



AİHM KARARLARI IŞIĞINDA TERÖRLE MÜCADELEDE İDARİ KOLLUĞUN GENEL İZLEME VE TAKİP YETKİSİ VE ÖZEL HAYATIN KORUNMASI

General Monitoring and Pursuit Authority of Administrative Law Enforcement in the Fight against Terrorism, and Protection of Private Life in the Light of ECHR Decisions

İbrahim AYDIN¹

¹Doktora Öğrencisi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir, ibrahim.aydin20@ogr.deu.edu.tr, orcid.org/0000-0002-2542-5713

Araştırma Makalesi/Research Article

Makale Bilgisi

Geliş/Received:
16.11.2023
Kabul/Accepted:
28.12.2023

DOI:

10.18069/firatsbed.1392078

Anahtar Kelimeler

terör, güvenlik, özel hayatın korunması, kolluk, istihbarat.

Keywords

terrorism, security, protection of private life, law enforcement, intelligence.

ÖZ

Terör eylemlerinin ana hedefi cebir ve şiddet kullanarak anayasal düzeni ortadan kaldırmak ve temel hak ve hürriyetleri yok etmektir. Siyasi gerilimler, savaşlar, kitlesel göçler, iletişim, bilişim ve ulaşım teknolojilerinde yaşanan devasa değişimler yeni güvenlik tehditlerini de beraberinde getirmiştir. Sınır aşan terörist faaliyetler, organize kaçakçılık ve siber suçlar giderek yaygınlaşmıştır. Bu tehditlere karşı devletler, idari kolluğun teröre mücadelede, istihbarat toplama, izleme ve takip gibi yetkilerini artırma eğilimine girmiştir. Diğer taraftan bu durum özel hayatın korunması hakkının ihlali tartışmalarını da beraberinde getirmiştir. Ulusal mahkemelere ve Avrupa İnsan Hakları Mahkemesine ihlal başvuruları yapılmıştır. AİHM'in bu konudaki kararları hükümetler açısından da yol gösterici niteliktedir. Bu çalışmada idari kolluğa verilen genel izleme ve takip yetkisinin AİHM içtihatları açısından tartışılması amaçlanmıştır. Özel hayatın korunması ve gizliliği, ulusal güvenlik ve istihbarat kavramları hakkında açıklayıcı bilgilerin verilmesinin ardından idari kolluğa verilen genel izleme ve takip yetkileri tartışılmış ve devamında benzer uygulamalar hakkında AİHM içtihatları örneklendirilmiştir. Bu çalışmanın son kısmında bir kısım öneriler de üretilmiştir.

ABSTRACT

The main goal of terrorist acts is to eliminate the constitutional order and destroy fundamental rights and freedoms by using force and violence. Political tensions, wars, mass migrations, and huge changes in communication, information and transportation technologies have brought with them new security threats. Transnational terrorist activities, organized smuggling and cyber crimes have become increasingly common. In response to these threats, states have tended to increase the powers of the administrative law enforcement in the fight against terrorism, such as intelligence collection, monitoring and follow-up. On the other hand, this situation has also brought about discussions about the violation of the right to protection of private life. Violation applications have been made to national courts and the European Court of Human Rights. The ECHR's decisions on this issue are also guiding for governments. In this study, it is aimed to discuss the general monitoring and follow-up authority given to the administrative law enforcement in terms of ECHR jurisprudence. After giving explanatory information about the concepts of protection and confidentiality of private life, national security and intelligence, the general monitoring and follow-up powers given to the administrative law enforcement are discussed and the ECHR jurisprudence on similar practices is exemplified. Some suggestions were also produced in the last part of this study.

Atıf/Citation: Aydın, İ. (2024). AİHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 34, 1, 217-235.

Sorumlu yazar/Corresponding author: İbrahim AYDIN, ibrahim.aydin20@ogr.deu.edu.tr

1. Giriş

Terör eylemlerinin ana hedefi devlet otoritesini zaafa uğratmak, yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini ve genel sağlığı bozmaktır. Terör eylemleri bu amaçlarına ulaşabilmek için sistemli bir şekilde cebir ve şiddet kullanmaktadır (Ergil, 1992;140). Dolayısıyla terör eylemleri bireyin ve toplumun varlığı ve kamu düzeni için büyük bir tehlike ve tehdit oluşturmaktadır. Terörizm nedeniyle yüzbinlerce insan hayatını kaybetmiş, daha da fazlası sakatlanmış ve insanlar kalıcı travmalar yaşamışlardır. Ülke ekonomileri terör kaynaklı milyarlarca dolar zarara uğramıştır. 11 Eylül saldırılarının ABD'ye yol açtığı ekonomik maliyetin 50 milyar dolardan fazla olduğu tahmin edilmektedir. Türkiye'de sadece PKK terörüne bağlı olarak 50 bin kişi hayatını kaybetmiş ve 200 milyar dolardan çok daha fazla ekonomik kayıp yaşanmıştır (Delice ve Dağlar, 2011;4).

Terör tehdidine karşı devletin diğer organlarıyla birlikte kolluk da mücadele etmektedir. 11 Eylül saldırılarının doğurduğu ortam ve devamında iletişim, bilişim ve ulaşım teknolojilerinde yaşanan devasa değişimler yeni güvenlik risklerini, tehditlerini ve tehlikelerini de beraberinde getirmiştir. Sınır aşan terörist faaliyetler, organize kaçakçılık suçları ve siber suçlar giderek yaygınlaşmıştır (Can, 2020;1). Tüm bu gelişmelere bağlı olarak kolluğun terörle mücadelesini düzenleyen yetkilendirilmeler yapılmış ve yapılmaya da devam edilmektedir. Tüm dünyada idari kolluğa geniş çaplı istihbarat toplama, izleme ve takip, kişisel veri işleme (parmak izi ve fotoğraf alma, MOBESE, plaka tanıma, iletişimin takibi, bankacılık işlemleri takibi, seyahat bilgileri takibi (PNR) gibi) vb. yetkiler verildiği var olan yetkilerin genişletildiği görülmektedir.

Ulusal güvenlik söz konusu olduğunda bir kısım haklara müdahale meşru hale gelmektedir (Bayındır, 2016;49). Bununla birlikte ulusal güvenlik ile özel hayatın gizliliğinin korunması arasında bir denge gözetilmesi gerekmektedir. Ulusal güvenlik ve terörle mücadele söz konusu olsa dahi kolluk tarafından gizli biçimde iletişimin denetlenmesi gibi güvenlik tedbirlerine başvurulduğunda özellikle AİHS sözleşmesine taraf olan ülkelerden bu tedbirlerin güvenlik ve anayasal düzeninin iç ve dış tehditlere karşı korunması için ve özel yaşamın gizliliğine hakkına saygı içerisinde uygulanması beklenmektedir (Öncü, 2011;78).

Bu çalışmada Türk hukuk sisteminde idari kolluğa verilen genel izleme ve takip yetkisinin AİHM içtihatları açısından tartışılması amaçlanmıştır. Özel hayatın korunması ve gizliliği, ulusal güvenlik ve istihbarat kavramları hakkında açıklayıcı bilgilerin verilmesinin ardından Türk hukuk sisteminde idari kolluğa verilen genel izleme ve takip yetkileri tartışılmış ve devamında benzer uygulamalar hakkında AİHM içtihatları örneklendirilmiştir. Bu çalışmanın son kısmında bir kısım öneriler de üretilmiştir.

1.1. Özel Hayatın Korunması

Evensel haklar olarak insan yaşamı ve onuru vazgeçilmez değerlerdir ve bunlar her türlü tehlike ve riske karşı korunmalıdır. İnsan onuruna duyulan saygının gereği yapılması gerekenlerden bir tanesi özel hayatın korunması ve gizliliğinin teminat altına alınmasıdır. İnsan her ne kadar sosyal bir varlık olsa dahi bir yönüyle de başkalarının müdahil olmasını istemediği özel alanları vardır ve toplumdan bilinçli bir biçimde gizlediği özel bir yaşamı da bulunmaktadır. Özel hayatın korunması konusunda devlet öncelikli olarak sorumludur ve bu konuda pozitif ve negatif yükümlülükleri bulunmaktadır. Devletin özel hayatın gizliliğine müdahale etmemesi ve kişilerin mahremiyetini koruması beklenir. Ayrıca devlet başkaları tarafından kişinin özel hayatının gizliliğinin ihlal edilmesine de engel olmalıdır (Ahmetoğlu, 2023;42).

Özel hayatın gizliliği ve korunması uluslararası insan hakları belgelerinde ve Türkiye Cumhuriyeti Anayasa'sında da vurgulanan bir konudur. İnsan Hakları Evrensel Beyannamesinin 12. maddesinde, Avrupa İnsan Hakları Sözleşmesinin Özel ve Aile Hayatına Saygı başlıklı 8. maddesinde, Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşmenin 17. maddesinde özel hayatın gizliliği ve korunmasına vurgu yapıldığı gibi Türkiye Cumhuriyeti Anayasasının 20, 21 ve 22. Maddelerinde de özel hayatın gizliliği güvence altına alınmıştır. Anayasanın 20. maddesi koruma "herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" şeklindedir. Anayasanın 20. Maddesinde 07.05.2010 tarihli ve 5982 sayılı Kanunla yapılan Anayasa değişikliği ile kişisel verilerin korunması da anayasal bir hak olarak tanımlanmıştır. Düzenleme ile kişisel verilerin korunması anayasal güvenceye kavuşturulmuştur. 2016 yılında Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme iç hukuka kazandırılmıştır. Yine Anayasa değişikliği ile getirilen kişisel verilerin korunmasına ilişkin esasların kanunla düzenleneceği hükmü gereği 07.04.2016

tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir. Kanunla kişisel veri işleyen gerçek ve tüzel kişilerin uyacakları ve usul ve esasların belirlendiği görülmektedir. Bu kapsamda kişisel verinin ancak belirli, açık ve meşru amaçlar için işlenebileceğinin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekliliğinin hüküm altına alındığı görülmektedir.

Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun ilgili maddelerinde de kişisel verilerin korunmasına yönelik düzenlemeler yapılmıştır. Ayrıca TCK 134., 135., 136. ve 138. Maddelerinde özel hayatın gizliliğinin ihlalinin, usule aykırı kişisel veri işleme, saklama ve açıklamanın suç olarak düzenlendiği anlaşılmaktadır. 2021 yılında yayımlanan İnsan Hakları Eylem planında da özel hayatın gizliliği ve korunması üzerinde durulmuştur. Ulusal hukuk alanında yapılan çok sayıda düzenlemeyle rağmen kişisel verileri koruyan suç tipleri ile özel hayatın gizliliğini ihlal suçu farkının belirlenmesinde birtakım zorluklar bulunmaktadır. Bu zorlukların aşılabilmesi için özel hayatın gizliliğini ihlal suçunun genel norm olarak kabul edilmesi gerekmektedir (Boğa, 2022;82)

1.2. Ulusal Güvenlik

Güvenlik insanın temel ihtiyaçlarından birisidir. Bireyin varlığını sürdürmesi ve diğer ihtiyaçlarını karşılayabilmesi güvenlik ihtiyacının karşılanmasına bağlıdır. İnsanın özgürce haklarını kullanabilmesi güvenliğin sağlandığı bir ortamda mümkün olabilmektedir. Temel bir hak olarak güvenliğin yoksunluğun diğer bütün haklardan da bir yoksunluk anlamına gelmektedir (Shue, 1996;30). Güvenliğin personel güvenliği, sektör güvenliği, kamu güvenliği ve ulusal güvenlik gibi farklı türleri bulunmaktadır. Ulusal güvenlik devlet güvenliği veya milli güvenlik olarak da isimlendirilmektedir ve diğer güvenlik türlerini de ihtiva eden şemsiye bir tanım konumundadır (Yılmaz, 2007;210-211).

Ulusal güvenlik devletin her türlü iç ve dış tehditlerden korunmuş bir biçimde hukuki, sosyal ve bağımsız bir biçimde varlığını sürdürebilmesi olarak tanımlanabilir (Beren, 2010;31). Devlet yetkili organlarını kullanarak güvenliği sağlamak, tehditleri bertaraf etmek, değerlerini korumak, çıkarlarını savunmak ve kendisine yönelik tehditlere karşı caydırıcı olmak için faaliyetler yürütür. Devletin vatandaşlarının özel hayatının gizliliğini korumak görevi olduğu kadar vatandaşlarını iç ve dış tehditlere karşı korumak ve kamu düzenini sağlamak görevi de bulunmaktadır. Anayasanın 5. maddesi devletin temel amaç ve görevlerinden birisinin, kişinin ve toplumun refah, huzur ve mutluluğunu sağlamak olduğunu vurgulamaktadır. Devlet bu görevini silahlı veya silahsız organlarını kullanarak icra etmektedir (Girgin, 2003;92). Devlet güvenlik faaliyetleri için ise askeri güç, kolluk gücü, lobiler, diplomatik kanallar, ekonomik güç, örtülü operasyonlar ve istihbarat örgütleri gibi araç ve yöntemleri kullanır (Yılmaz, 2007;301).

Devletin ulusal güvenliği sağlaması iç ve dış güvenliğin sağlanmasıyla mümkün olabilmektedir. İç güvenlik ülke sınırları içerisinde muhtemel tehdit ve saldırıların olmaması, devletin sabotaj ve benzeri tehlikelere karşı korunaklı olması ve vatandaşlarının huzur içinde olması anlamına gelmektedir. Dış güvenlik ise ülkenin yabancı devletlerden tehdit ve saldırılara karşı koyması ve başka devlet veya örgütlerin egemenliği altında kalmadan tam bağımsız olması anlamına gelmektedir. Devlet iç güvenliğin sağlanması için polis, jandarma, sahil güvenlik gibi kolluk güçlerini ve iç istihbaratı kullanırken dış güvenliği sağlamak için orduyu ve dış istihbaratı kullanmaktadır (Cin, 2008;3; Kuloğlu, 2015;16-17).

Türk hukukunda kolluk genel ve özel kolluk olarak tanımlanmıştır. Genel kolluk ülke genelinde kolluk hizmetlerini yürüten ve kamu düzeni sağlayan polis, jandarma, sahil güvenlik gibi birimlerdir. Özel kolluk ise özel alanların güvenliğinden sorumlu olan birimlerdir. Bunların suçları önleme ve işlenmiş suçları araştırma görevleri bulunmamaktadır (Güney, 2006;3). Kolluk ayrıca adli ve idari kolluk olarak da sınıflandırılabilir. İdari kolluk kamu düzenini sağlayan ve suçlar daha işlenmeden bunların önlenmesi için mücadele eden kolluktur. Adli kolluk ise suç işlendikten sonra görevi başlayan ve işlenmiş suçların aydınlatılması için görev yapan kolluktur (Günday, 2011;293).

1.3. Ulusal Güvenliğin Sağlanmasında Kolluk İstihbaratın Rolü

Ulusal güvenliğin sağlanabilmesi için gerekli faaliyetlerden bir tanesi istihbarattır. İstihbarat siyasi otorite tarafından talep edilen bilgilerin yasal olarak yetkilendirilmiş istihbarat birimleri tarafından toplanması, analiz edilmesi ve işlenmesi sürecidir (Kuloğlu, 2015;17). İstihbarat Arapça kökenli bir kelimedir ve yeni

öğrenilen bilgiler, haberler, duyular, bilgi toplama, haber alma anlamlarına gelmektedir (Pınarbaşı, 2014;47). İstihbaratın farklı tanımları yapılmaktadır. Bir tanıma göre istihbarat açık veya gizli kaynaklar kullanılarak kişiler, yerler, nesnelere ve olaylarla ilgili verilerin bilimsel yöntemlerle analiz edilmesi ve topluma veya devlete yönelik tehlikeleri önceden algılayarak, tedbir alması ve gelecekteki eylemlerin planlanması için yetkililere rapor edilmesi faaliyetidir (Yenisey, 2015;241). Bir başka tanıma göre ise istihbarat, gelecekte gerçekleşme olasılığı olan olaylarla ilgili en doğru tahmini yapabilmek için tarafsızlık, gizlilik, doğruluk ve süreklilik ilkelerine göre toplanan bilgilerin değerlendirilmesi, analiz ve sentezlenmesi faaliyetidir (Acar, 2011;73). İstihbaratın temel özellikleri olarak merkezden yönetilmesi, zamana bağlı olması, sürekli bir eylem olması, gizli olması, doğru olması, kesin olması, tarafsız olması, hukuka uygun olması, esnek olması, uzmanlık gerektirmesi, yenilikçi olması ve koordinasyon gerektirmesi özellikleri sıralanabilir (Acar, 2011;104-108).

İstihbarat faaliyetleri insanlık tarihi kadar eskidir ve siyasi, ekonomik ve güvenlik amaçlarla her toplumda binlerce yıldır uygulanmıştır. Ulusal güvenliğin sağlanması için istihbarat faaliyetleri zorunlu olarak görülmektedir (Avcı, 2004;12). Devletin tehditleri belirleme, tehditlere karşı bilinçlenme, önlemler arama ve politika belirleme arayışları istihbarat faaliyetlerini kullanılmasını ve bu alanda uzmanlaşma ve örgütlenmeyi beraberinde getirmektedir (Girgin, 2003). İstihbarat faaliyetleri sayesinde devletin güvenliği ve bekasını temin edildiği gibi devlet uygulamalarına da yön verilebilmektedir. Ayrıca istihbarat sadece güvenlik amacıyla değil ülkelerin diğer ülkelerle iyi ilişkiler geliştirmesinde ve işbirliklerinin artırılmasında da kullanılan önemli bir araçtır (Pınarbaşı, 2014;48).

İletişim ve ulaşım teknolojisindeki gelişmeler ve diğer teknolojik imkanlar devletlerin karşı karşıya kaldığı tehditlerin türünü ve şiddetini artırmaktadır. Buna bağlı olarak devletin ulusal güvenliği sağlayabilmek için karşı tedbirler alması ve bu tehditleri gerçekleştirmeden önleyecek uygulamalar geliştirmesi gerekmektedir (Pınarbaşı, 2014;38). Günümüzde ayrıca küreselleşme hiç olmadığı kadar hızlanmış, suçlar sınır aşan bir nitelik kazanmış, zengin ve fakir ülkeler arasındaki uçurum gerilimleri artırmış, yaşanan göçler nedeniyle toplumların yapısı farklılaşmış ve suç örgütleri ve suçlar için daha elverişli bir ortam oluşmuştur. Böyle bir ortamda özellikle terör suçları gibi örgütlü suçlara karşı istihbarat daha önemli bir konuma gelmiştir (Yenisey, 2012;7). Özellikle 11 Eylül tüm dünyada güvenlik kavramının yeniden ele alınmasına neden olmuştur. bu anlamda istihbarata verilen önemde de bir artış olmuştur. Ülkelerin güvenlik yaklaşımları farklılaşmış ve devlet organlarının faaliyetlerinin niteliği değişmiştir. Özellikle ABD’de ve Avrupa ülkelerinde üniversitelerde istihbarat eğitimi artırılmış ve sınıflar açılmıştır (Özdağ, 2009;38).

İstihbarat kullanma seviyelerine göre taktik, operasyonel ve stratejik istihbarat olarak sınıflandırılır. Stratejik istihbarat diğer ülkelere ve taraflara karşı ülke çapında stratejik kararlar alınması için kullanılan istihbarat türüdür. Operatif istihbarat orta vadede yapılması planlanan eylemlerle ilgilidir. Taktik istihbarat istihbari faaliyetlerin en küçük parçalarıdır ve kısa ömürlüdür. Güncel konu ve olaylarla ilgili hedef grupların taktik ve teknikleri hakkında toplanan istihbarattır. Oluşturma yöntemlerine göre istihbarat ise insan istihbaratı, görüntü istihbaratı, sinyal istihbaratı, açık kaynak istihbaratı, ölçüm ve iz istihbaratı olarak sınıflandırmak mümkündür (Avcı, 2004;11; Özdağ, 2008;146; Bayındır, 2016;16-20).

İstihbaratı yürüten kurumlara göre ise istihbarat devlet istihbaratı, askeri istihbarat, bakanlıklar ve diğer kurumlar tarafından yürütülen istihbarat ve kolluk istihbaratı olarak sınıflandırılabilir. Devlet istihbaratı Milli Güvenlik Teşkilatınca yapılan istihbarat faaliyetleridir. Askeri istihbarat Türk silahlı Kuvvetleri tarafından ülke güvenliğini tehdit eden unsurlara karşı yapılmaktadır. Dışişleri Bakanlığı, İçişleri Bakanlığı gibi bakanlıklar da kendi faaliyet alanları açısından istihbarat faaliyetinde bulunmaktadır (Pınarbaşı, 2014;40). Kolluk istihbaratı suç ve suçlulukla mücadele için polis ve jandarma tarafından yürütülen istihbarat faaliyetleridir. Suç öncesinde önleyici kolluk istihbaratı, suç sonrasında ise adli kolluk istihbaratı biçiminde sürdürülmektedir (Yenisey, 2015;383). Kolluk istihbaratı suçla ve suç örgütleriyle mücadele etmek, suçun işlenmesini önlemek, suçun bileşenlerini ortaya çıkartmak ve suç işleme yöntemlerini belirlemek için yapılır. Kolluk istihbarat birimleri adli birimlerle, olay yeri inceleme birimleriyle ve diğer kolluk birimleriyle irtibatlıdır (Kuloğlu, 2015;31). İç güvenlik istihbaratı ve kolluk istihbaratı birbirinden farklıdır. Kolluk istihbaratı suçla mücadele ve suçun önlenmesine odaklanmışken iç güvenlik istihbaratı suçun önlenmesi faaliyetlerinin yanında terörizmle mücadele ve casusluğu önleme faaliyetleri de yürütmektedir. suçun başarı ile önlenmesi için kolluk istihbaratı ile iç güvenlik istihbaratı arasında iletişim ve işbirliğinin varlığı gereklidir (Kızılırmak, 2018;119).

Kolluk istihbarat faaliyetinde bulunurken somut bir suç tehdidi olmasını beklemez. Kolluk istihbaratı kamu güvenliğini tehdit eden somut bir tehdit olmadan gizli bir biçimde gerçekleşmektedir (Karabulut, 2014;87). Bu sayede suç örgütlerinden veya münferit suçlulardan daha önce hareket geçerek suçun ortaya çıkmasına engel olunmaktadır (Birtok, 2011;101). Özellikle organize suçları önlemek ve gizli örgüt yapılanmalarıyla mücadele edebilmek için kolluğun istihbari faaliyetleri son derece önemlidir (Özbek, 2001;152). Kolluk suçla mücadele edebilmek için farklı iletişim araçlarıyla gerçekleştirilen iletişimi de denetleyebilmektedir (Centel, 2011;667).

Türk hukuk sisteminde kolluk istihbaratı tarafından elde edilen bilgiler delil niteliğinde değildir (Semiz, 2007;81). Alman hukukunda ise istihbarat faaliyetlerinde elde edilen bilgiler delili olarak kullanılabilir. Fransız hukuku ulusal güvenlik, bilimsel ve ekonomik kaynakların korunması, terörizm ve organize suçluluğun önlenmesi amacıyla kolluk tarafından yapılacak olan iletişim denetlemesine fişleme amacı olmamak kaydıyla müsaade etmektedir (Galli, 2016;669). Kolluk güçleri suçla mücadele etmek için yeni bilgi ve teknolojileri kullanmaktadır. Bunlardan bir tanesi drone kullanımınıdır. Bu uygulamanın özel hayatın gizliliği ve temel hak ve özgürlüklerin ihlali açısından dezavantajları tartışılrsa dahi ülkeler drone kullanımının şart ve esaslarını belirleyen yasal mevzuatları geliştirmek arayışındadırlar (Kaşlı, 2022;329).

Kolluğun istihbarat toplama yetkisi ve bu konuda yürüttüğü faaliyetler bazı tartışmaların odağı olmaktadır. Kolluk istihbaratının sadece örgütlü suçlarla sınırlı olması gerektiğini, bireysel suçlar için kolluk istihbaratının kullanılmaması gerektiğini savunan görüşler bulunmaktadır (Özbek, 2001;157). Ayrıca, her ne kadar kolluk istihbaratından beklenen önemli yararlar bulunsada dahi kolluk istihbaratı aşamasında henüz somut suç oluşumu gerçekleşmediğinden kişisel verilerin korunması hakkı ve özel yaşamın gizliliğine saygı hakkı bakımından bir müdahalenin olması durumu bulunmaktadır (Özbek, 2001;169). Örneğin, devlet bireysel haberleşme gizliliğine saygı duymak ve bu gizliliği ihlal etmemekle yükümlü olduğundan kolluğun farklı araçlar yoluyla yapılan iletişimi denetlemesi haberleşme hakkına ve özel hayatın gizliliği hakkına müdahale olarak kabul edilmektedir (Gözübüyük, 2016;360).

Kolluğun yürüttüğü istihbari faaliyetlerin denetlenmesi de bir diğer tartışmalı konudur (Güler, 2014). Türkiye’de istihbarat faaliyetlerinin tam anlamıyla denetlendiği söylenemez (Pınarbaşı, 2014;68). Bu alandaki denetimler özel olarak yetkilendirilmiş kişi ve komisyonlarca yapılmaktadır. Bu alandaki bir denetim mekanizması da meclis denetimidir. Meclis İnsan Hakları Komisyonu veya bu amaçla oluşturulacak başka komisyonlar aracılığıyla istihbaratın denetlenmesi mümkündür. Bu kapsamda, Türkiye’de istihbarat kurumları üzerinde Yasama, Yürütme ve Yargı organlarının koordinesinde bağımsız ve tarafsız bir denetim mekanizmasına ihtiyaç olduğu söylenebilir (Pınarbaşı, 2014;68).

1.4. Özgürlük ve Güvenlik Dengesi

İnsanlar özgür olmak ve bu özgürlüklerini güvenli bir ortamda kullanmak istemişlerdir. Bu iki durum birbiriyle bir tezat oluşturuyor gibi görünmektedir. Geçmişteki uygulamalar bu iki olguyu birbirinin alternatifini gibi algılandığını ve özgürlükler aleyhine çoğu zaman güvenliğin tercih edildiğini göstermiştir (Kuçuradi, 2018). Özgürlükler bireyin haklarını kullanabilmesi, insan onuruna yakışır bir biçimde yaşayabilmesi, potansiyelini geliştirip kullanabilmesi ve kendileri gerçekleştirebilmesi için gereklidir. Diğer taraftan güvenlik ise özgürlüğün kullanabilmesi için gereklidir. Güvenliğin olmadığı koşullarda bireyin kendisini özgür hissetmesi olası değildir (Erdoğan, 2013). Hiçbir özgürlük mutlak değildir ve kayıt ve şartsız kullanılamamaktadır. Devletin varlığının ve sürekliliğinin sağlanması için, güvenliğin ve kamu düzeninin teminatı için temel hak ve özgürlüklerin sınırlandırılması kaçınılmazdır. Bununla birlikte demokratik hukuk devletlerinde özgürlüklerin kısıtlanması meşru yasal kurallar çerçevesinde, zorunlu ve sınırlı olmalıdır. Ayrıca hak ve hürriyetlerin sınırlandırılması için kullanılan araçlar ile elde edilmek istenen amaçlar arasında bir orantı olması gereklidir (Gözler, 2011;144; Köksal, 2021;1763).

Günümüzde tüm yönetim sistemlerinin temel hak ve özgürlükleri temellerine alması ve bu bağlamda özgürlüklerin asıl güvenlik önlemlerinin ise istisna olması beklenmektedir. Özgürlükleri kısıtlayacak güvenlik önlemlerinin ise hukuki olarak düzenlenmiş bir biçimde uygulanması ve denetlenir olması istenmektedir. Uygulanacak güvenlik tedbirlerinin bireyin hak ve özgürlüğünü kısıtlamayı değil korumayı amaçlamalıdır. Demokratik bir devlette özgürlük ve güvenlik arasında bir denge aramak yerine bu kavramları birbirinin tamamlayıcısı gibi benimsemek ve özgürlüğün esas olduğunu kabul ederek özgürlüğü önceleyen

bir anlayış geliştirmek zarurettir (Çelik, 2015;237). Kolluk da görevini yerine getirirken odak noktasında insan hakları bulunmalıdır, meşruiyetini yasalardan almalıdır, ayırım yapmadan tüm vatandaşlara eşit muamele etmeli ve kişi hak ve özgürlüklerinin ancak bağımsız mahkemelerce kısıtlanabileceğinin bilincinde olmalıdır (Pınarbaşı, 2014;81).

2. Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi

2.1. İstihbarat Toplama

İstihbarat toplama ise iki yöntemle yapılmaktadır. Birinci yöntem açık kaynak istihbaratı olup özellikle internet ve sosyal medya üzerinden elde edilen verilerin işlenmesi yoluyla bilgiler, kişisel veri haline getirilerek işlenmekte ve değerlendirilmektedir. İkinci yöntem ise gizli bilgilerin elde edilmesi ve değerlendirilmesi yoluyla istihbaratın temin edilmesidir. Gizli bilgiler ise çoğunlukla parmak izi ve fotoğraf alma, MOBESE, plaka tanıma, iletişimin takibi, teknik araçlarla izleme, internet takibi (sosyal medya ve e posta), bankacılık işlemleri takibi, PNR, Genel Bilgi Sistemi (GBT) gibi önleyici kolluk işlemleri yoluyla ya da adli soruşturma sebebiyle teknik takip, gizli soruşturmacı görevlendirme, adli sicil kayıtları, hükümlü ve tutukluların kişisel verilerin tespiti ve kaydı gibi adli kolluk işlemleri yoluyla elde edilmektedir.

İdari kolluğun birinci görevi önleyicilik niteliği gereği kamu düzenini ve toplumu tehlikelerden korumaktır. İdari kolluğun toplumu tehlikelerden koruma görevinin gereği olarak da iç güvenliğe yönelik istihbarat toplama, kişisel veri işlemek durumunda olup buna yönelik yetkiler kullanmaktadır. İdari kolluğun bu yetkisinin ana kaynağını ise Polis Vazife ve Salahiyetleri Kanununun (PVSK) Ek 7. maddesi oluşturmaktadır. PVSK'nın Ek 7. maddesinin ilk fıkrasında polislinin genel istihbarat toplama yetkisinin, 2-5. fıkralar arasında önleme amaçlı iletişimin tespiti ve kaydı yetkisinin, 6. fıkra ile teknik takip yetkisinin düzenlendiği görülmektedir. Yine maddenin 7. fıkrasında toplanan kişisel verilerin gizliliği ve korunmasına, 8-9. fıkralarda ise bu madde kapsamında icra edilen faaliyetlerin denetimine ilişkin hükümler yer almaktadır. Maddenin 10-11. fıkralarında ise yukarıdaki esaslara aykırı elde edilen verilerin hukuken geçerli olmayacağına ve bu maddenin uygulanmasına ilişkin esas ve usullerin yönetmelikle gösterileceğine ilişkin hükümler yer almaktadır.

Kolluğun istihbarat toplama yetkisini düzenleyen bir diğer mevzuat Jandarma Teşkilat Görev ve Yetkileri Kanunudur (JTGYK). Bu kanunun Ek 5. maddesinde ise ülke çapında genel istihbarat toplama yetkisi ve ülke çapında iletişimin tespiti ve kayda alınması yetkisi hariç aynı yetkilerin jandarmaya da verildiği görülmektedir. Düzenlemeye göre Jandarma sadece kendi sorumluluk alanı ile sınırlı olmak üzere istihbarat toplama, iletişimin tespiti ve kaydı ile teknik takip yetkisine sahiptir. JTGYK'nun 7/a. fıkrası Jandarmanın istihbarat toplam yetkisinin kaynağını oluşturmaktadır. Düzenlemeye göre jandarma *emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almakla* yükümlüdür.

2.2. Telekomünikasyon Yoluyla İletişimin Tespiti, Dinlenmesi, Kayda Alınması

Telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması yetkisi genel idari kolluk olan polis, jandarma ve devlet istihbaratını üretmekten sorumlu MİT'na verilmiş bir görev ve yetkidir. Kolluğun telekomünikasyon yoluyla iletişimi tespiti, dinlemesi ve kayda alması adli ve idari gerekçelerle olabilmektedir. Ceza Muhakemesi Kanununun (CMK) 135-138. maddelerinde adli kolluk faaliyetleri kapsamında iletişimin tespiti ve kayda alınmasına ilişkin hükümler yer almaktadır. Bu maddeler kapsamında adli kolluk tedbiri olarak iletişimin tespiti ve kaydı mümkün olduğu gibi önleme dinlenilmesi sonucu kuvvetli suç şüphesi oluşması halinde önleme dinlenilmesi, CMK'nın bu hükümleri kapsamında adli tedbire dönüştürülmektedir. Kuvvetli suç şüphesi varlığı halinde önleme dinlemesi sona erdirilmeli, diğer koşulların varlığı halinde CMK 135. maddesi kapsamında yeni bir karar alınarak adli dinlemeye geçilmelidir (Özbek, Doğan ve Bacaksız, 2023;169).

İdari Kolluk önleme tedbiri olarak ancak şu dört amaçla kullanabilmektedir: İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler. Cep telefonu ve GPS verileri üzerinden kişilerin konum bilgisi tespiti yetkisi, önleyici tedbir kapsamında idari kolluğa tanınmamıştır. Bu tespit ancak CMK 135/5

AIHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması bağlamında suç soruşturmaları kapsamında adli tedbir olarak mümkündür (Öztürk, Kazancı ve Güleç, 2021;279).

Polis, PVSK'nın Ek 7., Jandarma ise JTGYK'nın Ek 5. ve casusluk hariç terör suçları dâhil Terörle Mücadele Kanunu (TMK) geçici 14. maddesinde yer alan suçların önlenmesi için iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması yetkisini kullanabilir. PVSK 7/1'de sayılan amaçlar şunlardır: "Polis, *Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişini sağlamak üzere, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur; bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar.*" JTGYK 7/a fıkrasında sayılan amaçlar şunlardır: "... emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almak".

PVSK'nın 7/2. fıkrası gereği polis ve jandarma tarafından, ancak silahlı terör örgütüne ilişkin suçları da içeren anayasal düzene ve bu düzenin işleyişine karşı suçlar dâhil TMK Geçici 14/6. fıkrasında sayılan suçların önlenmesi amacıyla hallerde iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kaydının alınması mümkündür. Bununla birlikte bu yetkinin kullanılabilmesi için sayılan suçların işlenebileceğine dair makul şüphenin bulunması gerekmektedir (Centel ve Zafer, 2018;483). Adli ve Önleme Aramaları Yönetmeliği 6. maddesine göre, "makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir". PVSK'nın 4/A fıkrasında düzenlenen durdurma ve kimlik sorma yetkisi ile 9. maddesinde düzenlenen önleme araması tedbirleri için de makul sebep öngörülmekte olup iletişimin tespiti ve kaydı tedbiri içinde, idari kolluk talep yazılarında makul sebebi ortaya koymalıdır (Yenisey, 2015;331). Şen'e göre makul sebepler somut bilgi ve bulgulara dayanmalıdır (Şen, 2011;69). Aslında, idari kolluğun istihbarat toplama ve istihbarat toplama araçlarından biri olan önleme amaçlı iletişimi tespit, dinleme ve kaydı görevi PVSK 7. madde ve JTGYK'nın 7/a fıkrası ile kolluğa verilen suçu önleme görev ve yetkisinden kaynaklanmaktadır. Kolluğun önleme yetkisinin amacı ileriye yönelik olup, suç işlenmesi tehlikesini önlemek ve gelecekte doğabilecek tehlikeleri yaratan sebepleri ortadan kaldırmaktır. Önleme görevi, suç işleninceye kadar olan safhadan oluşmaktadır.

İdari Kolluk ancak makul şüphe üzerine hâkim kararı veya gecikmesinde sakınca bulunan hallerde polis ve jandarma yetkilisinin (*poliste emniyet genel müdürü veya istihbarat daire başkanı, jandarma da ise J.Gn.K. veya istihbarat başkanı*) yazılı emri ile yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilmekte, dinleyebilmekte, sinyal bilgileri değerlendirilebilmekte ve kayda alabilmektedir. Polis ilave olarak internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edebilmekte, dinleyebilmekte, sinyal bilgileri değerlendirilebilmekte ve kayda alabilmektedir. Yetkinin kapsamı iletişimin tespiti, telekomünikasyon yoluyla yapılan iletişimi tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kaydıdır. Yönetmeliğe göre, iletişimin dinlenmesi ve kayda alınması işlemi içine; telekomünikasyon yolu ile yapılan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınması işlemleri girmektedir.

İletişimin tespitine ilişkin kolluk yetkilileri tarafından gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hâkimin onayına sunulmaktadır. Yetkili hâkim Ankara ağır ceza mahkemesi üyesidir. Hâkim, kararını en geç kırk sekiz saat içinde vermektedir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde, tedbir derhal kaldırılmakta ve bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilmektedir (Centel ve Zafer, 2018;483). Adli dinlemede halen acele hallerde cumhuriyet savcılarının tarafında verilen adli dinleme kararı yirmi dört saat içinde hâkimin onayına sunulmaktadır. Önleme dinlemesinin özel ve aile hayatının gizliliğine önemli ölçüde sınırlandırdığı dikkate alındığında, özgürlük ve güvenlik dengesinin korunması bakımından verilen idari kararın hâkim onayına sunulma süresinin yirmi dört saat olan süresinin 2005 yılında yapılan değişiklikle kırk sekiz saate çıkartılmış olması sakıncalı görülmektedir (Yenisey 2015;331).

Tedbir kararı üç ay için verilmektedir. Her seferinde üç ayı geçmemek üzere en fazla üç defa uzatılmaktadır. Tedbir ile elde edilen bilgiler ancak tedbirin amacını düzenleyen PVSK'nın 7/1. ve JTGYK'nın 7/a fıkrasında gösterilen amaçlar için kullanılabilir. Elde edilen kayıtlar gizli olup ihlali halinde cumhuriyet savcılarınınca doğrudan soruşturma yapılabilir. Tedbire ilişkin faaliyetlerin denetimi; sıralı kurum amirleri, mülki idare amirleri, J.Gn.K.ıgı/Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları tarafından yılda en az bir defa yapılmaktadır. Denetimlerin sonuçları bir rapor hâlinde Türkiye Büyük Millet

Meclisi Güvenlik ve İstihbarat Komisyonuna sunulmaktadır. İletişimi denetleme yetkisinin üç ay süreyle uygulanacağı ve bu sürenin en fazla üç kez aynı süre ile uzatılabileceği hükme bağlanmışken terör suçları için yapılan iletişim denetleme süre uzatımına bir sınır konulmamıştır. Bu hüküm de özel hayatın korunması hakkının korunması açısından bir risk oluşturmaktadır (Birtek, 2011;116). Ayrıca, kanunlarda hangi suç türlerine karşı kolluğun izleme yapabileceği belirlenmiş olmasına karşın kolluğa verilen iletişimin denetlenmesi yetkisi kişiler bakımından sınırlandırılmamıştır ki bu durum bu tedbirin herkes için kullanılabilmesi anlamına gelmektedir (Yüksel, 2012;112). Bir diğer sorun da kayıtların imhasıyla ilişkilidir. Her ne kadar iletişimi denetleme tedbirinin sona ermesini takiben 10 gün içerisinde kayıtların imha edileceği belirtilse dahi bu uygulamadan hakkında işlem yapılan kişi haberdar edilmemektedir ki bu uygulama Anayasanın 125. maddesiyle uyumsuzdur.

Elde edilen verilerin belirtilen amaçlar dışında ceza muhakemesine tabi diğer davalar bakımından kullanılması mümkün değildir (Yenisey, 2015;369). Yargıtay'ın 17.05.2011 tarih ve 9/93-95 sayılı kararında önleme amaçlı iletişimin tespiti, dinlenmesi ve kaydı ile elde edilen verilerin ceza yargılamasında kullanılmayacağını teyit etmekle birlikte, ceza soruşturmasının başlatılmasına dayanak oluşturabileceğine hükmettiği görülmektedir. Yetkinin sayılan amaçlar dışındaki başka amaçlarla, açık veya gizli olarak kullanılması mümkün değildir (Şen, 2011;69). Aksi halde yapılan tespitler, hukuka aykırı elde edilen delil olarak kabul edilmektedir. Ünver ve Hakeri'ye göre elde edilen verilerin başka bir suç için kullanılmaması anlamsızdır ve CMK 138. maddesinde olduğu gibi bir düzenlemeye ihtiyaç bulunmaktadır (Ünver ve Hakeri, 2021;487). Öztürk, Kazancı ve Güleç'e göre, yasada gösterilen amaç dışında kullanım, kişi hakkındaki tedbiri genel bir dinleme ve takibe dönüştüreceğinden, hukuka aykırılık oluşturmaktadır (Öztürk vd., 2021;312).

2.3. Teknik Araçlarla İzleme Yetkisi

Teknik araçlarla izleme, iletişimin tespiti ve kaydına benzer bir tedbirdir. Ancak bir fark bulunmaktadır. İletişimin tespiti ve kaydı yetkisinde kişilerin telekomünikasyon yoluyla yapmış olduğu haberleşme takip edilmektedir. Teknik araçlarla izleme yetkisi ile ise telekomünikasyon araçları yoluyla yapılan haberleşme dışındaki konuşma ve faaliyetleri takip edilmektedir. Teknik araçlarla izleme de belirli bir yerdeki seslerin, gürültünün, konuşmaların, arka plandaki tüm ses ve sohbetlerin, kişilerin faaliyetlerinin tespiti amacıyla yapılan bir alanın veya kapalı bir yerin dinlenmesi ya da fotoğraf, film gibi yöntemlerle görüntüsünün alınması söz konusudur. Dronlar ile yapılan izleme de bu kapsamda kalmaktadır (Ünver ve Hakeri, 2021;484). İdari kolluğun teknik araç kullanmaksızın gözle yapmış olduğu izleme ve kayıt tutması genel istihbarat yetkisi kapsamında her zaman mümkündür. Bu hal PVSK, JTGYK ve CMK kapsamında teknik araçlarla izleme teşkil etmemekte ve herhangi bir savcılık ve hâkim kararının da gerektirmemektedir.

Önleme amaçlı teknik araçlarla izleme yetkisinin, PVSK'nın 7/6. ve JTGYK Ek 5/6. fıkrasında düzenlendiği görülmektedir. Delil elde etme amaçlı adli teknik araçlarla izlemeye ilişkin esaslar, CMK'nın 140. maddesinde yer almaktadır. Önleme amaçlı düzenlemeye göre polis ve jandarma, yine iletişimin tespiti ve kaydı yetkisinde olduğu gibi PVSK'nın 7/1. ve JTGYK'nın 7/a fıkrasında sayılan aynı amaçlarla TMK Geçici 14. maddede sayılan suçlar bakımından terör suçları dâhil teknik araçlarla izleme yetkisine sahiptir. PVSK'nın 7/6. fıkrasına göre Polis jandarmadan farklı olarak, genel istihbarat yetkisi kapsamında da önleme amaçlı teknik araçlarla izleme yetkisine sahiptir. Teknik araçlarla izleme için gecikmesinde sakınca bulunan hal öngörülmemiş olup yetkinin kullanımı için hâkim kararı gerekmektedir. Yetkili mahkeme kolluğun görev yeri sulh ceza mahkemesidir.

Düzenlemelerde önleme amaçlı teknik araçlarla izleme yetkisi için süre belirlenmediği görülmektedir. Bizim de katıldığımız görüşe göre temel hak ve özgürlüklere müdahale oluşturan böyle bir yetkinin süresiz düzenlenmesi, başta hukuk devleti ilkesi olmak üzere hukukun genel ilkelerine aykırılık teşkil etmektedir (Özbek vd., 2023;169). CMK'nın 140. maddesinde yer alan, adli amaçlı teknik araçlarla izleme için belirlenen sürelerle benzer düzenleme yapılmalıdır. Yine uygulanan tedbirin sona ermesi halinde elde edilen verilerin yok edilip edilmeyeceğinin de düzenlenmediği görülmektedir. Kanaatimizce elde edilen veriler kişisel veri olduğundan, iletişimin tespiti ve kaydı yetkisinde olduğu gibi hâkim tarafından talebin reddi halinde tedbir derhal kaldırılmalı ve kayıtlar en geç on gün içinde yok edilmelidir. Elde edilen verilerin ancak sayılan amaçlar yönelik olarak kullanılması mümkündür. Elde edilen verilerin önleme dinlemesi tedbirinde olduğu gibi gizliliği söz konusu olup gizliliğin ihlali halinde cezai soruşturma açılmaktadır. Dinleme tedbirindeki

aynı esaslarla denetime tabidir. CMK'nın 140/5. fıkrasında kişilerin konutunda delil etmek için izleme yapılmasını açıkça yasaklandığı halde, PVSK'nın 7/6 ve JTGYK'nın Ek 5/6. fıkrasında buna yönelik bir düzenleme bulunmamaktadır. Ünver ve Hakeri'ye göre konutta iletişimin dinlenmesi ve kaydı mümkün iken mafya suçlarının çoğunlukla işyeri ve konut olarak kullanılan çiftliklerde organize edildiği düşünüldüğünde CMK'nın 140. maddesinde böyle bir kısıtlama öngörülmesi yersizdir (Ünver ve Hakeri, 2021;486). Bizim de katıldığımız görüşe göre düzenlemenin mefhumu muhalifinden ortam dinlemesinin ancak önleme amaçlı mümkün olduğunu söylemek mümkündür (Yenisey, 2015;362).

İdari kolluğa teknik araçlarla izleme yetkisi veren bir diğer düzenlemede 2911 sayılı Kanunun 11/Ek fıkrasında yer alan, toplantı ve gösteri yürüyüşü katılımcıları ve konuşmalarının ses ve görüntülerinin kaydı yetkisidir. Düzenlemeye göre *“toplantı ve gösteri yürüyüşlerinde katılımcıların ve konuşmacıların ses ve görüntüleri kolluk tarafından yapıldığı belli olacak şekilde kaydedilebilir. Elde edilen kayıt ve görüntüler şüphelilerin ve suç delillerinin tespiti dışında başka bir amaçla kullanılamaz.”* Aslında düzenlemede verilen yetki adli soruşturma amaçlı olmakla birlikte kayıt altına alma caydırıcılık sağlaması bakımından suç işlenmesinin önlenmesine de katkı yapmaktadır.

Önleme maksatlı teknik araçla izleme araçlarından birisi de MOBESE sistemidir. MOBESE, mobil elektronik sistem entegrasyonu kelimelerinin baş harflerinin birleşimi oluşmuş bir kelimedir. Amacı şehrin ana cadde ve meydanlarında, kritik kavşaklarda, şehrin giriş ve çıkış noktalarında anlık görüntü almaktır. Suç işlenmesinin önlenmesi kapsamında önleyici bir izleme tedbiri olarak ortaya çıkmaktadır. Son zamanlarda ayrıca plaka tanıma sistemleri ile de entegre edilmiş durumdadır. Başlangıçta suç ve suçluluk ile mücadele bağlamında bir tedbir olarak ortaya çıksa da zamanla yaygınlaşmış ve hatta özel şahıslar tarafından site apartman giriş ve çıkışlarının dahi izlenir hale geldiği görülmektedir. Son dönemde MOBESE'nin artık geniş çaplı izleme ve takibe dönüştüğü ve araç plakası, kişisel kimlik tespiti kapsamında fotoğraf ve görüntü alınır hale geldiği gözlemlenmektedir. Ancak bugün için ne PVSK ne de JTGYK'da buna yönelik önleyici tedbir kapsamında bir düzenleme bulunmamaktadır. İstihbarat toplama yetkisi kısmında ifade edildiği gibi her türlü kişisel veri işleme faaliyeti temel hak ve özgürlüklere kısıtlama getirmektedir. Anayasa 13. maddesi bağlamında her türlü sınırlandırmanın kanunla yapılması anayasal sebeplere bağlı olması dikkate alındığında bu tür bir yetkinin koşullarının kanunla belirlenmemiş olmaması sorundur. Konunun iç hukukta kanunla ve açıkça düzenlenmesi zorunludur.

Kişisel verilerin korunması özel hayatın gizliliğinin korunması hakkı çerçevesinde ele alınan bir konudur. Kolluk faaliyetleri ile kişisel verilerin korunması arasında yakından ilişkisi bulunmaktadır. Ancak, kolluk faaliyetleri açısından kişisel verilerin korunmasını düzenleyen genel hükümler ile özel hükümler arasında farklılıklar mevcuttur. Ayrıca Türk kolluk birimlerinde uygulanan kişisel verilerin korunmasıyla ilgili faaliyetler ile Eurapol ve 2016/680 sayılı Kolluk-Ceza Adaleti Direktifi hükümleri arasında da tam bir uyumluk bulunmamaktadır. Bu uyumun sağlanması için düzenlemeler yapılması zorunludur (Kaşlı, 2023;97).

3. AİHM Perspektifinden Özel Hayata ve Aile Hayatına Saygı Hakkı

3.1. AİHM Kararlarına Göre Özel Hayata ve Aile Hayatına Saygı Hakkının Kapsamı

Özel ve aile hayatına saygı hakkının, AİHS 8/1. fıkrasında *“herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir”* şeklinde düzenlendiği, 2. Fıkrasında ise meşru sınırlandırma sebeplerine yer verildiği görülmektedir. Sözleşmede sayılan özel hayat, aile yaşamı, konut ve haberleşmenin ne olduğu tanımlanmamış olup kapsamının 1994 tarihli Murray v. UK gibi AİHM içtihatları ile şekillendiği ve zaman içinde genişlediği anlaşılmaktadır (Harris, O'Boyle ve Warbrick, 2022;471). Kapsamlarının belirlenmesindeki güçlük nedeniyle AİHM tarafından kavramların, önüne gelen başvurunun somut koşullarında değerlendirildiği görülmektedir (Gözübüyük ve Gölcüklü, 2011;334).

Maddenin aslı işlevi sayılan dört hakka yönelik olarak devletin keyfi müdahalesinin önlenmesine yönelik negatif yükümlülüktür (Şen, 1996;8). Amacı kişiye kişiliğini geliştirme imkânı sağlayan, devlet tarafından rahatsız edilmeyeceği özerk bir alan sağlamaktır (Özbudun, 1977;265). Negatif yükümlülük düzenlenenin asli amacı olarak görülmektedir (Harris, O'Boyle ve Warbrick, 2022;472). Bunun yanında devletin, kişileri diğer özel kişilerin faaliyetlerinden koruma dahil maddede sayılan hakların etkin olarak kullanılmasına imkân sağlayacak koşulları oluşturma pozitif yükümlülüğü de bulunmaktadır. Pozitif yükümlülük sayılan hakların kullanımı bakımından usulü güvenceleri sağlanmasını da kapsamaktadır. Sayılan haklar medeni haklardan

olup bunlarla ilgili kararların adil yargılanma hakkı kapsamında usulü güvencelere tabi olmasını gerektirmektedir. Usulü gereklilikler önleyici arama, önleyici teknik ve fiziki takip önleyici kolluk tedbirlerinin uygulanmasında da hâkim kararı denetimine tabi olmayı gerekli kılmaktadır.

AİHS 8/1. Fıkra ile özel hayat, aile yaşamı, konut dokunulmazlığı ve haberleşme dokunulmazlığı olmak üzere dört menfaat korunmaktadır. Özel hayat kavramı oldukça geniş olup neleri kapsadığının AİHM içtihatları ile şekillendiği görülmektedir (Gözübüyük ve Gölcüklü, 2011;330-331). Mahkeme özel hayatı, aleniyetten korunma ve mahremiyetten ibaret saymamakta bir kişinin hayatı keyfi olarak müdahale ve rahatsızlıklardan korunmuş olarak yaşayabilmesine imkân sağlanması olarak anlamaktadır (1992 tarihli Niemetz v. Almanya kararı). İlişkilerin kişisel nitelikte olmasının gerekmediği avukatlık ofisinin aranmasında olduğu gibi mesleki faaliyetlerden kaynaklanan ilişkileri de kapsadığı vurgulanmaktadır. Kişisel verinin korunması (1981 tarihli X v. Almanya kararı) ile kişinin psikolojik ve ruhsal bütünlüğünü de kapsadığı ifade edilmektedir (1985 tarihli X ve Y v. Hollanda kararı). AYM’de kararlarında özel hayatın dokunulmazlığını geniş yorumlamakta, özel hayatın kişinin sadece yaşamını istediği gibi sürdürmeye indirgenemeyeceğini, sosyal bir yaşam sürdürmesini de güvence altına aldığına, açıkça belirtilen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunacağına vurgu yapmaktadır (2015 tarihli Faris Korkmaz vd. kararı). Buna karşılık kamuoyuna mal olmuş kişiler hayatlarının kişiye özel niteliğinin bir kısmını kaybetmektedir (Gözübüyük ve Gölcüklü, 2011;336).

Aile yaşamı kavramı, ailenin kurulması, evlilik dışı dahil çocukların durumunu, ebeveyn çocuk ilişkileri girmektedir (Harris, O’Boyle ve Warbrick, 2022;475-476). Kardeşler arasındaki, amca yeğen arasındaki büyükbaba/anne torun ilişkileri de aile yaşamı kapsamına girmektedir (2010 tarihli Mustafa ve Armağan Akın v. Türkiye kararı). Ancak bu halde müdahalenin orantılılığı incelenirken akbabalık bağının uzaklığı genellikle dikkate alınmaktadır (1994 tarihli Boyle v. UK kararı). Konut, kişinin yerleşik olarak yaşadığı yer ve genel ve özel yaşamını geliştirdiği fiziksel olarak belirlenmiş bir yer olarak tanımlanmaktadır (2006 tarihli Giacomelli v. İtalya kararı). Konut kişinin, ikinci evini, yazlığını, ofisini de kapsamaktadır (2008 tarihli Fagersgiöld v. İsveç kararı). Haberleşme dokunulmazlığı ise şekli ve içeriği ne olursa olsun özel iletişimin korunmasını amaçlamaktadır (2008 tarihli Michaud v. Fransa kararı). Teknik gelişmelere bağlı olarak mektup, telefon, e-posta, çağrı cihazı ve internet üzerinden iletişim vb. kapsamaktadır (2010 tarihli Kenedy v. UK kararı) Haberleşme dokunulmazlığı içine ayrıca genel belgeler ve dosyalar, sadece kişisel yazışmalar değil iş yaşamından kaynaklı yazışma ve belgelerde girmektedir (1990 tarihli Huwig v. Fransa kararı).

3.2. AİHM’in Özel Hayata ve Aile Hayatına Saygı Hakkının İhlali Başvurularındaki Tutumu

Terörle mücadele açısından devletlerin AİHS 8/1. Fıkra bağlamında kişilerin üst, araç ve konutlarının aranması ve el koyma, konutun korunması (yıkımama, tahrip etmeme vb.), haberleşmenin korunması bağlamında keyfi müdahale etmeme şeklinde negatif yükümlülüğü bulunmaktadır. Özel hayat ve haberleşmenin korunması kapsamında ise istihbarat amaçlı gizli takip (telefon dinlemeleri, teknik takip) yöntemleri ile müdahalelerde ve elde edilen kişisel verilerin toplanması ve işlenmesinde hem keyfi müdahale etmeme hem de usulü güvenceleri takip etme sorumluluğu bulunmaktadır.

Mahkeme AİHS 8. Maddenin ihlaliyle ilgili önüne gelen başvuruda ilk önce başvurunun 8. Madde kapsamında olup olmadığını incelemektedir. Eğer giriyorsa devletin negatif ve pozitif yükümlülüklerle aykırılığı incelenmektedir. Negatif yükümlülüğe aykırılık iddiasında devletin, 8/1. Fıkrasına aykırı davranıp davranmadığı, müdahalenin hukuka uygunluğu (yasallığı), 8/2. Fıkra bağlamında meşru amaca yönelik olup olmadığı, nihayetinde müdahalenin demokratik toplum gerekleri bakımından zorunlu olup olmadığını incelenmektedir. Pozitif bir yükümlülüğün ihlali başvurusunda ise menfaatin önemini ve karşı karşıya gelen menfaatler arasındaki dengeyi göz önünde bulundurarak ileri sürülen pozitif yükümlülüğün devlet açısından gerekli olup olmadığı, ölçülülüğü incelenmektedir (Kilkelly, 2001;43).

Müdahalenin hukuka uygunluğu usulü güvenceler bakımından önem taşımakta olup Mahkeme müdahalenin iç hukukta düzenlenmiş olup olmadığını incelemektedir. İç hukukta müdahalenin koşullarının belirli olmasını, etkin ve yeterli usulü güvencelerin varlığını aramaktadır. Düzenlemenin, açık, erişilebilir ve öngörülebilir olması, keyfi müdahaleyi önleyici tedbirler içermesi ve etkin bir denetim mekanizmasını sahip olması gerekmektedir. Takdir yetkisi ve sınırlarının belirlenmiş olması da gerekmektedir (Gözübüyük ve Gölcüklü, 2007;331). İç hukukta müdahalenin koşulları belirlenmiş olsa da sınırlandırma yine düzenlemeye aykırı ise tek başına ihlal için yeterli görülmektedir (Kilkelly, 2001;43).

Meşru amaçlara uygunluk bağlamında, AİHS 8/2. Fıkrası gereği sayılan haklara müdahale ancak ulusal güvenlik, kamu düzeninin korunması ve suç işlenmesinin önlenmesi, genel sağlık ve ahlak ile başkalarının hak ve özgürlüklerinin korunması amacıyla mümkündür. Sınırlandırma nedenleri sınırlı olarak sayılmış olup hakkın kullanımına güvence teşkil etmektedir. Sayılan nedenlere dayanmayan örtülü sınırlandırmalar ihlal niteliği taşımaktadır (Özdek, 2004;222). Bunların yanında müdahalenin son olarak da demokratik toplum için gerekli olması gerekmektedir. AİHM önün gelen başvurularında son olarak demokratik toplu bakımından gereklilik incelemesi yapmakta, müdahalenin meşru amaç ile ölçülü olmasını aramaktadır (Metin, 2017;27-28). Ölçülülük/orantılılık incelemesinde ise meşru amaçla, amaca ulaşmak için kullanılan araç arasındaki, yani sınırlandırma ile elde edilecek kamu yararı ile sınırlamadan doğan bireysel zarar arasındaki dengenin varlığını aramaktadır (Dost, 2018;386).

3.3. AİHM Kararlarında Terörle Mücadele Amaçlı Gizli İzleme ve Takip ile Özel Hayata ve Aile Hayatına Saygı Hakkı İlişkisi

AİHM'e göre gizli izleme ve takip kişinin özel alanına tecavüz oluşturmakta ve bu nedenle özel hayat kapsamına girmektedir. Çoğu zaman haberleşme ve konut hakkına saygı hakkını da ilgilendirmektedir. Gizli izleme ve takip idari kolluk tarafından kamu düzeninin korunması amacıyla kapalı devre kamera sistemleri ile dahil internet ortamında izleme, teknik araçlarla (GPS vb.) takip, telekomünikasyon yoluyla iletişimin takibi (telefon, internet iletişimi vb.) şeklinde ortaya çıkmaktadır. Aynı zamanda kişisel verinin toplanması ve işlenmesine yol açması bakımından kişisel verilerin korunması gerekliliğini de ortaya çıkarmaktadır.

AİHM'in terörle mücadele amaçlı *telefon dinlemeleri dahil gizli takip* ile ilgili esasları belirlediği ilk kararı 1978 tarihli *Klass ve diğerleri v. Almanya* kararıdır. Mahkeme, terörle mücadele amaçlı posta ve iletişim araçlarında yapılacak gizli izlemenin kanunla öngörülmesi ve ancak istisnai durumlarda kamu düzenini korumak ve suç işlenmesini önlemek amacıyla demokratik toplum için gerekli olduğu ölçüde mümkün olduğunu vurgulamaktadır. Karara göre gizli izleme işlemlerinin nasıl yapılacağına devletlerin takdirine bırakıldığı görülmektedir. Ancak bu durumun, yetkinin sınırsız kullanılabileceği anlamında gelmediği, hangi gizli izleme yöntemi kullanılırsa kullanılsın, devletin gizli izleme yöntemlerinin kötüye kullanımının önleyecek yeterli ve etkin güvenceleri temine zorunlu olduğu vurgulanmaktadır. Önüne gelen başvuruda incelemenin ise tedbirin niteliğine, kapsamına ve süresine, tedbire ihtiyaç duyulma sebeplerine, tedbiri uygulayan kolluk makamlarına ve iç hukukta getirilen denetim mekanizmasına göre yapılacağı ifade edilmektedir. Mahkemenin usulü güvencelerin varlığını sıkı bir şekilde aradığı anlaşılmaktadır. Mahkemenin kararında terörle mücadele amaçlı gizli takip yetkisini tanıdığı ve ancak bu yetkinin kötüye kullanılmasını önleyecek etkili ve yeterli güvencelerinde bulunmasını da aradığı anlaşılmaktadır. Dolayısıyla incelemeye konu olan başvuruda etkin ve yeterli önlemlerin alındığı gerekçesiyle ihlal bulunmadığına karar verdiği görülmektedir (1988 tarihli *Spillman v. İsviçre* kararı). Buna karşılık Mahkemenin sonraki birçok kararında gizli takibi meşru amaç bakımından (ulusal güvenlik, kamu düzeni ve suç işlenmesinin önlenmesi) uygun görmekle birlikte usulü güvenceleri yetersiz bulduğu ve tedbiri demokratik toplum gerekleri bakımından zorunlu bulmadığı anlaşılmaktadır (2017 tarihli *Mustafa Sezgin Tanrıkulu v. Türkiye* kararı).

Mahkemenin *iletişimin tespiti, dinlenmesi ve kaydıyla ilgili verdiği* bir diğer önemli kararı 2000 tarihli *Khan v. Birleşik Krallık* kararıdır. Olayda telefon dinlemenin ayrıntılarının idari uygulama ile düzenlendiği görülmektedir. Mahkemenin uygulama ile getirilen takdir yetkisini, kullanma şekli ve kapsamı bakımından incelediği ve yetkinin kapsamının yeterince açık olmadığı, bu nedenle hukuka uygun olmadığı gerekçesiyle ihlale karar verdiği görülmektedir. Mahkemenin kararında telefon dinlemeye ilişkin düzenlemede hangi hususların yasal olarak düzenlendiği, hangi hususların ise yürütme organının takdirine bırakıldığı noktasında yeterli açıklık bulunmadığı tespitinde bulunarak, yapılan dinlemenin hukuka uygun olmadığına karar verdiği anlaşılmaktadır. Buna karşılık Mahkemeye göre hukuka uygunluk ve yasallık ilkesi, dinlemenin amacını tehlikeye atmaması için dinlenen kişiye ne zaman dinleneceğine dair uyarı yapılmasını gerektirmemektedir (Harris, O'Boyle ve Warbrick 2022;504). Ayrıca yasanın telefon dinlemesi mümkün olan suçları sayarak tüketmesi gerekmektedir (2010 tarihli *Kenedy v. UK* kararı).

Telefon dinlemelerine ilişkin bir diğer durumda telefonu dinlenenin yanında, telefonu dinlenen ile görüşen diğer kişilerin durumudur. AİHM önüne gelen bir başvuruda kendisinin telefonu dinlenmediği halde konuştuğu kişinin telefonunun dinlenmesi nedeniyle kendisinin de dinlenmesinin yasal mevzuatın kişi için

etkin ve yeterli koruma sağlamadığı gerekçesiyle ihlale karar verdiği görülmektedir (1998 tarihli Lambert v. Fransa kararı). Mahkeme bir telefon dinleme tedbirinin hukuka uygun kabul edilebilmesi için, dinleme kararı verilebilecek suçların niteliği, dinleme yapılabilecek kişilerin kategorisinin, dinlemenin süresinin belirliliğini, elde edilen verilerin kullanılmasında ve saklanmasıdaki usul ve esasların varlığını, verilerin paylaşımına ilişkin esasların varlığını, imha edilmesine ilişkin esasların varlığını aramaktadır (Harris, O'Boyle ve Warbrick, 2022;504). Tedbire ilişkin etkin ve yeterli ve bağımsız denetim mekanizmasının varlığını ise demokratik toplum bakımından gereklilik incelemesinde dikkate almaktadır (2015 tarihli Roman Zakharov v. Rusya kararı).

Mahkeme, diğer koşullar yanında hukuka uygunluk ve yasallık ilkesinin gereklerini gizli e-posta izleme (2007 tarihli Compland v. UK kararı), gizli dinleme cihazları ile yapılan izlemelerde de sıkı bir şekilde aramaktadır (2009 tarihli Bykov v. Rusya kararı). İnternet izleme ile ilgili 2017 tarihli Barbulescu v. Romanya kararında başvurucunun işyerinde internet kullanımının takibini yarışan haklar arasında adil bir dengenin bulunmaması, başvuranın haberleşmesine müdahalenin sınırlarının belirsiz olduğu, keyfi müdahalenin önüne geçecek etkin ve yeterli önlem alınmadığı gerekçesi ihlal kararı verdiği görülmektedir. Mahkeme özel alanlarda kamera kullanımı gibi gelişen teknolojiler ışığında gerçekleşen karmaşık gizli izlemelerde, devletin pozitif sorumluluğu kapsamında yarışan hakların daha fazla gündeme geleceğine dikkat çekmektedir (2017 tarihli Antovic ve Mirkovic v. Karadağ kararı).

Mahkemenin, gizli yöntemle takibin (teknik takip/GPS) demokratik toplumun gereklerine uygunluk bakımında ayrıntılı incelemesi yaptığı Uzun v. Almanya kararı önem taşımaktadır. Olayda başvurucu ve arkadaşı S'nin, aşırı sol örgüt üyesi oldukları ve bombalı saldırılara karıştıkları gerekçesiyle kolluk tarafından hâkim kararı ile S'nin arabasına takip cihazı konarak GPS yoluyla takip edildiği anlaşılmaktadır. Yine kişilerin telefonlarının dinlemeye alındığı, ancak kişilerin takipten kurtulmak için vericiyi kırdıkları ve telefon ile iletişim kurmadıkları ifade edilmektedir. Mahkeme kararında öncelikle gizli takibin Alman mevzuatında öngörüldüğü ve başvurucu tarafından erişilebilir olduğu, sonrasında ise düzenlemenin keyfiliğe karşı yeterli ve etkin güvenceleri sağladığı tespitinde bulunmaktadır. Demokratik toplum gerekleri bakımından ise müdahalenin, ulusal güvenlik, kamu düzeninin korunması ve suç işlenmesinin önlenmesi meşru amacın yönelik olduğu ve güdülen meşru amaçla oranlı olduğunu ifade etmektedir. Yine GPS ile gizli takibin daha hafif yöntemler denendikten sonra uygulandığı, başvurucuya, arkadaşı işbirlikçi S'nin arabasında olduğu müddetçe sınırlı olarak uygulandığı, süresinin birkaç ayla sınırlı tutulduğunu vurgulamaktadır. Dolayısıyla başvurucunun genel ve ayrıntılı bir takibe maruz kaldığının söylenemeyeceği, bu halde bombalı saldırı gibi ağır suçlarda GPS ile yapılan takibin demokratik toplum için gerekli olduğu sonucuna vardığı, ihlal bulunmadığına karar verildiği görülmektedir. AİHM'in kamuya açık alanlarda GPS ile yapılan izlemelerde, özel hayata müdahaleyi daha sınırlı olarak gördüğü, telefon dinlemesi gibi gizli takibe ilişkin içtihatları ile getirdiği katı standartları uygulamadığı bu nedenle tedbiri hem yasal hem de gerekli bulunduğu anlaşılmaktadır (Harris, O'Boyle ve Warbrick, 2022;505).

AİHM'in terörle mücadelede idari kolluk tedbiri olarak gizli takibe ilişkin diğer önemli bir kararı ise Szabo ve Visy v. Macaristan kararıdır. Olayda başvurucuların, yürürlükte bulunan gizli takibe ilişkin yasal düzenlemenin, ulusal güvenlik gerekçesi haklarına ölçsüz müdahale ihtimali barındırması sebebiyle Mahkemeye başvurdukları görülmektedir. Karar günümüzde artan terör tehdidi sebebiyle idari kolluğa geniş çaplı gizli takip yetkisi verilmesine yönelik düzenleme ve uygulamalara Mahkemenin yaklaşımını göstermesi bakımından önem taşımaktadır. Kararda, Mahkemenin prensip olarak alınan terör eylemi istihbaratı nedeniyle devletlerce geniş çaplı takipte, iletişimin geniş çaplı takibinin de yer aldığı son teknolojik yöntemlere başvurulmasını günümüzde yaşanan terör eylemlerinin karmaşıklığı ve çeşitliliğinin doğal sonucu olduğunu kabul ettiği görülmektedir. Ancak Mahkeme başvuruda yapılan takibe ilişkin iç hukuk düzenlemelerinin yeterli ve etkin güvenceden yoksun olduğu tespitinde bulunmaktadır. Mahkeme, kullanılan son teknoloji ürünü cihazlar dikkate alındığında uygulanan tedbirin, hedef şahıslar dışında kalan ve nerdeyse Macaristan'da bulunan tüm kişilerden geniş çapta veri toplamaya imkân sağlayacak nitelikte olduğunu vurgulamaktadır. Mahkeme ayrıca böyle bir tedbiri uygulamaya karar verme yetkisinin tamamen yürütmenin elinde olduğu ve bu tür kararların iletişimin tespitine mutlak surette gereklilik değerlendirmesi yapılmaksızın alındığı, kararlara ilişkin adli bir yana idari dahi düzeltici denetim öngörülmediği dolayısıyla ihlal bulunduğuna karar verdiği görülmektedir. Karardan da anlaşıldığı üzere idari kolluk tarafından verilen önleyici iletişimin tespiti ve gizli takip uygulanması kararlarının makul süre içinde hâkim onayına sunulması,

tedbir kararları ve uygulamaları üzerinden bağımsız denetim mekanizmaları teşkili önem arz etmektedir. AIHM telefon dinlemede olduğu gibi teknik araçlarla gizli takip tedbirinde de yasallık ve hukuka uygunluk kriterini aramaktadır. Bir kararında kolluğun, şüphelileri takip etmek amacıyla hem nezarethaneye hem de evlerine dinleme cihazı koyularak yapılan takipte ihlal kararı verdiği anlaşılmaktadır. Mahkemenin ihlale, icra edilen şekliyle yapılacak takibin yasayla öngörülmediği gerekçesiyle karar verdiği görülmektedir (2001 tarihli PG ve JH v. UK kararı).

AIHM'in bir diğer kararı da kamuya açık alanlarda teknik araçlarla ses ve görüntü alınması imkânı veren güvenlik kameralarına ilişkindir. AIHM kararında kolluk tarafından gizlice görüntüsü alınan kişinin görüntüsünün kendisi ve avukatının bilgisi dışında kullanılması olayında ihlal kararı verdiği görülmektedir (2003 tarihli Perry v. UK kararı). Mahkemenin kararında, prensip olarak idari kolluğun suç işlenmesinin önlenmesi amacıyla kamuya açık alanlarda görüntü almasının 8. Maddeyi ihlal etmeyeceğini vurguladığı anlaşılmaktadır (2003 tarihli Peck v. UK kararı). Ancak önüne gelen başvuruda kolluğun kişinin hedef alınarak net görüntüsünün alınması amacıyla kameranın ayarlanması ve görüntünün alınmasını, teşhis amacıyla tanıklara gösterebilmek amacıyla montaj yoluyla videoya aktarılması ve tanıklara gösterilmesini kişisel verinin işlenmesi ve kullanılması olarak değerlendirmiştir. Dolayısıyla kolluğun görüntüyü iradi ve olağan şekilde almadığı, teşhis amaçlı kaydettiği ve kullandığı tespitinde bulunmaktadır. Bu nedenle müdahaleyi 8. Maddedin ihlali olarak görmektedir. Karar idari kolluğun MOBESE benzeri yönetmeler ile görüntü aldığı hallerde kişisel veri işleme ve kayıtlarla ilgili yol gösterici olması bakımından önem taşımaktadır.

Terörle mücadele amaçlı geniş çaplı gizli takibe ilişkin olarak Mahkemenin 2021 tarihli Big Brother Watch ve diğerleri v. Birleşik Krallık kararı önem taşımaktadır. Olayda başvurucuların elektronik ve diğer iletişim verilerinin, doğrudan ya da iletişim hizmet sağlayıcılarından veya ABD Ulusal Güvenlik Ajansı gibi yabancı istihbarat kurumlarından temin edilerek işlendiği, iletişimlerinin kitlesel olarak takip edildiği ve bu nedenle 8. Madde ile güvence altına alınan, özel hayata ve aile hayatına saygı hakkı ile haberleşme haklarının ihlal edildiği iddiasında bulunduğu anlaşılmaktadır. Olayda hükümetin yasal düzenleme ile istihbarat birimlerine terörle mücadele ve suç işlenmesinin önlenmesi amacıyla geniş çaplı gizli takip yetkisi verdiği görülmektedir. Mahkemeye göre devletlerin modern toplumda karşı karşıya kaldıkları terör gibi çok sayıda tehdit nedeniyle, kitlesel bir müdahale rejimi yürütmesi başlı başına Sözleşmeyi ihlal etmemektedir. Ancak, böyle bir rejimin karar verme ve uygulama dahil tüm süreçlerinin Sözleşme kapsamında değerlendirmeye tabi olması gerekmektedir. Yani geniş çaplı ulusal düzeyde alınacak önlemin demokratik toplum bakımından gerekliliği ve orantılılığının sürecin her aşamasında göz önünde bulundurulması gerektiği gibi operasyonun amacı ve kapsamı tanımlanırken başlangıçta bağımsız yetkilendirmeye tabi olması, alınan önlemler geriye yönelik yargısal incelemeye tabi olması ve herhalde bağımsız idari denetime tabi olması gerekmektedir. Dolayısıyla Mahkemenin, karara konu başvuruda istihbarat birimlerine kitlesel iletişim takibi imkânı veren 2000 tarihli Soruşturma Yetkileri Yasasını yukarıdaki açıklamalar ışığında 8. Madde kapsamında incelediği görülmektedir. Bu bağlamda Mahkemenin, anılan kanunla istihbarat birimlerine verilen kitlesel iletişim takibi yetkisi ile ilgili yaptığı incelemede; kitlesel iletişim takibine yönelik bağımsız bir yetkinin bulunmamasını, hedef arama terimi kategorilerinin izin başvurusunda yer alamamasını, bir kişiyle bağlantılı arama terimlerinin (yani, bir e-posta adresi gibi belirli tanımlayıcıların) önceden dahili izne tabi olduğunun belirginleştirilmiş olmamasını sorunlu bulduğu görülmektedir. Yani istihbarat birimlerine verilen yetkinin sınırları noktasında belirsizlik, keyfi müdahaleye yol açma riski bulunmasını yasallık ve gereklilik bağlamında Sözleşmeye aykırı bulmaktadır. Bunun yanında Mahkemenin kullanılan bu yetkilerle ilgili sağlanan yargısal denetimi ve bağımsız denetim mekanizmasını yeterli bulduğu anlaşılmaktadır. Ancak sağlanan bu denetimlerinde kitlesel müdahale rejimindeki eksikleri gidermeye yetmediği tespitinde bulunmaktadır. Dolayısıyla anılan eksiklikler nedeniyle iletişimin geniş çaplı takip rejimi ile yapılan müdahalenin, demokratik toplum gereklerini karşılama bakımından yetersiz kaldığı ve Sözleşmenin 8. Maddesinin ihlal edildiğine karar verdiği görülmektedir.

Diğer yandan Mahkemenin, yabancı istihbarat teşkilatlarından dinleme verileri alma ve işleme yetkisine ilişkin olarak hem alma hem de işleme ve korunmasına yönelik keyfi müdahalelerin önüne geçilmesi dahil etkin ve yeterli güvencelerin bulunduğu kanaatine vardığı görülmektedir. Mahkeme ayrıca bu yetkinin kullanımına yönelik de etkin bir denetim mekanizmasının varlığına ve geriye yönelik olarak yargısal denetim imkanının da bulunduğu vurgu yapmaktadır. Dolayısıyla yabancı istihbarat birimlerinden kitlesel iletişim

verisi alınması ve işlenmesini Sözleşmenin 8. Maddesine uygun bulunduğu anlaşılmaktadır. İletişim hizmet sağlayıcılarından iletişim verileri alınması ve işlenmesine ilişkin olarak ise kanun ile verilen bu yetkinin yine yabancı istihbarat birimlerinden alınmada olduğu gibi aynı gerekçeler ile keyfi kullanımın önlenmesine yönelik etkin ve yeterli güvencelerin varlığı sebebiyle hukuka uygunluk ve yasallık ilkesine uygun bulunduğu görülmektedir. Dolayısıyla iletişim sağlayıcılarından iletişim verisi alınması ve işlenmesini Sözleşmenin 8. Maddesine uygun bulunduğu anlaşılmaktadır.

Bunun yanında başvuruda Mahkemenin kitlesel iletişim takibi rejimi ile 10. Maddede belirtilen ifade özgürlüğü bağlamında bir gazetecinin kaynaklarını koruması hakkına yönelik müdahale ettiği yönünden de incelediği anlaşılmaktadır. Olayda yetkinin kullanımında gazetecilik faaliyeti ile ilgili olduğu bir arama teriminin kasıtlı olarak kullanılması durumunda oraya çıkan gazetecilik faaliyeti ile ilgili iletişimin yargısal ve bağımsız denetim mekanizması ile denetime tabi olmaksızın analist tarafından incelemeye devam etme imkânı verdiği ve bu durumun keyfi kullanımına yol açtığı iddia olunmaktadır. Mahkemeye göre bir gazetecinin kaynaklarının korunması basın özgürlüğünün temel taşıdır. Bu korunmasını zayıflatılmasının ise kamu hizmeti olan toplumun doğru ve güvenilir bilgi alma özgürlüğüne zarar vereceğinin şüphe bulunmamaktadır. Dolayısıyla basın özgürlüğüne yeterli ve etkin güvence sağlamayan kitlesel iletişim takip rejimi 10. Maddeyi ihlal etmektedir.

ABD ve Birleşik Krallıkta geniş çaplı gizli takibe ilişkin olarak Mahkeme önünde halen Bureau of Invasive Journalism v. Birleşik Krallık ve 10 İnsan Hakları Örgütü v. Birleşik Krallık başvuruları derdest durumdadır. Terörle mücadele amaçlı geniş çaplı gizli takipte nelerin demokratik toplum bakımından gerekli olduğu noktasında açıklanacak kararların da Big Brother kararında olduğu gibi yol gösterici olacağı beklenmektedir (Harris, O'Boyle ve Warbrick, 2022;505).

3.4. AİHM Kararlarında Terörle Mücadele Amaçlı Kişisel Veri Toplama ve İşleme ile Özel Hayata ve Aile Hayatına Saygı Hakkı İlişkisi

Terörle mücadelede AİHM 8. Maddesi bağlamında önem arz eden bir diğer hususta terörle mücadele amaçlı kişisel verilerin toplanması, kullanılması ve korunmasına yönelik uygulamalardır. Bu uygulamalar kolluk tarafından gerçekleştirilen geçmişte suç işlemiş sabıkalılara ait kişisel verilerinin işlenmesi ile istihbarat amaçlı kişisel veri toplama ve işleme (kamera ile görüntü alma ve kaydı, GPS verisi alma, parmak izi alma, fotoğraf alma, DNA ve hücre örneği alma) olarak görülmektedir (2012 tarihli Van der Velden v. Hollanda kararı). Kişisel verilerin korunması hakkı ile özel hayatın gizliliğinin korunması hakkı birlikte incelenen, iç içe geçmiş hem ulusal hem de uluslararası hukukta korunan demokratik toplumun vazgeçilmez haklarındadır (Küzeci, 2010;71). AYM'de bir kararında kişisel verilerin korunması hakkını özel hayatın korunması hakkı içinde değerlendirmekte, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak tanımlamaktadır (2021, E.2020/24, K.2021/39). Ayrıca AYM'nin bir diğer kararına göre genel bir çerçeve hak olması sebebiyle sadece kişisel veri işlemeye karşı korunma değil kişisel verilere yönelik her türlü müdahale ve sınırlamaya karşı güvence temin etmektedir (2015, E.2014/180, K.2015/30).

Kişiler hakkında devletler tarafından bilgi toplanması, işlenmesi ve açıklanması kişinin özel hayatına müdahale oluşturduğunda şüphe bulunmamaktadır (Harris, O'Boyle ve Warbrick, 2022;508). Hatta AİHM, kolluğun açık kaynaklardan (internet, medya vb.) kişiler hakkında topladığı bilgileri sistematize ederek saklamasının da özel hayata müdahale oluşturabileceğini ifade etmektedir (2012 tarihli MM v. UK kararı). Bununla birlikte AİHM kamuya açık alanlardan kolluk tarafından görüntü alınmasının tek başına özel hayat müdahale anlamına gelmeyeceğini, görüntülerin kaydedilmesi ve kullanılması halinde müdahale oluşturabileceğini vurgulamaktadır (2013 tarihli Khmel v. Rusya kararı). AİHM prensip olarak yeni teknolojik cihazların kişisel veri toplama ve işleme amaçlı kullanımında özenli olunması gerekliliğini ifade etse de terörle mücadele amacıyla kişisel bilgilerin toplanması ve işlenmesini Sözleşmeye aykırılık olarak görmemektedir (2004 tarihli Von Hannover v. Almanya kararı). Ancak bu amaçla yapılacak faaliyetlerin tamamının demokratik kurumları korumak için mutlak gereklilik hallerinde mümkün olabileceğini vurgulamaktadır (Kilkelly, 2001;82).

AİHM ulusal güvenlik gerekçesiyle devletlerin, idari kolluğa ve istihbarat birimlerine kamunun ulaşmadığı kayıtlara ulaşma ve bilgi toplama yetkisi veren kanunlara ihtiyaç duyduğunu kabul etmektedir (1987 tarihli Leander v. İsveç kararı). Bu bilgilerin ulusal güvenlik amacıyla özel görevlere alınacak kişilerin değerlendirilmesinde kullanılmasını kabul edilir bulmaktadır. Ancak Mahkeme, bu uygulamalara ilişkin

düzenlemelerin ayrıntılı olarak yapılmasının, istisnai ve özel koşullarının belirlenmesinin, keyfi uygulamaların önüne geçecek yeterli ve etkin teminatlarla (usulü güvencelere) bağlanmasının gerekliliğine vurgu yapmaktadır (Kilkelly, 2001;62). Mahkemenin Rotaru v. Romanya kararında, başvurusunun Romanya'da komünist rejim tarafından hakkında tutulmuş olan kayıtlarının silinmesini talep ettiği, ancak Romanya İstihbarat Servisinin bu talebi reddettiği görülmektedir. Mahkeme Rotoru v. Romanya kararında ulusal kanunların kişisel bilgi toplama ve işlemeye yönelik sınırlama getirmediği tespitinde bulunmaktadır. Ayrıca düzenleme ile her ne kadar idari kolluğa önleme amaçlı müdahale imkânı verilmiş olsa da müdahale koşul ve gerekçelerinin yeterli açıklıkta düzenlenmediğini vurgulamaktadır. Dolayısıyla hukuken öngörülebilir olmayan düzenleme ile yapılan müdahalenin 8. Maddeyi ihlal ettiğine karar verdiği görülmektedir (2011 tarihli Dmitrov-Kazakov v. Bulgaristan kararı).

Mahkemenin terörle mücadele amaçlı kişisel veri işleme ile ilgili bir diğer kararı ise Mcveigh, O'Neil ve Evans v. Birleşik Krallık Kararıdır. Olayda başvuru sahiplerinin terörle mücadele mevzuatı kapsamında arandığı, sorgulandığı, parmak izleri ve fotoğraflarının alındığı görülmektedir. Başvuru sahipleri alınan kişisel verilerin saklanması özel hayatlarına müdahale oluşturduğunu iddia etmektedir. Ancak Mahkemenin, terörle mücadele konusunda toplumsal ihtiyacın yapılan müdahaleye göre daha önemli olduğu ve istihbarat maksatlı alınan bilgilerin gerekli olduğu ve bu nedenle uygulanan tedbirin ihlal oluşturmadığı yönünde karar verdiği görülmektedir (Kilkelly, 2001;61). Mahkemenin Murray v. Birleşik Krallık kararında ise başvuru sahiplerinin askeri karakolda kişisel bilgilerinin kaydedilmesini ve rıza dışında fotoğraflarının alınmasını iç hukukta yasal dayanağının bulunması ve hukukun öngördüğü tedbirler olması sebebiyle Sözleşmeye uygun bulunduğu anlaşılmaktadır. Kararda, terörle mücadele amaçlı kişisel veri toplanması ve işlenmesi noktasında devletlerin vatandaşlarını terör eylemlerinden koruma sorumluluğu bulunduğunu vurgulanmakta, devletlerin takdir hakkına atıf yaparak toplumsal ihtiyaçla kişilerin hakları arasında adil bir dengenin kurulması zorunluluğuna dikkat çekilmektedir. Dolayısıyla yapılan müdahalenin izlenen meşru amaçla oranlı olduğuna karar verildiği görülmektedir.

Mahkemenin Leander v. İsveç kararında ise güvenlik soruşturması sebebiyle tutulan kolluk kayıtlarının özel hayata müdahalesini tartıştığı görülmektedir. Olayda, askeri bir tesiste geçici olarak çalışmakta olan başvuru sahibi, kolluk sicilinde yer alan kayıtlar sebebiyle geçici işine son verildiğini ve daimî kadroya alınmadığını, kolluk sicilinde yer alan kayıtların saklanması ve kendisine aksini ispat hakkı verilmemesinin özel hayatına müdahale oluşturduğunu iddia etmektedir. Mahkemenin ise belirtilen tedbiri özel hayat müdahale olarak gördüğü, ancak hassas kadrolarda çalıştırılacak personel kontrol sisteminde, kişilerin haklarının sınırlandırılmasının keyfi müdahaleye karşı alınmış yeterli ve tekin korumanın varlığı halinde demokratik toplum için gerekli olduğuna karar verdiği anlaşılmaktadır (Kilkelly, 2001;62-64).

AIHM'in idari kolluğun kişisel veri işleme ile ilgili bir diğer kararı da Segersted-Wiberg ve diğerleri v. İsveç kararıdır. Bu kararda Mahkemenin, kolluk tarafından bir başvuru sahibiye yönelik bombalı saldırı bilgisinin saklanması ve başvuru sahibine verilmemesinin suç işlenmesinin önlenmesi amacıyla yönelik olduğu gerekçesi ile ihlal bulunmadığına karar verdiği görülmektedir. Olayda diğer başvuru sahipleri ile ilgili olarak da idari kolluğun, başvuru sahiplerinin üye olduğu siyasi parti bilgileri ile katıldıkları mitingler gibi siyasi faaliyetlerine ilişkin kişisel verilerin toplandığı ve işlendiği anlaşılmaktadır. Mahkemenin, bu başvuru sahipleri ile ilgili ise hükümetin, ulusal güvenlik nedeniyle kişisel verilerinin işlendiği savunmasını, tehdidin yeterince ortaya konulmadığı gerekçesi ile yetersiz bulunduğu ve meşru amaca yönelik olmayan müdahale sayarak ihlale karar verdiği görülmektedir (2006 tarihli Segersted-Wiberg ve diğerleri v. İsveç kararı).

Mahkemenin diğer bir kişisel veri kararı ise işlenmiş suçlara ilişkin yapılan soruşturma ve kovuşturma sebebiyle kolluk tarafından işlenen parmak izi, DNA ve hücre örneklerinin saklanmasına ilişkindir. Olayda başvuru sahiplerinin hırsızlık ve tacizden suçlandığı, ancak birincisinin yargılama sonucu beraat ettiği, diğeri hakkındaki kamu davasının ise uzlaşma sebebi ile düşüldüğü anlaşılmaktadır. Sonrasında başvuru sahiplerinin alınan kişisel verilerinin kolluk kayıtlarından silinmesini talep ettikleri görülmektedir. AIHM önüne gelen bu başvuruda, kişisel veri işleme yasaya dayansa dahi beraat ve uzlaşma ile sona eren başvuruda kamu yararı amacı ile özel menfaat arasındaki dengenin bozulduğu ve devlete tanınmış olan takdir hakkının sınırlarının aşıldığı tespitinde bulunmaktadır. Bu nedenle Mahkemenin alınan tedbirin demokratik toplum gerekleri bakımından zorunlu olmadığı ve başvuru sahiplerinin özel hayatına orantısız müdahale teşkil ettiği gerekçesiyle ihlal kararı verdiği görülmektedir (Songül, 2010;118). Mahkeme kararında, hukuka uygunluğun ve yasallığın, müdahalenin sınırlarının belirlenmesi ve keyfi müdahaleyi önleyecek etkin ve yeri güvenceler sağlaması

yanında, verilerin saklanma süresi, depolama, kullanılma, paylaşılma, korunma ve imhasına ilişkin usullerinde belirli olmasını gerektirdiğine vurgu yapmaktadır (2012 tarihli MM v. UK kararı).

Mahkemenin bu kararları, kolluğun hem suç işlenmesinin önlenmesi hem de işlenen suç veya önleyici faaliyetler kapsamında rızaya dayanmayan parmak izi ve fotoğraf alma gibi kişisel veri toplama ve işlemeye ilişkin esasları göstermesi bakımından önem taşımaktadır. İdari kolluğun özellikle terörle mücadele amaçlı olarak kişilerin konusu suç teşkil etmeyen siyasi faaliyetlerini kaydetmesini ve istihbarat amaçlı kullanılmasını demokratik toplum gerekleri bakımından zorunlu olduğunu ortaya koyması gerekmektedir. Ayrıca veri işlemede keyfi müdahalelere yönelik etkin ve yeterli güvencelerin tesis edilmiş olduğunun da (süre, imha usulü ve erişimde usuller) gösterilmesine ihtiyaç bulunmaktadır.

4. Sonuç

11 Eylül saldırılarının doğurduğu ortam ve devamında teknolojik ve siyasi değişimlere bağlı olarak tehdit ve risklerin artmasına bağlı olarak son yıllarda terörle mücadele amacıyla kolluğun gizli takip, kişisel veri toplama ve işleme gibi yetkilerinin geniş çaplı olarak artırıldığı görülmektedir. Bu uygulamalara hem Anglo Sakson hem de ağırlıklı olarak Fransa hukukunda olduğu gibi Kara Avrupası hukukunda rastlanmaktadır. Hatta AB tarafından kişisel veriler PNR yoluyla tüm Shengen bölgesine girenler bakımından toplanmakta ve işlenmektedir. Tüm bu yetkilerin kullanımındaki temel sorunu; verilen yetkilerin keyfi kullanımının önüne geçecek etkin ve yeterli güvencelerin varlığı konusundaki tartışmalardır. İdari kolluk veya istihbarat birimleri tarafından bu yetkiler genişletilmeye çalışılmakta ve belirli ırk, dinsel geçmişe sahip insanlara yönelik kötüye kullanımın vasıtası haline getirilebilmektedir.

AİHM prensip olarak devletlerin, vatandaşlarını terör gibi ağır tehditlerden korumak amacıyla geniş çaplı takip (iletişim, bankacılık faaliyetleri ve görüntü dahil), önleyici durdurma, sorgulama ve arama gibi önleyici önlemlerin alınmasını AİHS'ye aykırı bulmamaktadır. Ancak bu yetkilerin kullanımında etkin ve yeterli güvencelerin varlığını, devletin takdir hakkının sınırlarını belirlenmiş olmasını, keyfi kullanımın önüne geçecek önlemlerin alınmış olmasını, demokratik topluma gerekli ve zorunlu olanı aşmamasını ve orantılı olmasını aramaktadır.

Türkiye'de özel hayatın gizliliği, konut dokunulmazlığı ve haberleşme özgürlüğü konuların anayasal güvence altına alındığı ve yasal düzenlemelerde AİHS 8. Maddesinin temel alındığı görülmektedir. Özel hayatın gizliliği, konut dokunulmazlığı ve haberleşme özgürlüğü ile ilgili yapılan yasal düzenlemeler terörle mücadelede idari kolluğun iletişim tespiti ve kaydı dahil teknik ve fiziki takip, kişisel veri toplama ve işleme gibi önleyici kolluk faaliyetleri bakımından önem taşımaktadır. Düzenlemeler kapsamında kişisel verinin ancak belirli, açık ve meşru amaçlar için işlenebileceğinin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekliliğinin hüküm altına alındığı görülmektedir.

AİHM'in idari kolluğun özellikle terörle mücadele amaçlı kişisel veri işlemeye ilişkin konularda aldığı kararlar incelendiğinde; başvuruya konu kişisel verilerin istihbarat amaçlı kullanılmasının gerekçelendirilmesi ve demokratik toplum gerekleri bakımından zorunlu olduğunun ortaya konulması şartlarının arandığı görülmektedir. Ayrıca veri işlemede keyfi müdahalelere yönelik etkin ve yeterli güvencelerin tesis edilmiş olduğunun da (yasallık, yargısal denetim, işleme süresi, imha usulü ve erişimde usuller) gösterilmesi gerekliliğine vurgu yapılmaktadır. Bu anlamda, Türkiye'deki düzenlemenin AİHM içtihatları ile uyumlu olduğu çıkarımı yapılabilmektedir.

Siyasi ve idari kolluk iç güvenlik istihbaratını elde etmek ve terör eylemlerinin önlemek amacıyla geniş çaplı takip (internet haberleşmesi takibi, görüntü alma, ortam dinlemesi vb.) ve telekomünikasyon yoluyla gerçekleştirilen iletişimin tespiti, dinleme, sinyal bilgilerini değerlendirme ve kaydı almaya yetkilidir. Polis jandarmaya ilave olarak internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edebilmekte, dinleyebilmekte, sinyal bilgileri değerlendirilebilmekte ve kayda alabilmektedir. Polis yine jandarmadan farklı olarak, ülke çapında genel istihbarat toplama yetkisi ile bu yetkisi kapsamında da önleme amaçlı teknik araçlara izleme yetkisine sahiptir.

Bu yetkilerde de teknik takip hariç ancak hâkim kararı ile ya da 24 saat içinde hâkim kararına sunulması koşuluyla kanunda gösterilen idari/siyasi kolluk mercilerinin emriyle kullanılabilir. Teknik araçla izleme için gecikmesinde sakınca bulunan hal öngörülmemiş olup yetkinin kullanımı için hâkim kararı gerekmektedir. Düzenlemelerde iletişimin takibine ilişkin esasların düzenlendiği, yazılı emir veya kararda

hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları, ilgili internet bağlantı adresi veya bağlantıyı tespitte imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenlerinin yer alacağı, elde edilen kişisel verilerin saklama süresinin ve imha usullerinin gösterileceğinin hüküm altına alındığı anlaşılmaktadır. Yine her iki tedbirinde ancak sayılarak tüketilen terör suçları dahil ağır suçlar için öngörüldüğü görülmektedir. Yine her iki tedbir içinde makul şüphenin varlığı aranmaktadır. Dolayısıyla istihbarat amaçlı geniş çaplı takip ve telekomünikasyon yolu iletişimin takibinde AİHM içtihatlarında aranan etkin ve yeterli usulü güvencelerin sağlandığı görülmektedir (Aras, 2009).

Görüldüğü gibi hem Anayasal düzenlemeler hem de idari kolluğun kanunlarında yer alan genel istihbarat yetkisi içinde geniş çaplı takip, telekomünikasyon yolu yapılan iletişimin takibi ve teknik takip faaliyetleri AHİS 8. Madde ve AİHM içtihatları ile genel olarak uyumdur. Ancak spesifik olarak MOBESE benzeri kent güvenlik sistemleri ile kamuya açık alanlarda ses ve görüntü olarak takibi sürekli olarak yapılmaktadır. Mevcut düzenlemelerde bu durum ilişkin açıklık bulunmamaktadır. Süresiz takip her ne kadar AİHM içtihatlarında sorunlu bulunsun da AİHM, devletlerin toplumu terör gibi ağır tehlikelerden koruma sorumluluğuna yaptığı atıfla bu konuda devletlerin geniş bir takdir hakkının bulunduğunu kabul etmektedir. Prensip olarak idari kolluğun suç işlenmesinin önlenmesi amacıyla kamuya açık alanlarda görüntü almasının 8. Maddeyi ihlal etmeyeceğini vurgulamaktadır. Dolayısıyla MOBESE benzeri tedbirler AİHM tarafından sözleşmeye aykırılık olarak görülmesi de tedbirler alınan verilerin işlenmesi de söz konusu olduğundan, tedbirin usulü güvencelere kavuşturulması için kapsamının kanunla düzenlenmesi gerekmektedir.

Yine AİHM terörle mücadelenin zorluğundan hareketle, terörle mücadele amacıyla 8. Madde bağlamında yapılan müdahalelerde tek başına makul şüphenin yokluğunu ihlal saymamakta, önüne gelen başvuruda tedbirde keyfiliğin bulunup bulunmadığı hususu ve demokratik toplum gerekleri bakımından gereklilik koşulu ile birlikte değerlendirmektedir. Bu nedenle, keyfiliklerin önüne geçilmesi için var olan hem idari hem yargısal denetimin iyi işletilmesi şartıyla, terörle mücadele amaçlı önleyici tedbirler bağlamında makul şüphenin geniş yorumlanmasının faydalı olacağı değerlendirilmektedir.

Bununla birlikte yasal düzenlemelerde teknik araçlar ile izlemeye ilişkin süre belirlenmediği gibi uygulanan tedbirin sona ermesi halinde elde edilen verilerin yok edilip edilmeyeceğinin de düzenlenmediği görülmektedir. Teknik takip tedbirine ilişkin süre sınırlamasının bulunmaması ve işlenen verilerin akıbetine göre saklama ve imha usullerinin öngörülmemesi, AİHM içtihatları bağlamında etkin ve yeterli usulü güvencelerin yokluğu anlamında gelmektedir. Her iki hususa ilişkin düzenleme yapılmasında fayda bulunmaktadır.

Kaynaklar

- Acar, Ü. (2011). *İstihbarat*. Ankara: Akçağ Yayınları.
- Ahmetoğlu, A. B. (2023). Eylem Planı ile Özel Hayata ve Aile Hayatına İlişkin Güvenceler Artıyor. *İnsan Hakları Dergisi*, 7, 41-47.
- Aras, B. (2009). Türk Hukukunda İletişimin Denetlenmesi Tedbirinde Yargısal Denetim. *Terazi Dergisi*, 4(30), 31-39.
- Avcı, G. (2004). *İstihbarat Teknikleri*, (Üçüncü Baskı). İstanbul: Timaş Yayınları.
- Bayındır, Z. (2016). *Özel Yaşamın Korunması Çerçevesinde İstihbarat Faaliyetleri*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.
- Beren, F. (2010). *İç Güvenlik İstihbaratında Saydamlık-Etkililik İlişkisi*. Doktora Tezi, Ankara: Polis Akademisi Yayınları.
- Birtek, F. (2011). İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği. *CHD*, 6(16), 100-148.
- Boga, B. (2022). *Türk Ceza Kanunu'nda Özel Hayatın Gizliliğini İhlal Suçu ile Kişisel Verileri Koruyan Suçlar Arasındaki İlişkiye Dair Bir Değerlendirme*. 2022 Uluslararası Necmettin Erbakan Hukuk Kongresi Tam Metin Bildiri Kitabı, 81-110.
- Can, N. (2020). *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı.
- Centel, N. & Zafer, H. (2018). *Ceza Muhakemesi Hukuku* (15. Baskı). İstanbul: Beta Yayınları.
- Centel, N. (2011). 5271 Sayılı Ceza Muhakemesi Kanunu'na Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi. *GSÜHFD*, 9(1), 161-192.

- Cin, E. (2008). *Türk Hukukunda Kolluk Yetkisinin Kullanılması ve Sınırları*. Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü.
- Çelik, A. (2015). Özgürlük ve Güvenlik Bağlamında İç Güvenlik Paketinde Yer Alan Bazı Maddelerinin Değerlendirilmesi. *Uyuşmazlık Mahkemesi Dergisi*, 0(5), 235-263.
- Delice, M. & Dağlar, M. (2011). *Alternative Tactics for Combating Terrorism: Citizens Police Academies*, IPES working paper series.
- Dost, S. (2018). Uluslararası Hukukta Orantılılık İlkesi, *Uyuşmazlık Mahkemesi Dergisi*, 0(12), 361-399.
- Erdoğan, M. (2013). Anayasal-Demokratik Bir Rejimde Özgürlük ve Güvenlik. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 12(24), 21-29.
- Ergil, D. (1992). Uluslararası Terörizm. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 47(3), 139-143.
- Galli, F. (2016). The Interception of Communication in France and Italy – What Relevance for The Development of English Law? *The International Journal of Human Rights*, 20(5), 666-683.
- Girgin, K. (2003). *Uluslararası İlişkiler Modern İstihbarat ve Türkiye*. İstanbul: Okumuş Adam Yayınları.
- Gözler, K. (2011). *Anayasa Hukukuna Giriş*. (On yedinci Baskı). Bursa: Ekin Yayınevi.
- Gözübüyük, A. Ş & Gölcüklü, F. (2016). *Avrupa İnsan Hakları Sözleşmesi ve Uygulaması*, (11. Bası). Ankara: Turhan Kitabevi.
- Gözübüyük, Ş. & Gölcüklü, F. (2011). *Avrupa İnsan Hakları Sözleşmesi ve Uygulaması*, (9. Basım). Ankara: Turhan Kitabevi.
- Güler, M. (2023). *MİT Yasasında Değişiklik ve İstihbaratın Denetimi*. <https://21ypte.org/tr/merkezler/islevsel-arastirma-merkezleri/milli-guvenlik-ve-dis-politika-arastirmalari-merkezi/mit-yasasinda-degisiklik-ve-istihbaratin-denetimi>, (Erişim Tarihi: 28.10.2023).
- Günday, M. (2011). *İdare Hukuku*, (Onuncu Baskı). Ankara: İmaj Yayınevi.
- Güney, A. (2006). *Türkiye’de Özel Güvenlik Teşkilatlarının Yetkilerinin Analizi*. Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü.
- Harris, David., O’Boyle, Michael. & Warbrick, Colin. (2022). *Avrupa İnsan Hakları Sözleşmesi*. İstanbul: Onikilevha Yayıncılık.
- Kaşlı, E. (2022). Kolluk Uygulamalarında Drone Kullanımı. *Karadeniz Sosyal Bilimler Dergisi*, 14(26), 329-340.
- Kaşlı, E. (2023). Kolluk Faaliyetlerinde Kişisel Verilerin Korunması: Avrupa Birliği 2016/794 Sayılı Europol Tüzüğü ve 2016/680 Sayılı Kolluk-Ceza Adaleti Direktifi Işığında Bir İnceleme. *Ankara Avrupa Çalışmaları Dergisi*, 22, 97-115.
- Kızılırmak, B. (2018). *Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği*. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.
- Kilkelly, U. (2001). *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı: AIHS’nin 8. Maddesinin Uygulanmasına İlişkin Klavuz*. İnsan Hakları El Kitapları, No:1. Strasbourg, Cedex: Avrupa Konseyi Yayınları.
- Köksal, T. D. (2021). Bilgi Toplamaya Yönelik İstihbari Kolluk Faaliyetine İnsan Hakları Perspektifinden Bakış. *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, 2, 1745-1798.
- Kuçuradi, İ. (2018). Etik İlkeler ve Hukukun Temel Öncülleri Olarak İnsan Hakları. İonna Kuçuradi, *İnsan Hakları: Kavramları ve Sorunları*, içinde, ss. 55-68 (4. Baskı), Ankara: Türkiye Felsefe Kurumu.
- Kuloğlu, G. (2015). *İç Güvenlik İstihbaratı ve Kolluk*. İstanbul: Beta Yayınevi.
- Küzeci, E. (2010). *Kişisel Verilerin Korunması Hakkı*. Ankara: Turhan Kitabevi.
- Metin, Y. (2017). Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir? *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 7(1), 1-74.
- Öncü, G. A. (2011). *Özel Yaşamın Korunması Hakkı*. İstanbul: Beta Yayıncılık.
- Özbek, V. Ö. (2001). Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi. *İÜHFİM*, 59(1-2), 181-202.
- Özbek, V. Ö., Doğan, K. & Bacaksız, P. (2023). *Ceza Muhakemesi Hukuku* (16. Baskı). Ankara: Seçkin Yayınları.
- Özbudun, E. (1977). Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 1, 1925-1975.
- Özdağ, Ü. (2008). *İstihbarat Teorisi*. Ankara: Kripto Yayınevi
- Özdağ, Ü. (2009). Devlet ve İstihbarat. *Stratejik Araştırmalar Dergisi*, 1(3), 33-50.
- Özdek, Y. (2004). *Avrupa insan hakları hukuku ve Türkiye: AIHS sistemi, AIHM kararlarında Türkiye*. Türkiye ve Orta Doğu Amme İdaresi Enstitüsü İnsan Hakları Araştırma ve Derleme Merkezi.

- AIHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması*
Öztürk, B., Kazancı, B. E. & Güleç, S. S. (2021). *Ceza Muhakemesi Hukuku Koruma Tedbirler* (4. Baskı). Ankara: Seçkin Yayınları.
- Pınarbaşı, M. (2014). *Özel Hayatın Korunması Kapsamında İstihbarat Faaliyetlerinin Hukuksal Sınırları*. Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı.
- Semiz, H. (2007). Uluslararası Terör Suçları Bakımından Terör Suçlarında Kolluk Yetkileri. Yüksek Lisans Tezi, Harp Akademisi Komutanlığı Stratejik Araştırmalar Enstitüsü.
- Shue, H. (1996). Temel Hakların Evrenselliği. *İnsan Haklarının Felsefi Temelleri Uluslararası Semineri*, Yayıma Hazırlayan İoanna Kuçuradi, (2. Baskı) Türkiye Felsefe Kurumu Yayınları.
- Şen, E. (1996). *Özel Hayatın Gizliliği ve Korunması*. İstanbul: Kazancı Yayınları.
- Şen, E. (2011). *Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, Muhbir (Telefon Dinleme)*, (5. Baskı). Ankara: Seçkin Yayınları.
- Ünver, Y. & Hakeri, H. (2021). *Ceza Muhakemesi Hukuku* (16. Baskı). Ankara: Seçkin Yayınları.
- Yenisey, F. (2012). *Kolluğun Suç Öncesi Faaliyetleri Çerçevesinde İstihbarat ve Güvenlik Hukuku*. Ankara: Jandarma Okullar Komutanlığı Matbaası.
- Yenisey, F. (2015). *Kolluk Hukuku*, (2. Baskı). İstanbul: Beta Yayıncılık.
- Yılmaz, S. (2007). *21. Yüzyılda Güvenlik ve İstihbarat*. İstanbul: Milenyum Yayınları.
- Yüksel, S. (2012). Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale. İstanbul: Beta Yayıncılık.

Etik, Beyan ve Açıklamalar

1. Etik Kurul izni ile ilgili;

Bu çalışmanın yazar/yazarları, Etik Kurul İznine gerek olmadığını beyan etmektedir.

2. Bu çalışmanın yazar/yazarları, araştırma ve yayın etiği ilkelerine uydıklarını kabul etmektedir.

3. Bu çalışmanın yazar/yazarları kullanmış oldukları resim, şekil, fotoğraf ve benzeri belgelerin kullanımında tüm sorumlulukları kabul etmektedir.

4. Bu çalışmanın benzerlik raporu bulunmaktadır.
