271 sayılı Kanun'un 134. maddesi gereğince Ankara 4. Sulh Ceza Hâkimliği tarafından verilen *"inceleme, kopyalama ve çözümleme"* kararına istinaden bilgisayar ve bilgisayar kütüklerindeki iletilerin tespiti işleminde herhangi bir hukuka aykırılık bulunmadığı bildirilmiştir. Ayrıca kanuna uygun olarak elde edilen ByLock programına ilişkin verilerin analiz edilmesi neticesinde kullanıcı bilgilerine ulaşıldığı, çalışmanın başlangıcında herhangi bir şahıstan yola çıkılmadığı, diğer bir ifadeyle başlangıçta herhangi bir şahsın kişisel verileri üzerinde çalışma gerçekleştirilmediği belirtilmiştir.

2. Değerlendirme

a. Uygulanabilirlik Yönünden

92. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak *"Özel hayatın gizliliği ve korunması"* kenar başlıklı 20. maddesinin ilgili kısmı şöyledir:

> *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*
>
> ...
>
> *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."*

93. Anayasa'nın 20. maddesinde 7/5/2010 tarihli ve 5982 sayılı Kanun ile yapılan değişikliğe ilişkin madde gerekçesi şöyledir:

> *"Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir."*

94. Anayasa'nın *"Haberleşme hürriyeti"* kenar başlıklı 22. maddesi şöyledir:

> *"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.*
>
> *Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.*

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

95. Anayasa'nın 22. maddesinde herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu hüküm altına alınmıştır. Sözleşme'nin 8. maddesinde de herkesin haberleşmesine saygı gösterilmesini isteme hakkına sahip olduğu düzenlemesine yer verilmiştir (*Yasemin Çongar ve diğerleri*, B. No: 2013/7054, 6/1/2015, § 48).

96. Anayasa ve Sözleşme'nin ortak koruma alanı, haberleşme hürriyetinin yanı sıra içeriği ve biçimi ne olursa olsun haberleşmenin gizliliğini de güvence altına almaktadır. Posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetlerinin haberleşme hürriyeti ve haberleşmenin gizliliği kapsamında değerlendirilmesi gerekir. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması gerekir (*Yasemin Çongar ve diğerleri*, §§ 49, 50).

97. Anayasa Mahkemesi, olayların başvurucu tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (*Tahir Canan*, B. No: 2012/969, 18/9/2013, § 16).

98. Başvurucu; ByLock programını kullanım bilgilerinin yasal olmayan şekilde elde edilmesi nedeniyle haberleşmenin gizliliğinin, haberleşme hürriyetinin ve kişisel verilerin korunmasını isteme hakkının ihlal edildiğini ileri sürmüştür. Bu iddianın incelenebilmesi için öncelikle ByLock programının bir haberleşme aracı olup olmadığının, dolayısıyla bu program üzerinden gerçekleştirilen iletişimlerin haberleşme hürriyeti kapsamında olup olmadığının açıklığa kavuşturulması gerekir.

99. Anayasa Mahkemesi ve Yargıtay kararlarında ByLock programının anlık mesajlaşma, e-posta gönderme, ekleme yoluyla kişi listesi oluşturma, grup içi mesajlaşma, sesli görüşme, görüntü veya belge gönderebilme özellikleri bulunduğu tespit edilmiştir. Yapısı ve yazılım mantığı itibarıyla kişiler arası anlık haberleşmeyi ve birtakım verilerin iletimini sağlayan bir yapıda olduğu açıklanmıştır. ByLock uygulamasına erişim sağlanabilmesi için online (çevrim içi) bağlantı gereklidir, uygulama çevrim dışı kullanımı desteklememektedir. Diğer bir ifadeyle kullanıcılar internet bağlantısını sağlayarak mesaj, mail ve veri aktarımı gerçekleştirebilmektedir (Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararı; *Ferhat Kara*, §§ 42-54). Tüm bu özellikleri nedeniyle ByLock programının online haberleşme programı olduğu konusunda kuşku yoktur. Haberleşme hürriyetinin posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetlerini içerdiği dikkate alındığında ByLock haberleşme programı üzerinden yapılan iletişimin de haberleşme hürriyeti kapsamında değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

100. Anayasa'nın özel hayata saygı hakkını düzenleyen 20. maddesinin üçüncü fıkrasında; herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme, bu veriler hakkında bilgilendirilme, verilere erişme, bunların düzeltilmesini veya silinmesini talep etme, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne yer verilerek anayasal sınırlar belirlenmiştir. Söz konusu Anayasa hükmünde kişilerin kendileri hakkındaki verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu özellikle vurgulanmıştır.

101. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamındaki bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale veya sınırlamalara karşı güvence getirdiği anlaşılmaktadır.

102. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alınarak Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir gerçek veya tüzel kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmiştir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; *Bülent Kaya* [GK], B. No: 2013/2941, 11/5/2016, § 49; *Fatih Saraman*, [GK], B. No: 2014/7256, 27/2/2019, § 57).

103. Bununla birlikte bir başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir.

104. Anayasa Mahkemesinin *Ferhat Kara* kararında belirtildiği üzere suç isnadı altındaki kişilerin adli soruşturma ve kovuşturmalar kapsamında el konulan cihazlarında tespit edilen ByLock programına dair kurulum dosyası vs. dijital veriler dışında ByLock verileri esas olarak iki kaynağa dayanmaktadır. Bunlardan ilki MİT'in adli makamlara ilettiği ve adli makamların mahkeme kararlarıyla üzerinde inceleme yaptığı ByLock sunucusundan elde edilen verilerdir. İkincisi ise ByLock sunucusuna ait hedef IP'lere Türkiye'den hangi IP'lerden erişildiğine ilişkin olarak mahkeme kararıyla BTK'dan elde edilen CGNAT kayıtlarıdır (*Ferhat Kara,* § 58). Cumhuriyet Başsavcılıkları ve mahkemelerin talebi üzerine BTK, ByLock IP'sine bağlanan numaraların abonelerine ait şahıs *kimlik bilgilerini* tespit ederek Başsavcılık ve mahkemelere bildirmiştir (*Ferhat Kara,* §§ 32-38). Anayasa Mahkemesi kararlarında haberleşme trafik bilgisi kapsamında yer alan IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve abone kimlik bilgilerinin *kişisel veri* olduğu belirtilmiştir (AYM, E.2014/149, K.2014/151, 2/10/2014).

105. Bu durumda kişinin telefon ve internet kullanımı, bağlandığı IP adresleri bilgisi, gönderdiği mail, mesaj ve arama kayıt bilgilerinin, dolayısıyla ByLock haberleşme programını kullandığına ilişkin verilerin toplanmasının hem özel hayata saygı hakkının içinde yer alan kişisel verilerin korunmasını isteme hakkının hem de haberleşme hürriyetinin kapsamında olduğu sonucuna varılmıştır. Bu nedenle başvurucunun ByLock kullanımını tespit eden belgelerin yasal olmayan şekilde elde edildiği yönündeki iddiasının hem kişisel veriler hem de haberleşmeyle sıkı bağlantısı dikkate alınarak kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyeti kapsamında incelenmesi gerektiği değerlendirilmiştir.

b. Kabul Edilebilirlik Yönünden

106. Mevcut başvuruda öncelikle başvurunun süresi içinde yapılıp yapılmadığının incelenmesi gerekir.

107. 6216 sayılı Kanun'un 47. maddesinin (5) numaralı fıkrası ile İçtüzük'ün 64. maddesinin (1) numaralı fıkrası uyarınca başvuru yollarının tüketildiği tarihten, başvuru yolu öngörülmemiş ise ihlalin öğrenildiği tarihten itibaren otuz gün içinde bireysel başvuruların yapılması gerekmektedir (*Bilent Aktaş ve diğerleri*, B. No: 2014/19389, 7/12/2016, § 11). Buna göre Anayasa'da güvence altına alınmış temel hak ve özgürlüklerden Sözleşme kapsamındaki herhangi birinin ihlaline neden olduğu ileri sürülen işlem, eylem ya da ihmale ilişkin otuz günlük bireysel başvuru süresi; söz konusu işlem veya eylem için herhangi bir başvuru yolunun kanunlarda öngörülmüş olması hâlinde bu yolun tüketilmesinden sonra verilen nihai kararın öğrenilmesinden, buna karşılık söz konusu işlem veya eyleme ilişkin olarak kanunlarda herhangi bir başvuru yolunun öngörülmemiş olması durumunda işlemin tesis edildiği ya da eylemin ika edildiği tarihten itibaren işlemeye başlayacaktır.

108. Bir başvuru yolunun tüketilmesi gereğinden söz edilebilmesi için bu hukuki yolun iddia edilen ihlalin sonuçlarını giderici, etkili ve başvurucu açısından makul bir çabayla ulaşılabilir nitelikte olması ve sadece teoride kalmayıp fiilen de işlerliği olması gerekmektedir. İhlalin sonuçlarını düzeltici bir vasıf taşımayan veya aşırı ve olağan olmayan birtakım şekli koşulların öngörülmesi nedeniyle fiilen erişilebilir ve kullanılabilir olmaktan uzaklaşan başvuru yollarının tüketilmesi zorunluluğu bulunmamaktadır (*Fatma Yıldırım*, B. No: 2014/6577, 16/2/2017, § 39). Bununla birlikte soyut olarak makul bir başarı sunma kapasitesi bulunan bir yolun uygulamada başarıya ulaşmayacağına dair şüphe, o başvuru yolunun tüketilmemesini haklı kılmaz (*Sait Orçan*, B. No: 2016/29085, 19/7/2017, § 36).

109. Başvurucunun başvuru yollarının tüketilmesi noktasında kendisinden beklenebilecek her şeyi yerine getirip getirmediğinin başvurunun özellikleri dikkate alınarak incelenmesi gerekir (*S.S.A.*, B. No: 2013/2355, 7/11/2013, §§ 27, 28). Ancak somut olayın koşulları itibarıyla başvuru yollarının tüketilmesinin yarar sağlamayacağının veya etkili olmadığının anlaşılması hâlinde anılan yollar tüketilmeden yapılan bir başvuru incelenebilir (*Şehap Korkmaz*, B. No: 2013/8975, 23/7/2014, § 33). Öte yandan başvuru yollarının tüketilmesi, çok katı olarak uygulanması gereken mutlak bir kural değildir. Teorik düzeyde var olan bir başvuru yolunun tüketilmesinin somut olayın koşullarında başvurucuya aşırı külfet yüklemesi hâlinde bu yolun tüketilmesinin gerekli olmadığına karar verilebilir (*Rasul Kocatürk*, B. No: 2016/8080, 26/12/2019, § 38).

110. Somut olayda başvurucunun ByLock haberleşme programını kullandığına ilişkin verilerin hukuka aykırı olarak elde edilmesi sebebiyle kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiği iddiası, başvurucu aleyhine yürütülen ve ByLock programı üzerinden elde edilen verilerin delil olarak kullanıldığı ceza yargılamasında ileri sürülmüş; ceza yargılamasının sonuçlanmasından sonra 26/7/2018 tarihinde bireysel başvuruya konu edilmiştir. Başvurucu aleyhine yürütülen ceza yargılamasında ceza mahkemesi, ByLock kullanım bilgilerine ulaşılmasının ve buradan elde edilen verilerin kullanılmasının haberleşme hürriyeti ile kişisel verilerin korunmasını isteme hakkını ihlal edip etmediğine yönelik bir denetim yapmayacağı gibi herhangi bir ihlal bulunması hâlinde uygun giderim sağlama yetkisine de sahip değildir. Bu sebeple başvurucu

aleyhine yürütülen ceza yargılamasının ByLock haberleşme programına ilişkin bilgilerin elde edilmesi ve kullanılmasının kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetini ihlal ettiği iddiası yönünden etkili bir başvuru yolu olarak kabul edilmesi zordur.

111. Buna karşılık ceza yargılamasının sözü edilen şikâyet yönünden etkisiz olması ceza yargılamasının sonuçlanmasından sonra yapılan bireysel başvurunun süresinde olmadığı hükmüne varılması için tek başına belirleyici bir unsur değildir. Bireysel başvuru süresine ilişkin olarak yorum yapılırken somut olayın tüm koşulları gözönünde bulundurulmalı ve başvurucuya aşırı külfet yüklenmemesine özen gösterilmelidir. Bu bakımdan kanunda öngörülen başvuru yolunun ihlali tespit etme ve uygun giderim sağlama kapasitesini haiz olup olmadığının tereddütlü olduğu, başvurucunun söz konusu başvuru yolundan netice elde edebileceğine dair beklentiye sahip olmasını haklı kılan nedenlerin bulunduğu hâllerde ilgili mekanizmanın tüketilmesinden sonra yapılan başvuruların süresinde olduğu kabul edilebilir. Anayasal şikâyete ilişkin olarak etkililiği hususunda tereddüt bulunan bir başvuru yolu dışında başkaca bir mekanizmanın bulunmadığı hâllerde ilgilinin etkililiği hususunda tereddüt bulunan yolu tükettikten sonra bireysel başvuruda bulunması durumunda başvuru süresiyle ilgili olarak daha esnek davranılmasını haklılaştıran güçlü nedenler bulunmaktadır. Zira asıl olan, ihlalin Anayasa Mahkemesinden önce olağan başvuru yolları kullanılarak tespit edilmesi ve giderilmesidir. Diğer taraftan Anayasa'nın 40. maddesi Anayasa'da güvence altına alınan hak ve özgürlüklere ilişkin ihlalleri tespit edecek ve giderecek hukuksal mekanizmalar oluşturma yükümlülüğünü devlete yüklemektedir. İlgilinin ikincil bir fonksiyona sahip olan Anayasa Mahkemesine başvuru yolunu kullanmasından önce ihlal iddiasını olağan hukuk yollarında öne sürmesi, ihlalin tespiti ve giderilmesi fırsatını öncelikle olağan hukuk mekanizmalarına tanıması anlaşılabilir bir durumdur.

112. Türk hukukunda iletişimin denetlenmesi ve sonrasında ceza davası açılması durumunda iletişimin tespiti suretiyle yapılan müdahalenin haberleşme hürriyetini ihlal ettiğine yönelik iddiaları inceleyecek, varsa ihlali tespit edecek ve gerektiğinde uygun giderim sağlayacak -bireysel başvuru öncesinde tüketilmesi gerekli- bir hukuksal mekanizma bulunmamaktadır. Öte yandan başvurucu aleyhine yürütülen ceza yargılamasında mahkeme ByLock programı bilgilerinin elde edilmesinin ve kullanılmasının haberleşme hürriyetini ihlal edip etmediğini tespit etme yetkisine sahip değil ise de ByLock verilerinin hukuka uygun olarak elde edilip edilmediğini inceleme yetkisine sahiptir. Nitekim somut olayda derece mahkemeleri bu incelemeye kararlarında yer vermişlerdir. Mahkemenin ByLock verilerinin hukuka aykırı olarak elde edilmediği sonucuna ulaşması, haberleşme hürriyeti yönünden ayrı bir değerlendirme mahiyeti taşımasa bile haberleşme hürriyetine yapılan müdahalenin kanuna uygunluğuyla ilgili olarak bir değere sahip olacaktır. Haberleşme hürriyetinin ihlali iddiasıyla ilgili olarak başka bir yolun da bulunmadığı gözetildiğinde başvurucunun dolaylı da olsa haberleşme hürriyetine yapılan müdahalenin kanuniliğiyle ilgili değerlendirme yapılması niteliğini haiz olan ceza yargılaması yolunu tükettikten sonra ve nihai kararın öğrenilmesinden itibaren otuz gün içinde yaptığı bireysel başvurunun süresinde olduğunun kabulü gerekir.

113. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

c. Esas Yönünden

i. Müdahalenin Varlığı

114. Somut olayda başvurucu suçu işlemediğinden bahisle tüm yargılama süreci boyunca ByLock kullanıcısı olduğu iddiasını kabul etmemiş olsa da aleyhine başlatılan soruşturmanın temel dayanaklarından birini anılan iddia oluşturmaktadır. Başvurucuya yönelik suçlamada ByLock haberleşme programı üzerinden ele geçirilen veriler de esas alınmıştır. Başsavcılığın talebi üzerine Sulh Ceza Hâkimliği kararına dayalı olarak başvurucunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgileri tespit edilmiştir. Başvurucunun ByLock kullanıcı bilgileri ve yazışmaları ile log kayıtlarına erişildiği, bu bilginin analiz edilerek soruşturma ile kovuşturma makamlarınca tespit edildiği anlaşılmaktadır (bkz. §§ 28-40). Belirli bir gerçek kişi olan başvurucuya ait olduğu derece mahkemelerince tespit edilen bu elektronik bilgiler kişisel veri olarak kabul edilmelidir. Olayda kamu makamlarınca bu elektronik verilerin tespiti suretiyle kişisel verilerin *toplanması*, yargısal makamlara nakledilmesi suretiyle *aktarılması* ve analiz edilerek mahkûmiyete esas alınması suretiyle de *kullanılması kişisel verilerin korunmasını isteme hakkı*na müdahale teşkil etmektedir. Öte yandan söz konusu veriler *haberleşme* kapsamında kaldığına göre bunlara erişilerek aktarılması ve kullanılması aynı zamanda *haberleşmenin gizliliğ*ine de müdahale niteliği taşımaktadır. Buna göre başvurucu hakkında uygulanan söz konusu tedbirler özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik bir müdahale oluşturmaktadır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

115. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

116. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 20. ve 22. maddelerini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama kriterlerine uygun olup olmadığının belirlenmesi gerekir (*Halil Berk*, B. No: 2017/8758, 21/3/2018, § 49; *Süveyda Yarkın*, B. No: 2017/39967, 11/12/2019, § 32; *Şennur Acar*, B. No: 2017/9370, 27/2/2020, § 34).

117. Başvuru konusu şikâyetin özü, kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yapılan müdahalenin kanuni dayanağının bulunup bulunmadığına ilişkindir. Bu nedenle öncelikle müdahalenin kanuni dayanağının incelenmesi gerekir.

(1) Kanunilik

(a) Genel İlkeler

118. Anayasa'nın temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 13. maddesinde hak ve özgürlüklerin *"ancak kanunla"* sınırlanabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü

cümlesinde kişisel verilerin *"ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla"* işlenebileceği belirtilmiş, aynı fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin *"kanunla"* düzenleneceği hüküm altına alınmıştır. Aynı şekilde Anayasa'nın 22. maddesinin ikinci fıkrasında *"kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça"* haberleşmenin engellenemeyeceği ve gizliliğine dokunulamayacağı düzenlenmiştir. Buna göre kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yapılan müdahalelerde dikkate alınacak öncelikli ölçüt, müdahalenin kanuna dayalı olmasıdır.

119. Müdahalenin kanuna dayalı olması öncelikle şeklî manada bir kanunun varlığını zorunlu kılar. Kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine müdahale edilmesi ancak yasama organınca kanun adı altında çıkarılan düzenleyici işlemlerde müdahaleye imkân tanıyan bir hükmün bulunması şartına bağlıdır. Ayrıca bu çerçevede belirtmek gerekir ki kişisel verilerin korunmasını isteme hakkına işleme suretiyle yapılan müdahaleler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla yapıldığı takdirde kanunilik koşulu sağlanmış kabul edilir.

120. Diğer taraftan Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin bir gereği olarak kanunun kalitesi de kanunilik koşulunun sağlanıp sağlanmadığının tespitinde önem arz etmektedir. Zira hukuki güvenlik ile belirlilik ilkeleri hukuk devletinin ön koşullarındandır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2014/183, K.2015/122, 30/12/2015, § 5) Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2010/80, K.2011/178, 29/12/2011). Buna göre bir hukuk devletinde temel hak özgürlüklere müdahalenin kanuna dayalı olması için şeklî anlamda bir kanunun varlığı yanında o kanunun metninin de bireylerin, davranışlarının sonucunu öngörebilmesine imkân verecek şekilde belirlilik taşıması gerekir. Diğer bir ifadeyle müdahaleye imkân veren kanun yeterince belirli ve öngörülebilir olmalıdır (benzer yöndeki karar için bkz. *Halime Sare Aysal* [GK], B. No: 2013/1789, 11/11/2015, § 62).

121. Öte yandan Anayasa Mahkemesi, Anayasa'da temel hak ve özgürlüklerin sınırlandırılması gibi münhasıran kanunla düzenlenmesi öngörülen konularda kanunun söz konusu meselenin temel esaslarını, ilkelerini ve çerçevesini belirlemiş olmasını gerektirdiğini ancak yasama organının meselenin temel kurallarını saptadıktan sonra uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakmasının yasama yetkisinin devri olarak yorumlanamayacağını kabul etmiştir (AYM, E.2014/133, K.2014/165, 30/10/2014). Bu bağlamda temel hak ve özgürlüklerin sınırlandırılmasına yönelik kanuni düzenlemelerde kanun koyucu tarafından temel esaslar, ilkeler ve çerçeve belirlendikten sonra diğer ayrıntıların düzenleyici işlemler ile belirlenebileceği kabul edilmiştir (*Mehmet Koray Eryaşa*, B. No: 2013/6693, 16/4/2015, § 63).

(b) İlkelerin Olaya Uygulanması

122. Anayasa Mahkemesinin *Ferhat Kara* kararında belirtildiği üzere suç isnadı altındaki kişilerin adli soruşturma ve kovuşturmalar kapsamında el konulan cihazlarında tespit edilen ByLock programına dair kurulum dosyası vs. dijital veriler dışında ByLock

verileri esas olarak iki kaynağa dayanmaktadır. Bunlardan ilki MİT'in adli makamlara ilettiği ve adli makamların mahkeme kararlarıyla üzerinde inceleme yaptığı ByLock sunucusundan elde edilen verilerdir. İkincisi ise ByLock sunucusuna ait hedef IP'lere Türkiye'den hangi IP'lerden erişildiğine ilişkin mahkeme kararıyla BTK'dan elde edilen CGNAT (ByLock sunucusuna ait IP adreslerine hangi tarihte kaç defa bağlanıldığı bilgisi) kayıtlarıdır (*Ferhat Kara*, § 58). BTK, ByLock IP'sine bağlanan numaraların abonelerine ait şahıs *kimlik bilgilerini* tespit ederek Başsavcılık ve mahkemelere bildirmiştir (*Ferhat Kara*, §§ 32-58). Bu nedenle somut olayda müdahalenin kanuni dayanağının olup olmadığının incelenmesi ByLock sunucusundan elde edilen veriler açısından ve ByLock verilerinin adli makamlara ulaştırılmasından sonraki süreç açısından olmak üzere iki başlıkta yapılmıştır.

(i) ByLock Sunucusundan Elde Edilen Veriler Açısından

123. Demokratik toplumlarda temel hak ve özgürlüklerin korunması amacıyla terör örgütleri gibi son derece karmaşık yapılarla etkin bir şekilde mücadele edilmesi ve bu tür örgütleri gizli yöntemlerle takip etmek amacıyla istihbarat organlarına ve onların yöntemlerine ihtiyaç duyulması kaçınılmazdır. Dolayısıyla terör örgütlerinin çökertilmesi amacıyla gizlilik taşıyan istihbarat yöntemleri kullanılarak bu örgütlerle ilgili bilgilerin toplanması ve analiz edilmesi demokratik toplumlardaki önemli bir ihtiyaca karşılık gelmektedir. Zira istihbarat birimlerinin elde ettikleri bu bilgiler vasıtasıyla demokratik anayasal düzene yönelik tehditlerin tespit edilmesi ve bunlara karşı önlemler alınması söz konusu olabilir (*Ferhat Kara*, § 130).

124. FETÖ/PDY'nin örgütlenmesi ve faaliyetleri öteden beri toplumda tartışma konusu olmakla birlikte özellikle 2013 yılı sonrasında soruşturma mercileri ve devletin güvenlik birimleri bu yapılanmanın millî güvenlik üzerinde tehdit oluşturduğunu değerlendirmeye başlamıştır. Bu bağlamda bilhassa 17-25 Aralık soruşturmaları ve MİT tırlarının durdurulması, bu yapılanmanın faaliyetlerinin Hükûmeti devirmeyi amaçladığı yönünde soruşturma mercileri ve yargı organlarınca yapılan değerlendirmelerin temel dayanakları arasındadır. Yine bu yapılanmayla bağlantılı olduğu değerlendirilen yargı mensupları eliyle açılan/yürütülen birçok davanın da örgütün başta Türk Silahlı Kuvvetleri olmak üzere kamu kurumlarında ve sivil toplumun farklı alanlarında etkinliğini sağlama veya artırma gayesine yönelik olduğu çok sayıda soruşturma/kovuşturma belgesinde ifade edilmiştir. Bu süreçte kamu makamları da bir taraftan FETÖ/PDY'nin illegal yönünü ortaya koyan karar ve uygulamalarda bulunmuş, diğer taraftan yapılanmaya karşı bazı tedbirlere başvurmuştur (*Ferhat Kara*, § 131)

125. Devletin istihbarat organlarının FETÖ/PDY'nin ulusal güvenlik üzerinde oluşturduğu tehdidin *yaklaşan* bir tehlikeye dönüşmekte olduğunu değerlendirerek bu konuda istihbarat çalışmalarında bulunmuş olmasının hukukiliğinin veya yerindeliğinin takdiri Anayasa Mahkemesinin görevi olmadığı gibi eldeki bireysel başvurunun inceleme konusu da değildir. İlgili makamlardan gerekli önleyici tedbirleri almaları için terör tehdidinin fiilen gerçekleşmesini beklemeleri istenemez. Karmaşık yapısı ve uluslararası niteliğinin FETÖ/PDY ile ilgili olarak -darbe teşebbüsü öncesinde- istihbarat anlamında bazı çalışmalar yapılmasını zorunlu kıldığı anlaşılmaktadır. Nitekim 15 Temmuz darbe teşebbüsü millî güvenlik üzerinde FETÖ/PDY'den kaynaklanan tehdidin ne denli büyük olduğunu ve bunun -öncesinde alınan birtakım tedbirlere rağmen- ulusun varlığını ve bütünlüğünü yok etmeye yönelik nasıl ağır bir tehlikeye dönüştüğünü göstermiştir (ayrıntılı açıklama ve değerlendirmeler için bkz. *Aydın Yavuz ve diğerleri*, §§ 12-25; 212-221; *Ferhat Kara*, § 132).

126. FETÖ/PDY'nin kamu kurum ve kuruluşlarındaki örgütlenmesinin, bunun yanı sıra başta eğitim ve din olmak üzere farklı sosyal, kültürel ve ekonomik alanlardaki faaliyetlerinin millî güvenlik üzerinde tehdit oluşturduğunun soruşturma mercileri ve devletin güvenlik birimlerince kabul edilmeye başlandığı süreçte MİT de kendi görev alanı çerçevesinde bu yapılanmanın faaliyetleriyle ilgili çalışmalarda bulunmuştur. Nitekim 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (a) bendinde MİT'in Türkiye Cumhuriyeti'nin bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkındaki millî güvenlik istihbaratını devlet çapında oluşturmak ve bu istihbaratı gerekli kuruluşlara ulaştırmakla yükümlü olduğu belirtilmiştir.

127. MİT tarafından yapılan çalışmalar kapsamında FETÖ/PDY mensuplarının örgütsel haberleşmelerinin sağlanması amacıyla geliştirildiği anlaşılan, ana sunucusu yurt dışında bulunan ByLock adlı mobil uygulama ve bu uygulamanın iletişim kurduğu sunucular olduğu tespit edilmiş; bunlar ayrıntılı teknik çalışmalara tabi tutulmuştur. Kendi görev alanı kapsamında MİT tarafından bu uygulamayla ilgili olarak yapılan çalışmalar adli soruşturma işlemi niteliğinde değildir. Zira 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (i) bendinde MİT'in terörle mücadele konularında da her türlü teknik istihbarat usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplama, kaydetme, analiz etme, üretilen istihbaratı gerekli kuruluşlara ulaştırma görev ve yetkisine sahip olduğu düzenlenmiştir (*Ferhat Kara*, § 128).

128. 2937 sayılı Kanun'un 6. maddesinde; MİT'in bu görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabileceği, telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabileceği de hüküm altına alınmıştır. Dolayısıyla anılan Kanun'un ülkenin anayasal düzeninin korunması ve millî güvenliğin sağlanması amacı ile terör faaliyetlerinin eyleme dönüşmeden belirlenebilmesi için MİT'e ilgili kişi ve gruplar hakkında teknik yöntemlerle bilgi ve veri toplama, topladığı bu bilgileri analiz etme yetkisi verdiği görülmektedir.

129. 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (a) bendinde MİT'in Türkiye Cumhuriyeti'nin bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkındaki millî güvenlik istihbaratını devlet çapında oluşturmak ve bu istihbaratı gerekli kuruluşlara ulaştırmakla yükümlü olduğu belirtilmiştir. Aynı fıkranın (i) bendinde de terörle mücadele konularında da her türlü teknik istihbarat usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak görev ve yetkisine sahip olduğu düzenlenmiştir. MİT'in bu görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanılabileceği, telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabileceği aynı Kanun'un 6. maddesinde hüküm altına alınmıştır. Anılan Kanun'un ülkenin anayasal düzeninin korunması ve ulusal güvenliğin sağlanması için terör faaliyetlerinin eyleme dönüşmeden belirlenebilmesi amacıyla MİT'e ilgili kişi ve gruplar hakkında teknik yöntemlerle bilgi ve veri toplama ve topladığı bu bilgileri analiz etme yetkisi verildiği görülmektedir. Bu bağlamda MİT'e 2937 sayılı Kanun'un 4. ve 6. maddeleri uyarınca yurt dışında bulunan bilgisayar verilerini satın alma da dâhil olmak üzere terörle mücadele konusunda telekomünikasyon kanallarından terör suçlarıyla ilgili geçen bilgi, belge ve diğer tüm verileri her türlü teknik istihbarat yöntemlerini kullanmak suretiyle toplama, analiz etme

ve bunları gerekli kuruluşlara ulaştırma yetkisi verilmiştir. Buna göre ilgili düzenlemelerin yeterince açık, anlaşılabilir ve öngörülebilir olduğu, *kanunilik* ölçütünü karşıladığı sonucuna varılmıştır.

(ii) ByLock Verilerinin Adli Makamlara Ulaştırılmasından Sonraki Süreç Açısından

130. MİT tarafından ByLock iletişim sistemine ilişkin dijital materyaller ve bu materyallere ilişkin düzenlenen teknik analiz raporunun Ankara Cumhuriyet Başsavcılığına iletilmesi üzerine bu aşamadan itibaren soruşturma işlemleri 5271 sayılı Kanun'a göre yürütülmüştür. Bu kapsamda söz konusu dijital materyaller üzerinde 5271 sayılı Kanun'un 134. maddesine göre inceleme, kopyalama, çözümleme işlemi yapmak için Ankara Cumhuriyet Başsavcılığınca Ankara 4. Sulh Ceza Hâkimliğine talepte bulunulmuştur. Anılan talep üzerine Ankara 4. Sulh Ceza Hâkimliği *"dijital materyaller üzerinde inceleme yapılması, kopya çıkarılması ve kopya üzerinde bilirkişi incelemesi yapıl*[masına]" karar vermiştir (*Ferhat Kara*, § 28).

131. Söz konusu mahkeme kararına dayalı olarak Ankara Cumhuriyet Başsavcılığı tarafından ByLock IP'sine bağlanan aboneliklere ait *"ByLock abone listesi"*nde yer alan abonelerin ByLock IP adreslerine kaç defa bağlandığına dair raporlar (CGNAT verileri) BTK'dan talep edilmiştir (*Ferhat Kara*, § 32). Bağlantı yapan GSM ve ADSL numaralarına ait abonelik bilgileri BTK tarafından Ankara Cumhuriyet Başsavcılığına iletilmiştir. Ankara Cumhuriyet Başsavcılığından KOM Daire Başkanlığınca teslim alınan abonelik bilgileriyle *"user ID_list"* (kullanıcı listesi) tablosu oluşturulmuştur (*Ferhat Kara*, § 35).

132. Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararında da ByLock iletişim sistemindeki veri tespitlerinin 5271 sayılı Kanun'un 134. maddesi kapsamında kaldığı vurgulanmıştır (bkz. § 56). Anılan karara göre internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından bu iletişim kayıtları hakkında 5271 sayılı Kanun'un 134. maddesinin (1) numaralı fıkrası gereğince arama, kopyalama ve elkoyma koruma tedbirleri uygulanabilir. Yargıtaya göre 5271 sayılı Kanun'un 134. maddesindeki *"bilgisayar kütükleri"* ifadesi teknik anlamda sadece masaüstü ve dizüstü bilgisayarlarda bulunanları değil CD, DVD, flash disk, disket, hard disk vs. tüm çıkarılabilir bellekler, telefon vb. dijital tabanlı mobil cihazlar da dâhil olmak üzere herhangi bir bilgi işlem veya veri toplama araç ya da gerecinde bulunabilecek tüm dijital dosyaları kapsamaktadır.

133. Somut olayda Kayseri 3. Sulh Ceza Hâkimliğince 5271 sayılı Kanun'un 116., 127. ve 134. maddeleri uyarınca başvurucunun ikametgâhında 6/9/2016 tarihinde arama yapılmasına, bulunan cep telefonu, bilgisayar, hard disk, hafıza kartları, sim kartları vb. kayıt tutma özelliği bulunan her türlü dijital materyallere el konulmasına, ele geçirilecek kayıtlardan kopya alınmasına, kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir. Kayseri 1. Sulh Ceza Hâkimliğinin 2/11/2016 tarihli kararı ile 5271 sayılı Kanun'un 135. maddesi uyarınca başvurucunun telefon numarasının 1/10/2013 ile 1/10/2016 tarihleri arasında iletişim kayıtları ve hangi baz istasyonlarından servis aldığının tespitine karar verilmiştir. Ayrıca Kayseri İl Emniyet Müdürlüğü KOM Şube Müdürlüğünce 6/2/2017 tarihinde Yeni ByLock CBS Sorgu Sonucu Raporu sunulmuş ve başvurucuya ait telefonun hat numarası ve IMEI numarası bilgilerine göre başvurucunun telefonuna ByLock haberleşme programını yükleyerek *(4397) ID kullanıcı numarasıyla* kullandığının anlaşıldığı belirtilmiştir. Aynı şekilde Ankara Cumhuriyet Başsavcılığının 2016/180056 sayılı

soruşturma dosyasından elde edilen bilgi kapsamında başvurucuya ait ByLock kullanımını gösteren ByLock Tespit ve Değerlendirme Tutanağı sunulmuştur. Bölge Adliye Mahkemesi kararıyla da başvurucunun kullandığı GSM hattının ve bu hatlarda kullanılan IMEI numaralarının HTS kayıtları ile ByLock'un belirlenen IP numaralarına bağlantı yaptığı tarih, saat ve baz istasyonu gösterir HTS kayıtları BTK'dan temin edilmiştir.

134. Buna göre başvurucunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgilerinin tespit edilmesi şeklindeki müdahalenin hâkim kararına dayalı olarak öncelikle 5271 sayılı Kanun'un 134. maddesi kapsamında dijital materyallere el konulması, ele geçirilecek kayıtlardan kopya alınması, kayıtların çözümlenerek metin hâline getirilmesi hükmü çerçevesinde, daha sonra aynı Kanun'un 135. maddesi uyarınca ve hâkim kararıyla başvurucunun telefon numarasının iletişim kayıtları ve hangi baz istasyonlarından servis aldığının tespiti şeklinde gerçekleştirildiği anlaşılmaktadır. 5271 sayılı Kanun'un 134. ve 135. maddelerinde öngörülen arama, dijital verilere elkoyma, telefon kayıtlarının tespitine yönelik açık ve detaylı kurallar ortaya konmuş; kamu makamlarının değerlendirme yetkisinin kapsam ve sınırları net bir şekilde belirtilmiştir. Aynı şekilde uygulanan tedbirlerin hangi suçlar için verileceği ve süresi ile kayıtların saklanma ve imha edilme şartları belirlenmiştir. Ayrıca söz konusu tedbirlerin acil hâllerde dahi keyfiliğe karşı yeterli bir güvence sağlayacak şekilde hâkim onayına tabi tutulması öngörülmüştür. Buna göre müdahalenin dayanağı olan kanun hükümleri, hak ve özgürlüğe yöneltilen müdahalelerin sınırlarını yeterli açıklıkta ortaya koyan, erişilebilir ve öngörülebilir niteliktedir. Yapılan değerlendirmeler neticesinde 5271 sayılı Kanun'un anılan maddelerinin *kanunilik* ölçütünü karşıladığı sonucuna varılmıştır (benzer yöndeki değerlendirmeler için bkz. *Mehmet Seyfi Oktay* [GK], B. No: 2013/6367, 10/12/2015, § 53; *Rıdvan Bayram,* B. No: 2013/1171, 9/9/2015, § 43; *C.E.*, B. No: 2016/436, 12/9/2019, § 49; *Günay Dağ ve diğerleri,* B. No: 2013/1631, 17/12/2015, § 136).

(2) Meşru Amaç

135. Anayasa'nın 13. maddesinde temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlandırılabileceği hüküm altına alınmıştır. Ancak Anayasa'nın 20. maddesinin üçüncü fıkrasında kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahaleler yönünden özel bir sınırlama sebebine yer verilmediği görülmektedir. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadına göre özel sınırlama nedeni öngörülmemiş hak ve özgürlüklerin de o hak ve özgürlüğün doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler, özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir (birçok karar arasından bkz. AYM, E.2014/177, K.2015/49, 14/5/2015).

136. Anayasa'nın 20. maddesinin üçüncü fıkrasındaki düzenlemelerden kişisel verilerin korunmasını isteme hakkına sınırlama getirilebileceği anlaşılmaktadır. Ancak fıkrada tüketici sayıda bir sebepler ya da meşru amaçlar listesine yer verilmemiştir. Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eden kişisel veri kavramının kullanım alanlarının oldukça geniş olması nedeniyle her bir kullanım alanı yönünden farklı sınırlama sebeplerinin ya da meşru amaçların kabul edilmesi kaçınılmazdır. Bu durumda hangi alanda kişisel verilerin korunmasını isteme hakkına yönelik sınırlama getirildiği ya da müdahale edildiğine bağlı olarak sınırlama nedeni ya da meşru amaç değişebilir. Buna göre yapılacak incelemede kişisel verilerin korunmasını isteme hakkının bu hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu dikkate alındığında her dosya ve başvuru kapsamında işin doğasından kaynaklanan sınırlama sebebinin tespit edilmesi ve

bunun meşru bir sebep olarak kabul edilip edilemeyeceğinin değerlendirilmesi gerekir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin de bu hakka sınır teşkil edebileceği kabul edilmelidir.

137. Türkiye Cumhuriyeti'ne yönelik terör faaliyetlerinin tespiti ve önlenmesi devletin temel ödevlerindendir. Bu açıdan terör örgütlerinin ve bunların faaliyetlerinin tespiti, bu suretle suç işlenmesinin önlenmesi amacıyla kişisel verilerin korunması hakkının sınırlandırılmasının meşru bir amaca dayandığı sonucuna ulaşılmaktadır.

138. Diğer taraftan Anayasa'nın 22. maddesinin ikinci fıkrasına göre millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak haberleşme hürriyeti sınırlandırılabilir. Somut olayda terör örgütüyle mücadele, suç işlenmesinin önlenmesi ve suç kanıtlarının elde edilmesi amacına yönelik olarak 5271 sayılı Kanun'un 134. ve 135. maddeleri uyarınca ve hâkim kararlarıyla başvurucunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgileri tespit edilmiştir. Dolayısıyla müdahalenin Anayasa'nın 22. maddesinde gösterilen suç ve suçlularla mücadele bağlamında kamu düzeni ve güvenliğinin sağlanmasına yönelik meşru bir amaç taşıdığı anlaşılmaktadır.

(3) Demokratik Toplum Düzeninin Gereklerine Uygunluk ve Ölçülülük

(a) Genel İlkeler

139. Temel hak ve özgürlüklere yönelik bir müdahalenin demokratik toplum düzeninin gereklerine *uygun* kabul edilebilmesi için zorunlu bir toplumsal ihtiyacı karşılaması ve ölçülü olması gerekir. Açıktır ki bu başlık altındaki değerlendirme, sınırlamanın amacı ile bu amacı gerçekleştirmek üzere başvurulan araç arasındaki ilişki üzerinde temellenen ölçülülük ilkesinden bağımsız yapılamaz. Çünkü Anayasa'nın 13. maddesinde *demokratik toplum düzeninin gereklerine aykırı olmama* ve *ölçülülük ilkesine aykırı olmama* biçiminde iki ayrı kritere yer verilmiş olmakla birlikte bu iki kriter bir bütünün parçaları olup aralarında sıkı bir ilişki vardır (*Ferhat Üstündağ*, B. No: 2014/15428, 17/7/2018, § 45).

140. Müdahaleyi oluşturan tedbirin zorunlu bir toplumsal ihtiyacı karşıladığının kabul edilebilmesi için amaca ulaşmaya elverişli olması, başvurulabilecek en son çare ve alınabilecek en hafif önlem olarak kendisini göstermesi gerekmektedir. Amaca ulaşmaya yardımcı olmayan veya ulaşılmak istenen amaca nazaran bariz bir biçimde ağır olan bir müdahalenin zorunlu bir toplumsal ihtiyacı karşıladığı söylenemeyecektir (*Ferhat Üstündağ*, § 46).

141. Orantılılık ise sınırlamayla ulaşılmak istenen amaç ile başvurulan sınırlama tedbiri arasında dengesizlik bulunmamasına işaret etmektedir. Diğer bir ifadeyle orantılılık, bireyin hakkı ile kamunun menfaatleri veya müdahalenin amacı başkalarının haklarını korumak ise diğer bireylerin hak ve menfaatleri arasında adil bir dengenin kurulmasına işaret etmektedir. Dengeleme sonucu müdahalede bulunulan hakkın sahibine terazinin diğer kefesinde bulunan kamu menfaati veya diğer bireylerin menfaatine nazaran açıkça orantısız bir külfet yüklendiğinin tespiti hâlinde orantılılık ilkesi yönünden bir sorunun varlığından söz edilebilir (*Ferhat Üstündağ*, § 46).

142. Bununla birlikte kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahalelerin demokratik toplum düzeninin gereklerine uygun olabilmesi için zorunlu bir toplumsal ihtiyacı karşılaması yetmez. Zira Anayasa'nın 20. maddesinin üçüncü fıkrasının ikinci cümlesinde *"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."* denilerek kişisel verilerin korunmasını isteme hakkına yönelik sınırlamalar ya da müdahaleler bakımından bazı özel güvencelere de yer verilmiştir. Bunlar, kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ya da müdahalelerin demokratik bir toplum düzeninin gereklerine uygun olabilmesi için Anayasa koyucu tarafından özel olarak belirlenmiş güvenceler mahiyetindedir.

143. Ayrıca Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir."* denildikten sonra ikinci cümlesinde bu hakkın yukarıda belirtilen bazı özel güvenceleri de kapsadığı belirtilmiştir. İkinci cümlede geçen *"...de kapsar"* ibaresi birinci cümle ile birlikte değerlendirildiğinde Anayasa koyucunun iradesinin demokratik bir toplumda kişisel verilerin korunmasını isteme hakkı kapsamında tanınması gereken güvenceleri ikinci cümlede sayılanlarla sınırlı tutmak olmadığı anlaşılmaktadır. Nitekim uluslararası belgeler ve karşılaştırmalı hukuk metinleri incelendiğinde kişilere Anayasa'da sayılan güvencelerin tanınmasının yanında bazı durumlarda bu güvencelerin daha geniş olan bazı ilkelerin parçası olarak öngörüldüğü, bazı durumlarda Anayasa'daki özel güvencelerin detaylarının ortaya konulduğu, bazı durumlarda ise ilave bazı güvencelere yer verildiği görülmektedir (bkz. §§ 58-60). Anayasa değişikliğinin uluslararası belgelere ve karşılaştırmalı hukuk metinlerine atıf yapan gerekçesi (bkz. § 93), Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesindeki kişisel verilerin korunmasını isteme hakkına ilişkin genel hüküm, ikinci cümlesinde güvencelerin tüketici şekilde sayılmamış olması dikkate alındığında Anayasa'nın 13. maddesindeki sınırlama ölçütlerinden demokratik toplum düzeninin gereklerine uygunluk ölçütü kapsamında yorum yapılırken uluslararası belgelerde ve karşılaştırmalı hukuk metinlerinde yer alan ilkelerin de her başvurunun somut koşullarına uygun düştüğü ölçüde değerlendirmeye alınabileceği sonucuna ulaşılmaktadır.

144. Bu bakımdan kamu müdahalesine konu olan kişisel verinin niteliğine bağlı olarak aşağıdaki ek güvencelerin bir kısmının veya tamamının sağlanması gerekebilir:

i. Kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak veri sahipleri önceden bilgilendirilmelidir. Bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- kişisel verilerin işlenmesinin hukuki dayanağı ve işlemenin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemenin sonuçları ve verilerin muhtemel yararlanıcıları hususlarını kapsaması gerekir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

ii. Kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli, bunun bir gereği olarak veri sahiplerine kişisel verilerine erişim imkânı tanınmalı ve bu imkânın kolayca kullanılması için gerekli tedbirler alınmalıdır.

iii. Kişisel veriler doğru ve güncel bir biçimde tutulmalı, yanlış olan, güncel olmayan ya da hukuka aykırı olarak tutulan kişisel verilerin gecikmeksizin düzeltilmesi veya silinmesi için gerekli tedbirler alınmalı, bu kapsamda kişilere talepte bulunma hakkı tanınmalıdır.

iv. Kişisel verilerin gizliliğinin sağlanması ve bu verilerin yetkisiz veya kanuna aykırı olarak işlenmemesi, kaybolmaması, imha edilmemesi ya da zarar görmemesi için uygun teknik ve yapısal tedbirler öngörülmeli; bu tedbirler etkili bir biçimde uygulanmalıdır.

v. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ya da müdahalenin orantılı kabul edilebilmesi için kişisel veriler sınırlama ya da müdahale amacı için gerekenden daha uzun süre saklanmamalıdır.

vi. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın ya da müdahalenin orantılı kabul edilebilmesi için veri sahibine, menfaatlerini zedeleyen bir yöntem olan kişisel verilerden veri sahibi hakkında otomatik sonuçlar çıkarılması yöntemine kural olarak başvurulmamalıdır. İşin niteliğinin bu yöntemin uygulanmasını gerektirdiği durumlarda ise veri dezavantajlı durumunu hafifletmek amacıyla söz konusu yönteme dayanmayan bir karar alınmasını talep etme hakkı gibi usule ilişkin güvenceler sağlanmalıdır.

vii. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın ya da müdahalenin orantılı kabul edilebilmesi için işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir. Ayrıca kişilere hakkın sağladığı güvencelerin ihlali hâlinde yargı yoluna başvurma imkânı tanınmalı ve yargılamanın adil bir şekilde yapılmasını temin için usule ilişkin güvenceler sağlanmalıdır.

viii. Din veya felsefi inanç, ırk veya etnik köken, cinsel yönelim, bazı örgütlenmelere üyelik, sağlık, genetik veriler, biyometrik veriler ve mahkûmiyet verileri gibi hassas kişisel verilerin söz konusu olduğu durumlarda kişisel verilerin korunmasını isteme hakkı kural olarak sınırlanmamalı ya da bu hakka müdahale edilmemelidir. Sınırlama ve müdahalenin zorunlu olduğu bazı istisnai hâllerde ise bunun kişiler üzerinde ortaya çıkaracağı sonuçların ağırlığı ve kişiler hakkında ayrımcı uygulamalara yol açma tehlikesi dikkate alınarak kişisel verilerin korunmasına ilişkin güvenceler daha katı uygulanmalıdır.

145. Millî güvenlik, kamu düzeni, devletin mali menfaatleri, suçların önlenmesi, ilgili kişinin veya başkalarının hak ve özgürlüklerinin korunması, istatistikî veya bilimsel araştırma gibi amaçlarla yapılan sınırlama ve müdahaleler bakımından kimi durumlarda işin niteliğinin zorunlu kılması hâlinde kişisel verilerin korunması hakkına yönelik sınırlama ve müdahaleler yönünden ortaya çıkan özel güvencelere istisna getirilebilir. Ancak bu durumda bile Anayasa'nın 13. maddesinde tüm temel hak ve özgürlükler yönünden öngörülmüş olan sınırlama ölçütlerinin asgari standartlarına uyulmalıdır. Diğer bir ifadeyle istisna hâlleri bulunsa bile sınırlama ve müdahale kanuna dayanmalı, sınırlama sebeplerini barındırmalı ya da meşru amaç takip etmeli, demokratik toplum düzeninin gereği olarak zorunlu bir toplumsal ihtiyacı karşılamalı ve ölçülü olmalıdır. Bu durumda anılan ölçütler özel güvenceler dikkate alınmaksızın yorumlanır. Bununla birlikte bir istisna hâlinin varlığı özel güvencelerin tamamının otomatik olarak ortadan kalkmasına neden olmaz. Böyle bir

durumun varlığı hâlinde işin niteliği dikkate alınarak her bir özel güvence yönünden istisna getirilmesinin zorunlu olup olmadığı değerlendirilmelidir.

(b) İlkelerin Olaya Uygulanması

146. Başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin amacının FETÖ/PDY'nin ve faaliyetlerinin tespiti, bu suretle suç işlenmesinin önlenmesidir. ByLock haberleşme programı verilerinin elde edilmesi, tahlil edilmesi ve soruşturma makamlarına aktarılmasının, yine başvurucunun bu programı kullanıp kullanmadığının ortaya konulması gayesiyle iletişim kayıtları ve hangi baz istasyonlarından servis aldığının tespit edilmesinin belirtilen amaca ulaşılması yönünden elverişli bir araç olduğu açıktır.

147. İkinci olarak müdahalenin zorunlu bir toplumsal ihtiyaca karşılık gelip gelmediği ve bu çerçevede başvurucunun ByLock verilerinin elde edilmesinin, iletişim kayıtları ile baz hareketliliğinin temin edilmesinin son çare olarak başvurulan bir araç olup olmadığı incelenmelidir.

148. Günümüzde terör, tüm dünyada demokratik topluma ve bireylerin şiddetten ari bir ortamda yaşamını sürdürmesine yönelik en ciddi tehditlerin başında gelmektedir. Terör örgütleri çoğunlukla belli bir ülkenin coğrafi hudutlarıyla sınırlı olarak faaliyet göstermemekte, uluslararası mahiyeti bulunan bir küresel güvenlik sorunu olarak karşımıza çıkmaktadır. Kendine özgü yapısı ve gizlilik esasına dayanan çalışma yöntemi, sivil organizasyonları örgütsel amaçlarına ulaşabilmek amacıyla kullanmadaki maharetiyle FETÖ/PDY çok sayıda ülkede kendine alan açmayı başarmış ve faaliyetleri dünyanın her yanına yayılmış en organize ve tehlikeli terör örgütlerinden biridir. Bu sebeple örgütün millî güvenlik üzerinde oluşturduğu tehdit ve tehlikenin bertaraf edilebilmesi bakımından yalnızca ceza soruşturması bağlamında soruşturma makamlarına tanınan yetkilerle iktifa edilmesinin yeterli olmayacağı açıktır. Dolayısıyla örgütün faaliyetlerinin ve mensuplarının tespiti için gizlilik taşıyan istihbarat tekniklerine başvurulması kaçınılmaz hâle gelmiştir. Anayasa'nın 20. ve 22. maddeleri istihbarat yöntemleri kullanılmak suretiyle haberleşme hürriyeti ile kişisel verilerin korunmasını isteme hakkına müdahalede bulunulmasını yasaklamamaktadır. Hiçbir demokratik devlet, kendi varlığına yönelmiş tehditler karşısında hareketsiz kalamaz. Devletin demokratik toplum düzenini, anayasal nizamı ve meşru hükûmeti zorla ortadan kaldırmayı hedefleyen kişi ve yapılara karşı mücadele etme yetki ve görevinin bulunduğu tartışma götürmez bir gerçektir. Bu açıdan gizli istihbarat teknikleri kullanılmak suretiyle ByLock verilerine ulaşılmasının demokratik toplum düzeninin gereklerine aykırı olduğu söylenemez.

149. Nitekim örgütün faaliyetlerinin ve üyelerinin tespitinde ByLock sunucusundan elde edilen veriler oldukça önemli bir role sahip olmuştur. Örgütün birçok üst düzey yöneticisi ByLock verilerinin analizi neticesinde tespit edilebilmiştir. FETÖ/PDY'nin kendine özgü yapısı gözetildiğinde daha hafif bir aracın tercihiyle aynı sonucun elde edilmesinin mümkün olamayacağı da ortadadır. Şu hâlde istihbarat yöntemleri kullanılmak suretiyle ByLock sunucusunda bulunan verilerin elde edilmesinin ve bunların yargılama makamlarına aktarılmasının demokratik toplum düzenin gereklerine uygun olma kriterini taşıdığı sonucuna ulaşılmaktadır.

150. Üçüncü olarak kişisel verilerin korunması hakkının mahiyetinden kaynaklanan özel güvencelerin sağlanıp sağlanmadığı incelenmelidir. Ancak öncelikle somut olayda kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahaleler yönünden

ortaya çıkan özel güvencelere istisna getirilmesi gereken bir durumun bulunup bulunmadığı irdelenmelidir.

151. Anayasa'nın 13. maddesi ve 14. maddesinin birinci fıkrasında yer alan *"Anayasada yer alan hak ve hürriyetlerden hiçbiri, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmayı ve insan haklarına dayanan demokratik ve laik Cumhuriyeti ortadan kaldırmayı amaçlayan faaliyetler biçiminde kullanılamaz."* şeklindeki hüküm uyarınca demokratik devlet düzeni ve millî güvenliğin sağlanması, terörle mücadele amacıyla kişisel verilerin korunması hakkının özel güvencelerine istisna getirilmesi mümkündür. Nitekim konuyla ilgili uluslararası hukuk belgelerinde de millî güvenliğin korunması ve terörle mücadele amacıyla kişisel verilerin korunmasını isteme hakkının özel güvencelerine istisna getirilebileceği kabul edilmiştir (bkz. §§ 61, 66). 6698 sayılı Kanun'un *"istisnalar"* kenar başlıklı 28. maddesinde suçla mücadele ve millî güvenlik amacıyla kişisel verilerin önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi istisnalar arasında sayılmıştır (bkz. § 48).

152. Olayda başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin amacının millî güvenliğin sağlanması ve suç işlenmesinin önlenmesiyle yakından ilgili olduğu açıktır. Kamu makamları örgütün faaliyetlerinin ve mensuplarının tespiti ve örgütün varlığının kamu düzeni ve millî güvenlik üzerinde doğurduğu risklerin önlenmesi için yalnızca adli soruşturma yapmakla yetinilmesinin yetersiz kalacağı kanaatine ulaşmış, bu nedenle ceza soruşturması kapsamında bulunmayan birtakım gizli istihbarat tekniklerine başvurmuşlardır. Bu yönteme başvurulmasında, örgütün Türkiye Cumhuriyeti'nin egemenliğine yönelik olarak oluşturduğu ve 15 Temmuz 2016 tarihinde yaşanan darbe teşebbüsüyle görünür hâle gelen tehdidin büyüklüğünün etkili olduğu inkâr edilemez. Dolayısıyla somut olaydaki müdahalenin kişisel verilerin korunmasını isteme hakkı yönünden ortaya çıkan özel güvencelere istisna getirilmesini gerektiren türden olduğu açıktır.

153. Bununla birlikte bir istisna hâlinin varlığı özel güvencelerin tamamının otomatik olarak ortadan kalkmasını gerektirmez. Somut olayın özelliği gözetildiğinde (1) sınırlı olma, (2) uzun süre saklanmama, (3) veri sahibiyle ilgili olarak otomatik sonuç doğurmama ve (4) etkili yargısal denetim güvencelerinin sağlanması gerektiği değerlendirilmiştir. Bu durumda somut olayda bunların sağlanıp sağlanmadığı ele alınmalıdır.

154. ByLock verilerinin istihbarat tekniklerinin kullanılması suretiyle elde edilmesi suretiyle kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik olarak gerçekleşen müdahalenin örgütün faaliyetlerinin ve mensuplarının açığa çıkarılması ve örgütün çökertilmesi amacının ötesine geçtiğine dair bir bilgi bulunmamaktadır. Başvurucunun da bu verilerin amacı ile sınırlı olarak kullanılmadığı yönünde bir şikâyeti bulunmamaktadır. ByLock haberleşme programından elde edilen veriler yalnızca bu örgüte üye olma suç isnadıyla yürütülen ceza yargılamasında kullanılmıştır. Dolayısıyla başvurucuya ait kişisel verilerin amacı dışında kullanılmadığı anlaşılmaktadır.

155. Başvurucunun ByLock haberleşme programını kullandığına ilişkin veriler ile ile BTK'dan temin edilen telefon ve internet kullanımı, bağlandığı IP adresleri bilgisi, gönderdiği mail, mesaj ve arama kayıt bilgilerinin yargılama süresince saklanması öngörülmektedir. Yargılamada delil olarak kullanılan kişisel verilerin yargılama süresince saklanmasının adil yargılanma hakkı bakımından gerekli olduğu açıktır. Başvurucunun da saklama süresine uyulmadığı yönünde hiçbir şikâyeti bulunmamaktadır. Dolayısıyla saklama süresinin gereğinden uzun olmadığı değerlendirilmiştir.

156. ByLock sunucusundan elde edilen veriler başvurucu ile ilgili olarak otomatik sonuç doğurmamış; öncelikle kolluk birimlerince ardından da yargı mercilerince değerlendirilip analizi yapıldıktan sonra bu veriler, başvurucu aleyhine soruşturma konusu edilmiştir. Son olarak başvurucu, aleyhine yürütülen yargılamada bunlara yönelik itirazlarını derece mahkemeleri önünde dile getirebilmiş, derece mahkemeleri ise başvurucunun itirazlarını ayrıntılı olarak değerlendirmiş ve karşılamıştır. Dolayısıyla başvurucunun *"Genel İlkeler"* bölümünde değinilen kişisel verilerin korunmasını isteme hakkına yönelik özel güvenceler bakımından bir şikâyeti bulunmadığı gibi bu güvencelere yönelik herhangi bir eksiklik tespit edilmemiş, başvurucunun yargısal güvencelerden de yararlanabildiği kanaatine varılmıştır.

157. Açıklanan gerekçelerle Anayasa'nın 20. ve 22 maddelerinde güvence altına alınan özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edilmediğine karar verilmesi gerekir.

C. Diğer İhlal İddiaları

158. Başvurucu; ByLock programının kullanıldığı tarih itibarıyla bu programı kullanmanın suç olmadığını, sonradan suç olarak ilan edilmesinin işlendiği zaman suç olmayan bir fiile dayanılarak mahkûm olması anlamına geldiğini, bunun suç ve cezaların kanuniliği ilkesini ihlal ettiğini ileri sürmüştür.

159. Anayasa Mahkemesine başvuru konusu olaylarla ilgili delilleri sunmak suretiyle olaylar hakkındaki iddiaları temellendirmek ve dayanılan Anayasa hükmünün ihlal edildiği iddiasına dair açıklamalarda bulunarak hukuki iddialarını ortaya koymak başvurucuya düşer. Başvurucunun kamu gücünün işlem, eylem ya da ihmali nedeniyle ihlal edildiğini ileri sürdüğü hak ve özgürlük ile dayanılan Anayasa hükümlerini, ihlal gerekçelerini, dayanılan deliller ile ihlale neden olduğu ileri sürülen işlem veya kararların neler olduğunu başvuru dilekçesinde belirtmesi şarttır. Başvuru dilekçesinde kamu gücünün ihlale neden olduğu iddia edilen işlem, eylem ya da ihmaline dair olayların tarih sırasına göre özeti yapılmalı; bireysel başvuru kapsamındaki hak ve özgürlüklerden hangisinin hangi nedenle ihlal edildiği ve buna ilişkin gerekçeler ve deliller açıklanmalıdır (*Veli Özdemir*, B. No: 2013/276, 9/1/2014, §§ 19, 20; *Ünal Yiğit*, B. No: 2013/1075, 30/6/2014, §§ 18, 19).

160. Başvurucunun ByLock kullanma fiilinden değil örgüt üyeliği suçundan mahkûm olduğu vurgulanmalıdır. Bu açıdan derece mahkemesinin ByLock kullanımını suç olarak nitelendirmesi söz konusu değildir. Derece mahkemesi, başvurucunun ByLock kullanmış olmasını örgüt üyeliği suçunu işlediğinin bir delili olarak kabul etmiştir. Bu sebeple başvurucunun suç ve cezaların kanuniliği ilkesinin ihlal edildiği iddiasının incelenebilir bir temeli bulunmamaktadır. Başvurucu suç ve cezaların kanuniliği ilkesinin anayasal koruma alanına temas eden başkaca bir iddia da öne sürmemiştir. Bu itibarla suç ve cezaların kanuniliği ilkesinin ihlal edildiğine ilişkin şikâyetin temellendirilemediği kanaatine varılmıştır.

161. Açıklanan gerekçelerle başvurunun bu kısmının *açıkça dayanaktan yoksun olması* nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. 1. Kişi hürriyeti ve güvenliği hakkının ihlal edildiğine ilişkin iddianın *süre aşımı* nedeniyle KABUL EDİLEMEZ OLDUĞUNA,

2. Özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

3. Diğer ihlal iddialarının *açıkça dayanaktan yoksun olması* nedeniyle KABUL EDİLEMEZ OLDUĞUNA,

B. Anayasa'nın 20. maddesinde yer alan kişisel verilerin korunmasını isteme hakkının ve 22. maddesinde düzenlenen haberleşme hürriyetinin İHLAL EDİLMEDİĞİNE,

C. Yargılama giderlerinin başvurucu üzerinde BIRAKILMASINA,

D. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 17/9/2020 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan Zühtü ARSLAN	Başkanvekili Hasan Tahsin GÖKCAN	Başkanvekili Kadir ÖZKAYA
Üye Serdar ÖZGÜLDÜR	Üye Burhan ÜSTÜN	Üye Engin YILDIRIM
Üye Hicabi DURSUN	Üye Celal Mümtaz AKINCI	Üye Muammer TOPAL

Üye	Üye	Üye
M. Emin KUZ	Rıdvan GÜLEÇ	Recai AKYEL

Üye	Üye
Yusuf Şevki HAKYEMEZ	Yıldız SEFERİNOĞLU

Üye	Üye
Selahaddin MENTEŞ	Basri BAĞCI