İLETİŞİMİN KİTLESEL GÖZETİMİNDE USULİ GÜVENCELERİN SAĞLANMASI: AİHM'NİN İKİ KARARI ÇERÇEVESİNDE DEĞERLENDİRME[*]

Araştırma Makalesi

Deniz KIZILSÜMER ÖZER[**]

ÖZET

25 Mayıs 2021 tarihinde, AİHM Büyük Dairesi, In Centrum för Rattvisa v. İsveç ve Big Brother Watch ve Diğerleri v. İngiltere davasında, Birleşik Krallık ve İsveç hükümetlerinin, kitle iletişiminin gözetimi (KİG) hakkındaki ulusal mevzuatlarının gizliliğin korunması için yeterli usul güvenceleri içermemesi nedeniyle AİHS Madde 8'i ihlal ettiğine hükmetti. Mahkemenin bu kararlardaki yaklaşımı özellikler gösterdiği için çeşitli yönlerden incelenmelidir. Öncelikle, Mahkeme, KİG'nin özelliğini göz önünde bulundurarak, mağduriyeti kanıtlamanın neredeyse imkansız olması nedeniyle mağduriyet gerekliliğini ortadan kaldırarak, davalının iç başvuru yollarını tüketmesini aramadan davayı soyut olarak karara bağladı. İkinci olarak, Mahkeme, KİG ile ilgili mevzuatın "kanunun kalitesi" koşulunu karşılayıp karşılamadığını değerlendirdi. Mahkeme, hedefli gözetim konusundaki önceki davalarında bazı usulî güvenceleri

[*] Bu makale Yaşar Üniversitesi tarafından gerçekleştirilen 140 Nolu "Türk Kamu Yönetiminde idari Makamların İdari Faaliyetlerinde Yapay Zekayla İlgili Uyması Gereken İlkelere Dair Çerçeve Metin Oluşturulması" başlıklı BAP projesi tarafından desteklenmiştir.

[**] **Prof. Dr.,** Yaşar Üniversitesi Hukuk Fakültesi, Milletlerarası Hukuk ABD,
ORCID ID: 0000-0001-7512-7928, **e-posta:** deniz.ozer@yasar.edu.tr,
DOI: 10.69958/ihy.1573602

Makalenin Geliş Tarihi: 25.10.2024
Makalenin Kabul Tarihi: 11.11.2024

belirlemiş olsa da, bu kararlarında özel hayatın gizliliğinin korunması için KİG ile ilgili mevzuatın içermesi gereken minimum güvenceleri belirledi. Mahkeme, "toplu gözetim rejiminin per se Sözleşmeyi ihlal etmediğine" karar verdi; ancak Mahkemeye göre KİG ile ilgili mevzuat özel hayatın korunmasını sağlamak üzere "baştan sona güvenceler" sağlamalıdır. Özetle, gizli gözetimi düzenleyen kanunların Mahkemenin önüne gelmesi halinde yapılan denetim sırasında müdahalenin hukuka uygunluğu "kanuna uygunluk" ve "gereklilik" koşullarının birlikte değerlendirilmesi suretiyle yapılmaktadır. Burada, "kanunun kalitesi" koşulu, ilgili kanunların hem "erişilebilir ve öngörülebilir" olmasını hem de gizli gözetim önlemlerinin yalnızca "demokratik bir toplumda gerekli" olduğunda uygulanmasını, özellikle kanunlarda özel hayatın korumasını sağlamak üzere yeterli ve etkili güvencelerin ve garantilerin bulunmasını ifade eder. Son olarak, Mahkemenin bu davalarda benimsediği "kanunun kalitesi" ve "usuli güvenceler" yaklaşımının gelecekte önüne gelecek benzeri türdeki toplu gözetim ve yapay zeka ile ilgili davalar için ne ölçüde geçerli olacağını zaman gösterecektir.

Anahtar Kelimeler: *Kitle iletişiminin gözetimi, YZ ile ilgili davalar, AİHS m.8 özel hayatın korunması hakkı, usulî güvenceler, hukukun kalitesi.*

PROCEDURAL SAFEGUARDS REGARDING THE BULK MASS SURVEILLANCE: AN ASSESSMENT OF TWO ECHR JUDGMENTS

ABSTRACT

On 25 May 2021, ECHR Grand Chamber ruled in the In Centrum för Rattvisa v. Sweden and Big Brother Watch and Others v. UK that the UK and Swedish governments violated the EConHR Article 8 as their national legislations on bulk mass surveillance (BMS) did not contain adequate procedural safeguards for the protection of privacy. The Court's approach in these judgments should be examined from various aspects. First, the Court decided the case in abstractio and decide that the case is admissable even before the exhaustion of domestic remedies. The Court has easen the victim status by eliminating the requirement of the individual harm but reling on potential victim. Second, the Court assessed if the relevant legislation on BMS satisfies the "quality of law" requirement. Although in its previous cases the Court decided on the procedural safeguards in targetted survelliance regimes, this time decided on the requirements of

minimum procedural safeguards in their laws on BMS. The ECHR ruled that "operating a bulk interception regime did not per se violate the Convention", however, the Respondent States' legislation on BMS must provide "end-to-end safeguards" for the protection of privacy. The Court asserted that the legality of the BMS will be assessed by evaluating the requirements of "in accordance with law" and "necessity" together. The "quality of law" requires not only the relevant laws to be "accessible and foreseeable", but also the BMS can be permitted only if they are "necessary in a democratic society", and adequate and effective safeguards and guarantees are provided against violation of privacy.

Keywords: *Bulk Mass Surveillance, AI Related cases, ECHR art. 8 right to privacy, procedural safeguards, quality of law.*

GİRİŞ

Avrupa İnsan Hakları Mahkemesi Büyük Daire(si) 25 Mayıs 2021 tarihinde verdiği iletişimin kitlesel gözetimine ilişkin *Big Brother Watch and Others v. Birleşik Krallık* [BD][1] ve *In Centrum för Rattvisa v. İsveç* [BD][2] kararlarında İsveç'in ve Birleşik Krallık'ın iletişimin kitlesel gözetimine ilişkin mevzuatlarının Avrupa İnsan Hakları Sözleşmesinin 8. ve 10. maddelerine uygunluğunu denetlemiştir.

İletişimin kitlesel gözetimi sorunu, 2013 Edward Snowden'in ABD Ulusal Güvenlik Ajansının[3] (NSA) iletişime küresel müdahalesini ifşa etmesi ile uluslararası kamuoyunun gündemine geldi. Değerlendirilecek kararlar, iletişime kitlesel müdahaleye, bu müdahale sonucunda elde edilecek verilerin korunmasına, elde edilen verilerin istihbarat paylaşımına ilişkin ulusal düzenlemelerde, başta kanunlarda bulunması gereken minimum usulî güvenceleri hükme bağlamaları bakımından önemlidirler. İletişime kitlesel müdahale, ulusal güvenliğin korunması ve ağır suçların önlenmesi, terörizmle mücadele, siber saldırıların önlenmesi, casusluk faaliyetlerinin, seçimlere müdahalenin önlenmesi, uyuşturucu kaçakçığı ya da çocuk pornosu ile mücadele ve benzeri amaçlarla yapılmaktadır.

[1] *Big Brother Watch and Others v. the United Kingdom*, BN. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

[2] *Centrum för Rättvisa v. Sweden*, BN. 35252/08 (ECtHR May 25, 2021).

Kararlar uyarınca, iletişime kitlesel müdahale *per se* AİHS'ye aykırı değildir; taraf devletlerin kitle iletişiminin gözetimine ilişkin konularda takdir marjları geniştir. Mahkeme, belli kişilerin izlendiği hedefli kitle müdahalelerine ilişkin önceki kararlarında ilgili mevzuatın Sözleşmeye uygunluğunu incelemiş konuya ilişkin bazı usulî güvenceler öngörmüşse de söz konusu güvenceler bu makalenin inceleme konusu olan kitle iletişiminin gözetimi bakımından yeterli değildir. Bunun sebebi, iletişimin kitlesel gözetimi ile yalnızca belli/bazı belirteçlerin kullanılması yoluyla geniş çapta, milyonlarca kişinin verilerinin toplanmasıdır. Her iki durumda da iletişime müdahale söz konusu olsa da kitle iletişiminin izlenmesi sonuçları itibariyle hedefli kitle müdahalelerine nazaran kitlesel temel hak ihlallerine sebep olabilir.

Mahkemeye göre, Avrupa İnsan Hakları Sözleşmesi çerçevesinde özel hayatın gizliliğinin korunması bakımından kitle iletişiminin gözetimine ilişkin mevzuatın ilk aşamadan son aşamaya kadar bazı usulî güvenceler içermesi gereklidir. Bu çerçevede, kitle iletişiminin gözetimine ilişkin kararın, izinlerin alınması, bunların uygulanması ve sona erdirilmesi aşamalarında usule ilişkin güvenceler sağlanmalı ve söz konusu işlem ve eylemler yargısal denetime açık olmalıdır. Keza, ulusal mevzuatta kitle iletişimine müdahale sürecinde kanunlarda her aşamada alınacak önlemlerin orantılılık ve gereklilik bakımından denetlenmesi öngörülmelidir. Bu çerçevede, kanunlarda iletişime kitlesel müdahale kararının yürütmeden bağımsız bir organ tarafından alınmasına; her bir operasyonun amacının ve kapsamının tanımlanmasına; her bir operasyon sona erdiğinde yürütmeden bağımsız bir organ tarafından denetlenmesine ilişkin güvenceler bulunmalıdır. Keza kanunlarda, gözetim yapan ülkelerin uygun bir zaman sonrasında çalınmasını önlemek için elde edilen verileri yok etmesine ilişkin hükümler de bulunmalıdır.

Bu davaların en büyük katkısı; Büyük Dairenin kitle iletişiminin gözetimine ilişkin Mahkeme içtihadında bir boşluk olduğunu tespit etmesi, bunun ardından özellikle kitle iletişimine müdahaleyi düzenleyen ulusal mevzuatın içermesi gereken güvenceleri belirlemesidir.

Her iki karar büyük ölçüde paralel hükümler içermektedir. *Big Brother Watch v. Birleşik Krallık* ve *In Centrum för Ratvisa v. İsveç* kararlarını inceleyeceğimiz bu çalışma kapsamında öncelikle, genel olarak bu davaların özelliklerinden söz edilecek; sonrasında her bir dava bakımından başvurucular ve başvuruculara iddiaları; Büyük Dairenin her

iki dava bakımından hüküm altına aldığı ortak konular; Büyük Dairenin ayrı ayrı davalar için verdiği hükümler ele alınacak son olarak yargıçların ve doktrinin kararlara yönelik eleştirileri üzerinde durulacaktır.

I. İletişime Kitlesel Müdahaleye ve Değerlendireceğimiz Davalara İlişkin Ön Açıklamalar

İncelenecek kararlarda öncelikle iletişime kitlesel müdahalenin hangi aşamalardan geçilerek yapılabileceği açıklanmıştır. Teknolojinin gelişmesi sebebiyle günümüzde iletişime devasa boyutlarda müdahaleler söz konusu olmakta neredeyse otomatik olarak kitle iletişimine ulaşılabilmektedir. Söz konusu müdahalenin nasıl gerçekleştiğinin bilinmesi, ilgili hakların anlamlı bir şekilde korunması bakımından çok önemlidir. Kitle gözetimi/izlenmesi[4], iletişime toplu müdahale Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde düzenlenen özel hayatın korunması hakkının kapsamındadır. Kitlesel gözetim her ülkede ya da her zaman aynı şekilde gerçekleşmese de aşama aşama gerçekleşen bir süreç

[4] "Kitlesel gözetim" (mass surveillance), iletişimin kitlesel gözetimi (mass surveillance of correspondence) çeşitli kurum ve örgütler bünyesinde farklı şekillerde anılmaktadır. Birleşmiş Milletler Genel Kurulu kitle dijital gözetimi (mass digital surveillance), çevrimiçi gözetim (online surveillance), toplu müdahale (bulk interception), Venedik Komisyonu 2015 tarihli Güvenlik Hizmetleri ve Sinyal İstihbarat Ajansları Demokratik Denetim Raporunda (the Venice Commission in its Report on Democratic Oversight of Security Services and the Report on Democratic Oversight of Signal Intelligence Agencies) stratejik genel gözetim (exploratory or generalized surveillance), AİHM kararlarında (*Klass ve Diğerleri v. Almanya, 6 Eylül 1978, Series A no. 28;* ve *Weber and Saravia v. Almanya, BN.54934/00, 29 Haziran 2006*) ise ya da genel gözetim, iletişime toplu müdahale i kitle iletişimine müdahale (bulk interception of communications), stratejik izleme (strategic monitoring) ifadeleri kullanılmıştır. Bkz.: Domazet, Sinisa; Dinic Slavica: ''International Legal Aspects of Mass Surveillance and Implications of Privacy'', Kultura Polisa, C. 19, S. 1, 2022, s. 87; bu çalışmada ise "gözetim" (surveillance), iletişimin kitlesel gözetimi, kitle iletişiminin gözetimi, kitlesel gözetim (bulk surveillance) ifadesi tercih edilmiştir: Türkçe terminoloji tercihleri için bkz.: Güzey, Emre: ''AİHM Kararları Çerçevesinde Kitlelerin İstihbarat Maksatlı Gözetimi'', SAVSAD Savunma ve Savaş Araştırmaları Dergisi, C. 30, S. 2, 2020, s. 197-208; Molu, Benan: ''İHAM Büyük Dairesi'nin Brother Watch v. Birleşik Krallık kararlarının özet çevirisi: Kitlesel dinleme ve iletişim hizmeti sağlayıcılarından iletişim verilerinin alınması rejimi, özel hayatı ve ifade özgürlüğünü ihlal eder.'', Anayasa Gündemi, 2021. (https://anayasagundemi.com/2021/06/25/iham-buyuk-dairesinin-big-brother-watch-ve-digerleri-v-birlesik-krallik-kararinin-ozet-cevirisi-kitlesel-dinleme-ve-iletisim-hizmeti-saglayicilarindan-iletisim-verilerinin-alinmasi/ Erişim Tarihi: 25/06/2021; Yokuş Sevük, Handan: ''Kolluk Tarafından Suçun Önlenmesine Yönelik Yapılan İletişimin Denetlenmesine İlişkin Değerlendirmeler'', Türkiye Barolar Birliği Dergisi, S. 67, 2006, s. 41-56.

olduğu için her bir aşamada 8. maddenin ihlal edilip edilmediği değerlendirilmelidir. Mahkemeye göre, kitlesel gözetim kabaca aşağıdaki aşamalardan geçerek gerçekleşmektedir.

İlk aşama, elektronik haberleşmeye istihbarat örgütleri tarafından ilk müdahale, başka bir deyişle haberleşmenin ve haberleşme verilerinin ele geçirilmesidir; çok sayıda kişinin iletişimine müdahale edilen ilk aşamada bazı verilerin filtre edilmesi mümkündür.

İkinci aşama, elde edilen haberleşme ve haberleşme verilerine bazı spesifik belirteçlerin uygulanmasıdır. Bu aşamada, yapılacak araştırmalar için e-mail adresleri gibi güçlü ve/veya karmaşık sorgular içeren belirteçler kullanılabilir; hatta hedeflenen kişilere ulaşmak için algoritmalar kullanılmaya başlanabilir;

Üçüncü aşamada, müdahale sonucu elde edilen veriler analistler tarafından değerlendirilir;

Son aşamada ise elde edilen verinin saklanması, "son ürünün" kullanılması ve bunların üçüncü taraflarla paylaşılması söz konusudur.[5]

Büyük Daire, iletişime kitlesel müdahalenin ve kitlesel gözetimin istihbarat teşkilatları bakımından suçların ve tehditlerin önlenmesi için çok önemli olduğunu bu sebeple, devletlerin bu konudaki takdir marjlarının geniş olduğunu belirtmiştir.

A. Kabul Edilebilirlik Şartlarına İlişkin Özellikler

AİHM'ye yapılan bireysel başvuruların kabul edilebilirliği için diğer kabul edilebilirlik şartları yanında başvuru sahibinin 34. maddede belirtilen başvurucu kategorilerinden (gerçek kişiler, birey; hükümet dışı kuruluşlar, NGO; kişi grupları) birine dahil olması ve başvurucunun Sözleşmenin ihlalinden kaynaklanan bir mağduriyetinin olması gerekir. Mahkeme, kural olarak, kanunların ya da idari uygulamaların soyut olarak (*in abstracto*) Sözleşmeye aykırılık iddialarını kabul etmemekte; *a priori* iddiaları reddetmekte yalnızca mevcut zararlara ilişkin başvuruları kabul etmektedir. Kural olarak, başvurucular kendileri bakımından herhangi bir

[5] *Big Brother Watch and Others v. Birleşik Krallık, p.* 325; *In Centrum för Rattvisa v. İsveç,* p. 239.

kişisel etki yaratmayan kanunlara ya da idari uygulamalara karşı *in abstracto* iddiada bulunamazlar.

Ayrıca Mahkeme, başvurucunun kendi çıkarlarını değil de başkalarının veya bir bütün olarak toplumun çıkarlarını korumak için açtığı davaları (*actio popularis)* da kabul etmemektedir. Başvuruculaların kural olarak, şikayetine konu olan önlemlerden "doğrudan doğruya etkilenmiş olduklarını" kanıtlamaları gereklidir.[6] Oysa, söz konusu davada başvuruculaların amacı kendilerinin yanında "başkalarının menfaatlerinin veya toplumun haklarının korunmasıdır."[7] Mahkeme büyük ölçüde önüne gelen davalarda, somut olayda yasama, yürütme, yargı organlarının ve idarenin Sözleşmeyi ihlal edip etmediğine ve bunun neticesinde bir mağduriyetin doğup doğmadığına ilişkin kararlar vermektedir. Ele aldığımız davalarda ise bu durumun bir istisnası söz konusudur; bunun sebebi bu tür davalarda başvuruculaların kitle iletişimlerine müdahale edildiğini ve müdahale neticesinde bireysel olarak mağdur olduklarını bilmelerinin dolayısıyla mağduriyetlerini ve zararlarını kanıtlamalarının neredeyse mümkün olmamasıdır. Bütün bu sebeplerle potansiyel mağdurların başvuruları kabul edilmiş ve başvuruların iç başvuru yollarını tüketmeleri koşulu aranmamıştır.[8]

Davalarda gizli gözetimle ile ilgili mevzuatın ve mevzuattan kaynaklanabilecek ancak henüz gerçekleşip gerçekleşmediği bilinmeyen bir uygulamanın yerine yalnızca soyut olarak hukuki rejimin, mevzuatın, kanunların Sözleşmeye uygunluğu değerlendirilmiştir. Bu tür soyut değerlendirmelerde, mevzuattan kaynaklanan yetkinin henüz kullanılıp kullanılmadığına, bir mağduriyetin doğup doğmadığına bakılmaksızın ya da uygulamanın Sözleşmeye aykırı olup olmadığı değerlendirilmeksizin yalnızca mevcut mevzuatın uygulanması halinde ortaya çıkabilecek

[6] Sloot, Bart van der/Kosta, Eleni: ''Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance'' European Data Protection Law Review, C. 5, S. 2, 2019, s. 252-261.

[7] AİHM önündeki *in abstracto* iddialar ayrıntılı açıklamalar için bkz.: Kosta, Eleni: ''Algorithmic state surveillance: Challenging the Notion of Agency in Human Rights'', Regulation & Governance, C. 16, S. 1, 2020, s. 216.

[8] Sloot, Bart van der: ''Big Brother Watch and Others v. the United Kingdom & Centrum for Rattvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?'', European Data Protection Law Review, C. 7, S. 2, 2021, s. 321.

ihlaller değerlendirilmektedir.[9] Bu çerçevede, Sözleşmeye aykırılığın sebep olduğu bir mağduriyetin henüz oluşup oluşmadığı bilinmeden, mevzuat ya da uygulamadan doğan bireysel mağduriyet kanıtlanmadan hatta bir mağduriyet iddiasında bulunulmadan, yalnızca iletişime müdahaleyi düzenleyen mevzuatın gerekli güvenceleri içerip içermediğinin denetlenmesi söz konusudur.

Benzeri bir soyut değerlendirme, 2015 tarihli *Zakharov v. Rusya* davasında söz konusu olmuştur. Mahkeme, *Zakharov v. Rusya* ve önceki bazı davalarda[10] hedefli kitle dinlemelerinin Sözleşmeye uygun olarak yapılabilmesi için ilgili mevzuatın içermesi gereken bazı güvencelere ilişkin kararlar vermiştir. Bu davaların en önemli katkısı, Büyük Dairenin hedefli kitle iletişimine müdahaleye ilişkin içtihadında bir boşluk olduğunu tespit etmesi ve hedefli kitle iletişimine müdahaleyi düzenleyen mevzuatın içermesi gereken usulî güvenceleri belirleyerek bu boşluğu doldurma yoluna gitmesidir.[11]

Ele alacağımız davalarda ise hedefli kitle iletişimine müdahaleden farklı olarak yalnızca bazı belirteçlerin kullanılması (sondajlama) yolu ile yapılan iletişimin kitlesel gözetimi Sözleşmenin 8. ve 10. maddelerine uygunluk bakımından değerlendirilmektedir. Mahkeme, bu davalarda da söz konusu mevzuatın yeterli denge ve denetim güvenceleri içerip içermediğini değerlendirirken devletin kitlesel gözetim yetkisini henüz kullanıp kullanmadığına bakmaksızın soyut bir değerlendirme yapmıştır. Başka bir deyişle, Büyük Daire, başvurucuların bireysel zararı olup olmadığına ya da yetkinin gerçekte yürütme organı tarafından kanuna uygun olarak kullanılıp kullanılmadığına ilişkin bir değerlendirme

[9] Mevzuatın soyut olarak Sözleşmeye aykırılığının ele alındığı benzeri bir dava ise *Dudgeon v. Birleşik Krallık, BN. 7525/76,* ve *Roman Zakharov v. Rusya* [BD], 2015, p. 173-78 davalarıdır. Bkz: Practical Guide on Admissability Criteria, updated on 31 August 2023, Council of Europe, https://www.echr.coe.int/documents/d/echr/admissibility_guide_eng; Gerards, Janneke: General Principles of European Court of Human Rights, Cambridge University Press, 2019.

[10] *Roman Zakharov v. Rusya*, BN. 47143/06; *Kennedy v. Birleşik Krallık*, BN. 26839/05, 18 Mayıs 2010, p. 155; *Klass and Others v. Almanya*, BN. 5029/71, 6 Eylül 1978, A 28.

[11] Sloot, Bart van der: ''The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases'', Journal of Intellectual Property, Information Technology and E-Commerce Law: JIPITEC, C. 11, S. 2, 2020, s. 163-164.

yapmadan yalnızca ilgili kanunların soyut olarak belli usulî güvenceleri içerip içermediğine yoğunlaşmıştır.[12]

B. Başvurucular ve İddiaları

1. In Centrum för Rattvisa v. İsveç

Centrum för Rattvisa, insan haklarına ilişkin davalarla ilgilenen, kâr amacı gütmeyen bir sivil toplum örgütüdür; çeşitli faaliyetleri gereği ülke içinde ve dışındaki kişilerle, benzeri örgütlerle, şirketlerle e-mail, telefon ve faks üzerinden haberleşmekte ve özel hayatın gizliliği bakımından hassas konularda bilgi paylaşımları söz konusu olmaktadır.

Centrum för Ratvisa, İsveç'te özellikle "sinyal istihbaratı" olarak adlandırılan iletişime toplu müdahalelerin gerçekleştirildiği iddiasında bulunmaktadır. "Sinyal istihbaratı", elektronik sinyallerden elde edilen istihbaratın yakalanması (ele geçirilmesi), işlenmesi, analiz edilmesi ve raporlanması anlamına gelmektedir. Sinyal istihbaratında veri trafiği çoğunlukla kablolar üzerinden gerçekleşmektedir. Bu şekilde elde edilen istihbarat, iletişimin içeriğine ve bunlarla ilgili iletişim verilerine (konum, gönderen, alıcı vb.) ilişkin olabilir.

Centrum för Rättvisa, İsveç'te etkin bir başvuru yolu olmadığı gerekçesi ile iddiaları için iç hukuk yollarına başvurmamıştır. İsveç kanunları uyarıca, dış istihbarat, dış politikayı, savunma ve güvenlik politikasını desteklemek ve ülkeye yönelik dış tehditleri tespit etmek amacıyla yürütülmektedir. İsveç'te dış istihbarat elektronik sinyallerin toplanması ile yapılmaktadır ve "Sinyal İstihbarat Kanunu[13]" ile düzenlenmektedir; bu kanun ile, Savunma Bakanlığı'na bağlı bir kamu kurumu olarak Ulusal Savunma Radyo Dairesi[14] (FRA) kurulmuş ve sinyal istihbaratı yürütme yetkisi bu kuruma verilmiştir.[15] Kanun uyarınca, FRA kitlesel müdahaleleri gerçekleştirmeden önce tamamıyla gizlilik içinde görev yapan Dış İstihbarat Mahkemesinden[16] izin almalıdır.

---

[12] Sloot: The Quality of Law:… s. 164-165.

[13] Signals Intelligence Act.

[14] National Defence Radio Establishment.

[15] 'Centrum för Ratvisa v. Sweden', https://globalfreedomofexpression.columbia.edu/cases/centrum-rattvisa-v-sweden/, erişim tarihi:10.11.2022.

[16] The Foreign Intelligence Court.

Başvurucular, sinyal istihbaratına ilişkin mevzuatın ve ilgili uygulamanın Sözleşmenin 8. maddesini geçmişte ihlal ettiğini ve bu ihlalin başvuru sırasında dahi devam ettiğini iddia etmiştir.

2. Big Brother ve Diğerleri v. Birleşik Krallık

Dava, ABD Ulusal Güvenlik Kurumu'nda sözleşmeli olarak çalışan Edward Snowden'in ABD ve Birleşik Krallık ulusal istihbarat servislerinin, iletişime müdahale ve istihbarat paylaşımının kötüye kullanıldığının ve bunlara ilişkin delillerin kamuoyu ile paylaşmasından sonra açılmıştır. Başvurucular, çeşitli sivil toplum örgütleri, kâr amacı gütmeyen gruplar, akademisyenler ve gazetecilerdir.[17]

Başvuruculara göre, Birleşik Krallık Hükümet İletişim Daire Başkanlığı[18] (GCHQ) ve Birleşik Krallık Sinyal İstihbarat Ajansının[19] faaliyetleri özel hayatın gizliliğini ve ifade özgürlüğünü ihlal etmektedirler. TEMPORA isimli bir program çerçevesinde sınır aşan iletişime otomatik olarak müdahale edilmekte ve yeraltı kablolarından devasa büyüklükte veri elde edilmektedir. Ayrıca, ABD Ulusal Güvenlik Ajansı[20] (NSA) tarafından PRISM ve UPSTRAM gözetim programlarını kullanarak elde edilen veriler Birleşik Krallık istihbaratına aktarılmaktadır. Son olarak, internet servis sağlayıcılarından geniş kapsamlı olarak ham (metadata) haberleşme verileri toplanmaktadır.

Bütün bunlar iletişimin toplu gözetimi olarak adlandırılmakta; 2000 tarihli Soruşturma Yetkilerini Düzenleme Kanunu[21] (RIPA), GCHQ'ya bu suretle elde edilen verilerin depolanması, sonrasında belli kriterler esas alınarak filtre edilmesi ve daha sonra incelenmesi konusunda yetkiler vermektedir.

---

[17] *Big Brother Watch and Others v. Birleşik Krallık* (BN. 58170/13); *Bureau of Investigative Journalism and Alice Ross v. Birleşik Krallık* (BN. 62322/14); and *10 Human Rights Organisations and Others v. Birleşik Krallık,* (BN. 24960/15).

[18] Government Communications Headquarters (GCHQ).

[19] Signal Intelligence Agency (SIGINT).

[20] U.S. National Security Agency (NSA).

[21] Regulation of Investigatory Powers Act.

Başvurucular, ilk olarak RIPA[22] çerçevesine çeşitli kitlesel müdahale teknikleri uygulanarak kendilerine ilişkin verilerin de elde edilmiş olabileceği; ikinci olarak yabancı devletlerle elde edilmiş olan verilerin istihbarat olarak üçüncü taraflar ile paylaşıldığı ve üçüncü olarak yine aynı Kanunun İkinci Bölümü çerçevesinde (muhtemelen) iletişim servis sağlayıcılarından da kendilerine ait verilerin elde edildiği iddiasında bulunmuşlardır.

Başvurucular, iddia edilen bu önlemlerin Sözleşmenin 8. maddesine uygun olmadığını; ayrıca ikinci ve üçüncü iddialar bakımından Sözleşmenin ifade özgürlüğünü düzenleyen 10. maddesinin ihlal edildiğini iddia etmektedirler.

II. Büyük Dairenin Her İki Dava İçin Verdiği Kararlardaki Ortak Noktalar

Büyük Dairenin her iki dava için aldığı kararlarda temel olarak iki ayrı konuda değerlendirmeler yapmaktadır. Bu konulardan ilki kitle iletişiminin gözetimine ilişkin hukuki düzenlemeler diğeri ise gizli gözetim tedbirlerine ilişkin genel ilkeler ve güvencelerdir. Esasen ele aldığımız davaların kitlesel gözetime ilişkin kuralların, güvencelerin oluşmasına yaptığı en önemli katkılar da bu paragraflarda yer almaktadır. Burada ele alacağımız ilk konu kitle iletişiminin gözetimine ilişkin hukuki düzenlemelerdir.

A. Kitle İletişiminin Gözetimine İlişkin Hukuki Düzenlemeler[23]

Mahkeme, her iki kararda da yaklaşık 50-60 paragrafta kitlesel gözetime ilişkin Uluslararası Hukuk, Avrupa Birliği Hukuku düzenlemelerini belirterek, ilgili karşılaştırmalı hukuk kuralları ve sınırlı olarak uygulamalar (Avrupa Konseyine üye bazı ülkeler ve ABD) konusunda örnekler vermiştir; bu paragraflar her iki kararda büyük ölçüde paraleldir.

[22] 1. section 8(4) of the RIPA.

[23] *Big Brother Watch and Others v. Birleşik Krallık,* p. 191-252; *In Centrum för Rattvisa v. İsveç,* p. 81-146.

1. Uluslararası Hukuk Düzenlemeleri

a. Birleşmiş Milletler Hukuku

Dijital Çağda Gizlilik Hakkı ile ilgili 68/167 sayılı 2013 tarihli BM Kararı,[24] tüm devletleri, insan hakları hukuku kapsamında gizliliği daha iyi sağlamak için gözetimle ilgili politikalarını ve uygulamalarını gözden geçirmeye; şeffaflığı ve hesap verebilirliği sağlamak için bağımsız, etkin denetim mekanizmaları oluşturmaya davet etmektedir.

Keza, 1992 Uluslararası Telekomünikasyon Birliği Anayasası ve Sözleşmesi[25] de Üye Devletlerin vatandaşlarının uluslararası yazışmalarının gizliliğini mümkün olduğu ölçüde güvence altına alması gereğini düzenlemektedir.

b. Avrupa Konseyi

Kararlarda, Avrupa Konseyi bünyesinde hazırlanan çeşitli belgelere atıf yapılmaktadır. Bunlar, Kişisel Verilerin Otomatik İşleme Taâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi,[26] Sözleşmenin Ek Protokolü,[27] 1995 Telekomünikasyon Hizmetleri Alanında Kişisel Verilerin Korunmasına ilişkin Bakanlar Komitesinin Tavsiye Kararı,[28] 2001 Budapeşte Siber Suçlar Sözleşmesi[29] ve "2015 Sinyal İstihbarat Teşkilatlarının Demokratik Gözetimi Hakkında Kanun Yoluyla Demokrasi için Avrupa Komisyonu Raporu[30]"dur. Bütün bu

[24] The Right to Privacy in the Digital Age: resolution adopted by the General Assembly, A/RES/68/254, 2013.

[25] 1992 Constitution and Convention of the International Telecommunication Union.

[26] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

[27] The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181).

[28] Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services, Recommendation (No. R (95) 4 of the Committee of Ministers).

[29] 2001 Convention on Cybercrime, Budapest Convention ETS No.185 and its Protocols.

[30] The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies.

belgelerde, BM Kararında ortaya konulan benzer gizliliği koruma ilkeleri yinelenmiş ve benimsenmiş, etkili bir gözetim çağrısında bulunulmuştur.

2. Avrupa Birliği

Avrupa Birliği Temel Haklar Şartı,[31] Avrupa İnsan Hakları Sözleşmesinin tamamlayıcısı niteliğindeki maddelerinde özel hayat ve aile hayatına, kişisel verilerin korunmasına, ifade ve bilgi edinme özgürlüğüne ilişkin hükümler içermektedir. Mahkeme, Veri Koruma Yönetmeliğinin, Genel Veri Koruma Yönetmeliğinin[32] (GDPR) ve Gizlilik ve Elektronik İletişim Yönetmeliğinin[33] özel hayatın gizliliği ile ilgili olabilecek hakları tanıyan ve koruyan düzenlemelerini işaret etmekte; ayrıca Avrupa Birliği Adalet Divanı'nın verilerin korunmasına ilişkin kararlarından örnekler vermektedir.[34]

3. Karşılaştırmalı Hukuk

Kararlarda Finlandiya, Fransa, Almanya, Hollanda, İsveç, İsviçre ve Birleşik Krallık olmak üzere resmi olarak en az yedi akit devletin kablo üzerinden ya da havadan kitle iletişimine müdahale gerçekleştirdikleri belirtilmektedir. İstihbarat paylaşma anlaşmalarına gelince en az 39 akit devlet diğer bir devletle istihbarat paylaşım anlaşması yapmıştır ya da böyle bir anlaşma yapması imkân dahilindedir. Söz edilen anlaşmalardan ikisi yabancı bir gücün kendilerine adına verilere müdahalesini açıkça yetkilendirirken ikisi de açıkça bu tür bir müdahaleye izin vermiştir. Diğer devletlerin ise konuya ilişkin tutumları net değildir. Son olarak, birçok devlet yurtdışında ve içinde uygulanabilecek standartları benzer şekilde tespit etmiştir; elde edilmiş verilerin kullanılması için çeşitli sınırlamalar getirilmiştir; bazı ülkelerde ise gereksiz hale geldiğinde verilerin yok edilmesine ilişkin yükümlülükler de mevcuttur.

---

[31] The Charter of Fundamental Rights of the European Union.

[32] The General Data Protection Regulation ("GDPR") adopted in 2016.

[33] The Privacy and Electronic Communications Directive Directive 2002/58 EC.

[34] Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and ärntner Landesregierung and Others (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238); Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970); Ministerio Fiscal (Case C-207/16; ECLI:EU:C:2018:788).

B. Gizli Gözetim Önlemlerine İlişkin Genel İlkeler ve Güvenceler

AİHS'nin 8. maddesinde düzenlenen hakların sınırlandırılmasına ilişkin genel ilkeler aynı maddenin 2. fıkrasında aşağıdaki şekilde düzenlenmiştir.

> "Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin hukuka uygun 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 önlem olması durumunda söz konusu olabilir."

Öncelikle, Mahkeme Sözleşmenin 8. maddesinin ihlaline ilişkin bir iddia önüne geldiğinde başvurucunun iddiasının 8. madde ile korunan hakların kapsamına girip girmediğini değerlendirmektedir. Daha sonra, Mahkeme, söz konusu hakkın sınırlandırılması ya da hakka bir müdahale söz konusuysa çeşitli aşamalardan geçerek bu sınırlamanın, müdahalenin Sözleşmeye uygunluğunu denetlemektedir.

Mahkeme, gizli gözetim önlemleriyle ilgili kararlarında da hakların sınırlamasına ilişkin temel ilkeleri esas almıştır. 8. madde bakımından hakların sınırlandırılmasına ilişkin ilkeler, 8. maddenin 2. fıkrası uyarınca "sınırlamanın hukuka uygun olması" (in accordance with law) ve 2. fıkranın atıfta bulunduğu "meşru amaçlardan birinin ya da birkaçının sağlanması amacıyla yapılmış olması ve demokratik bir toplumda bu amaçlara ulaşmak için gerekli olmasıdır".[35]

1. Hukuka Uygunluk Koşulu

"Hukuka uygunluk" koşulu ile önlemin iç hukukta bir temelinin olması aranmaktadır. Sınırlandırmanın 8. maddenin amaç ve kapsamında yer alan ve Sözleşmenin giriş kısmında söz edilen hukuk devleti ilkesi ile bağdaşması gerekir. Ayrıca, "hukuka uygunluk" çerçevesinde kanuni

[35] *Roman Zakharov v. Rusya*, p. 227; *Kennedy v. Birleşik Krallık*, BN. 26839/05, 18 Mayıs 2010, p. 130.

düzenlemelerin ilgili kişiler bakımından "ulaşılabilir olması" ve etkilerinin muhatapları tarafından öngörülebilir olması gerekir.[36]

Hukuka uygunluk koşulu, alınan önlemin iç hukukta bir temelinin olmasını gerektirmektedir. Bunun anlamı, bir hakkın sınırlanmasının kanun ya da bağlayıcılığı olan bir düzenleme hatta içtihat ile yapılmasıdır. Mahkeme, *Big Brother Watch and Others v. Birleşik Krallık* kararında "söz konusu kanuni düzenlemenin ilgili kişiler bakımından erişilebilir ve kanunun etkilerinin yeterince öngörülebilir olması gereğini" ifade etmiştir. Bu çerçevede, "demokratik toplumda gereklilik ve öngörülebilirlik koşullarının karşılanması için iç hukukun erişilebilir olması, yeterli ve etkin güvence ve garantileri içermesi gerekmektedir."[37] Hukuka uygunluk koşulunun gerçekleşmesi için ulusal hukuk açık, öngörülebilir ve yeterince erişilebilir olmalıdır.[38]

a. Yeterince Erişilebilir Olma Koşulu

Mahkeme kararlarında, yeterince erişilebilir olma koşulu, "gizli gözetim faaliyetleri bakımından, iç hukukun ya da kanuni düzenlemenin yeterince erişilebilir olması, gizli gözetiminin kapsamına ve süresine, verilere erişilmesine, verilerin saklanmasına, incelenmesine, kullanılmasına, elde edilen verilerin iletilmesine ve imha edilmesine, izin usullerine, gizli gözetim önlemlerinin uygulanmasının denetlenmesine yönelik düzenlemelere, bildirim mekanizmalarına ve ulusal mevzuatın öngördüğü çözüm yollarına yeterince erişilebilirliği" ifade etmektedir.[39]

b. Öngörülebilir Olma Koşulu

Öngörülebilir olma koşulu, iç hukukun bireylere, kamu kurumlarının hangi koşulda ve hangi durumlarda kendilerine Sözleşmede

---

[36] AİHS 8. Madde Rehberi, Özel Hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı, European Court of Human Rights, Güncelleme Tarihi 31 Ağustos 2019, *Big Brother Watch and Others v. Birleşik Krallık,* p. 332.

[37] *Big Brother Watch and Others v. Birleşik Krallık,* p. 361-365.

[38] Council of Europe, Guide on Article 8, Respect for Private and Family Life, Home and Correspondence, updated on 31 August 2020, p. 15; *Silver ve Diğerleri v. Birleşik Krallık*, p. 87.

[39] *Roman Zakharov v. Rusya*, p. 238; ayrıca, *Dragojević v. Hırvatisyan*, BN. 68955/11, 15 Ocak, 2015, p. 83; *Szabó and Vissy v. Macaristan*, BN.: 37138/14, 12 Ocak 2016, p. 56; *Centrum för Rättvisa v. İsveç*, BN. 35252/0819 Haziran 2018; *Big Brother Watch and Others v. Birleşik Krallık*, BN.58170/13, 13 Eylül, 2018, p. 307.

tanınan haklarını etkileyebilecek önlemlere başvurulabileceği konusunda yeterli işaretlerin sağlaması gerektiğini ifade eder.[40] Öngörülebilirlik mutlak bir öngörülebilirlik şeklinde anlaşılmamaktadır; başvurucular, en azından hukukçuların yardımıyla da olsa makul bir oranda, konu ile ilgili mevzuata tâbi olacaklarını öngörebilmelidirler.[41]

Hukuki düzenlemeler, kişilerin hukuka uygun olarak hareket etmesini sağlayabilecek ölçüde öngörülebilir olmalı ve kamu kurumlarının takdir yetkisinin kapsamını açık bir şekilde belirlemelidir. Örneğin, Mahkeme'nin gözetime ilişkin davalarda vurguladığı üzere, kanun hükümleri, vatandaşlara, hangi koşullarda ve durumlarda kamu kurumlarının gizli gözetim ve veri toplama faaliyetine yetkili olacakları hususunda yeterli ölçüde açık olmalıdır.[42]

Gizli gözetim önlemleri kapsamında öngörülebilirlik, diğer alanlardan bir ölçüde farklı anlaşılmalıdır. "Öngörülebilirlik", bireylerin iletişimin dinlenmesi gibi gizli gözetim önlemlerini ve çeşitli önlemlere başvurma ihtimalinin yüksek olduğunu öngörmesi ve davranışlarını buna göre ayarlaması anlamına gelmemektedir.[43] Ancak, özellikle gizli gözetim konusunda yürütmeye verilen yetkilerin gizlilik içinde icra edilmesi keyfilik tehlikesini arttıracaktır. Keza, gözetim teknolojilerinin sürekli olarak gelişmesi ve alınabilecek önlemlerin gittikçe daha da sofistike hale gelmesi gizli gözetime ilişkin kuralların açık ve ayrıntılı olmasını gerektirmektedir. İç hukuk düzenlemeleri, kamu kurumlarının hangi durumlarda ve koşullarda hangi önlemlere başvurmaya yetkili oldukları konusunda yeterince açık olmalıdır. Ayrıca, kanunlarda, keyfi müdahaleye karşı yeterli koruma sağlamak üzere yetkili makamların takdir yetkisinin kapsamı ve yetkilerin kullanılma biçimleri yeterli açıklıkla düzenlenmelidir.[44]

---

[40] AİHS 8. Madde Rehberi, parag. 14; *Fernández Martínez v. İspanya [BD],* BN. *56030/07, 2014,* p. 117.

[41] AİHS 8. Madde Rehberi, parag. 14; *Slivenko v. Letonya* [BD], BN. 48312/99, 9 Ekim 2003, p. 170.

[42] AİHS 8. Madde Rehberi, parag. 12, Bkz.: *Shimovolos v. Rusya,* BN. 30194/09, 21 Haziran 2011, p. 68.

[43] *Big Brother Watch and Others v. Birleşik Krallık,* p. 333; *In Centrum för Rattvisa v. İsveç,* p. 247

[44] *In Centrum för Rattvisa v. İsveç,* p. 247.

Gerards'a göre, birçok davada, bütün bu koşullar "öngörülebilirlik" koşulu çerçevesinde değil "orantılılık" ve "gereklilik" ya da "usuli pozitif yükümlülükler" çerçevesinde değerlendirilmektedir. Yazar, bu sebeple, sınırlama koşullarının birbirleriyle bağlantılı olduğunu ifade etmektedir.[45]

c. Kanunun Kalitesi Sorunu; Kanunlarda Çeşitli Usulî Güvencelerin Sağlanması

Gizli gözetime ilişkin kanunların açık ve ayrıntılı olması önemlidir ve gizli gözetim sürecinin farklı aşamaları için farklı kurallar ve güvenceler öngörülebilir. Bu çerçevede, gizli gözetim sırasında veri elde etme sürecinin aşamaları yukarıda da belirttiğimiz şekilde Mahkeme tarafından tanımlamıştır.

(a) ilk olarak iletişimin dinlenmesi ve iletişim verilerinin saklanması, ele geçirilmesi;

(b) saklanan, ele geçirilen iletişim verilerine belirli seçicilerin uygulanması yoluyla bazı iletişim verilerinin seçilmesi;

(c) seçilen iletişim ve ilgili iletişim verilerinin analistler tarafından incelenmesi; ve

(d) incelenen verilerin depolanması ve "nihai ürünün" kullanılması, verilerin üçüncü taraflarla paylaşılması.[46]

Bu aşamalar, özellikle Mahkemenin aşağıda ele alacağımız usulî güvencelerin baştan sona ve gizli gözetimin her aşamasında sağlanması gerektiğini hükme bağlaması sebebiyle önemlidir. *Turanjanin*, aşamaların özellikle sonlarına doğru özel hayatın gizliliğine ilişkin ihlallerin artabileceği gerekçesiyle aşağıda ele alacağımız güvencelerin artarak sağlanması gereğini vurguluyor.[47]

---

[45] Gerards: s. 219.

[46] *Big Brother Watch and Others v. Birleşik Krallık, p.* 333; *In Centrum för Rattvisa v. İsveç,* p. 247.

[47] Turanjanin, Veljko: ''When does bulk interception of communications violate the right to privacy? The limits of the state's power and European Court of Human Rights Approach'', International Cybersecurity Law Review, C. 4, S.1, 2023, s. 115.

Van der Sloot makalesinde, Mahkemenin Sözleşmede yer alan hakların sınırlandırılmasına ilişkin içtihadındaki gelişmeleri özetlemiştir. Mahkeme, ilk kararlarında yürütmenin kanunlarla düzenlenmiş sınırlamalar içinde kalıp kalmadığını denetlerken, 80'lerden itibaren hukuka uygunluğu 'erişilebilirlik ve öngörülebilirlik' koşulları çerçevesinde incelemiştir. Günümüzde ise Mahkeme, özellikle gizli gözetim gibi niteliği gereği yürütmenin bilfiil yetki kullandığı alanlarda "kanunun kalitesi" çerçevesinde kanunlarda bazı usul güvencelerinin mevcut olup olmadığını denetlemeye başlamıştır.[48]

Keza, yazar, Mahkemenin önceki kararlarında da "erişilebilirlik ve öngörülebilirlik" koşullarının özel hayatın gizliliği alanında uygulanması konusunda çekingen olduğunu belirtmektedir. Bunun sebebi hiç kuşkusuz, yukarıda açıkladığımız üzere gizli gözetimin niteliği gereği gizli bir şekilde icra edilmesidir. Mahkeme, gizli gözetim tedbirlerinin Sözleşmeye uygunluğunu ele aldığı davalarda "erişilebilirlik" ve "öngörülebilir" koşullarını daha esnek bir şekilde değerlendirirken hukuka uygunluk koşulu çerçevesinde önüne gelen kanunların bazı usulî güvenceler içermesi gerektiğine hükmetmiştir.[49] Mahkeme ilk kez, *Malone v. Birleşik Krallık* davasında "hukuka uygunluğun yalnızca mevcut ulusal hukuka uygunluk şeklinde anlaşılamayacağına", "hukuka uygunluğun 'kanunun kalitesi' ile ilgili olduğuna", "sınırlandırmaların 'Sözleşmenin Giriş kısmında açıkça belirtilen hukukun üstünlüğü' ile bağdaşması gerektiğine" hükmetmiştir.[50] Mahkeme, özellikle, gizli gözetimde de olduğu üzere yürütme organının bilfill yetki kullanmasını gerektiren alanlarda, ilgili kanuni düzenlemelerde bu yetkilerin kullanımına ilişkin ek bazı koşulların, sınırlamaların ve güvencelerin öngörülmesi gereğini ifade etmiştir. Bunun anlamı, gizlilik arzeden konularda, Mahkemenin Sözleşmeye uygunluk konusunda yapacağı değerlendirmeler sırasında mevcut kanunlarda özel hayatın korunmasına ilişkin (usule ilişkin) güvencelerin yasama organı tarafından sağlanıp sağlanmadığının denetlemesidir.[51]

---

[48] Sloot: The Quality of Law:… s. 179; ayr. bkz.: Kaplan, Onur: ""Hukuk Devleti" Bağlamında Kanun Kalitesi, Hukuk ve Adalet Eleştirel Hukuk Dergisi, C. 10, S.23, 2018, s. 83-118.

[49] Sloot: The Quality of Law:… s.163-164.

[50] *Malone v. Birleşik Krallık*, BN. 8691/79, 2 Ağustos 1984, p. 67.

[51] Sloot: The Quality of Law:… s.165.

Mahkeme, gizli gözetimi düzenleyen mevzuatın Sözleşmeye uygunluğu önüne geldiğinde "hukuka uygunluk" ve "müdahalenin gerekliliği" şartlarını birlikte değerlendirmektedir. Bu çerçevede "kanunun kalitesi" ile mevcut kanunların iç hukukun "erişilebilir ve öngörülebilir olması" yanında gizli gözetim önlemlerinin kötüye kullanılmasını engelleyecek etkin ve yeterli güvence ve garantiler içermesi ve sınırlamanın demokratik bir toplumda gerekli olması aranmaktadır.

aa. Kanunlarla Sağlanması Gereken Minimum Altı Güvence

Mahkeme, *Weber ve Saravia v. Almanya* ve *Liberty ve Others v. Birleşik Krallık*[52] kararlarında da ceza soruşturma ve kovuşturmaları sırasında belli kişilerin izlendiği hedefli müdahalelerin Sözleşmeye uygunluğunu incelemiş ve ilgili mevzuatta bulunması gereken minimum güvenceleri öngörmüşse de bu güvenceler kitle iletişiminin gözetimi söz konusu olduğunda yeterli değildir. Günümüzde teknolojik gelişmeler çok daha geniş kapsamlı müdahalelere imkan tanımaktadır. Daha önceki davalarda, Mahkeme hedefli müdahale ile kitle gözetimi arasındaki önemli farkları da yeterli açıklıkta ortaya koymamıştır. Hedefli müdahaleye nazaran kitle gözetimi çoğunlukla uluslararası iletişimin izlenmesine yöneliktir, yabancı istihbaratın toplanması ve bilinen ya da bilinmeyen aktörlerden kaynaklanabilecek tehditlerin saptanması amacıyla yapılmaktadır.[53]

Mahkeme, hedefli ya da ceza soruşturması çerçevesinde iletişime müdahaleye ilişkin davalar bakımından geliştirdiği içtihadında, yürütmenin gücünü kötüye kullanılmasını önlemek için kanunlarda açıkça düzenlenmesi gereken minimum usul güvencelerini belirtmiştir. Aşağıda belirteceğimiz usule ilişkin bu güvenceler "Altı Weber Güvencesi"[54] olarak adlandırılmaktadır.[55] Bu güvenceler kanunlarda

1. iletişime müdahale kararı alınabilecek suç tiplerinin belirtilmesine;

---

[52] *Weber and Saravia v. Almanya* (dec.), BN. 54934/00, 2006-XI; *Liberty and Others v. Birleşik Krallık*, BN. 58243/00, 1 Temmuz 2008; bkz.: *Big Brother Watch and Others v. Birleşik Krallık,* p. 335; *Centrum för Rättvisa v. İsveç*, p. 249 .

[53] *Big Brother Watch and Others v. Birleşik Krallık,* p. 332; *Centrum för Rättvisa v. İsveç*, p. 236.

[54] "Six Weber Criteria".

[55] Bkz.: *Big Brother Watch and Others v. Birleşik Krallık, p.* 361-2; *Centrum för Rättvisa v. İsveç*, p. 275-6.

2. iletişimlerine müdahale edilecek kişi kategorilerinin tanımlanmasına;

3. müdahale süresinin sınırlandırılmasına;

4. müdahale neticesinde elde edilen verilerin incelenmesi, kullanılması ve depolanması sırasında izlenmesi gereken usullerin;

5. elde edilen verilerin diğer Devletlerle paylaşılması sırasında alınması gereken önlemlerin;

6. müdahale neticesi elde edilen verilerin hangi durumlarda yok edileceğinin, kayıtların silinmesinin ya da silinebilmesinin düzenlenmesine ilişkindir.

Mahkeme, *Roman Zakharov v. Rusya* kararında da AİHM, "konu ile ilgili mevzuatta aşağıda inceleyeceğimiz 'usule ilişkin minimum güvencelerin' bulunması halinde öngörülebilirliğin gerçekleşeceğini" belirttikten sonra aynı altı asgari güvencenin, mümkün olduğu ölçüde ulusal güvenlik sebebiyle yapılan kitle iletişimin gözetimi bakımından da geçerli olacağına hükmetmiştir.[56]

Bununla beraber, toplu gözetim rejiminin 8. maddeyi ihlal edip etmediğini değerlendirilirken altı asgari güvenceye ek bazı güvencelerin de sağlanması gerekmektedir.[57] Günümüzde iletişim teknolojilerinin eriştiği düzey göz önüne alındığında, iletişime kitlesel müdahaleye ilişkin rejimlerin içermesi gereken (usule ilişkin) güvencelerin genişletilmesi gereği açıktır. Ele aldığımız davalarda da kitle gözetimine ilişkin mevzuatın içermesi gereken usule ilişkin güvencelerin daha da genişletilmesi yönünde kararlar verilmiştir. Mahkeme, daha sonra gizli gözetime ilişkin yeni bir dava önüne geldiğinde ilgili devletin kanunlarında bu güvencelerin yer alıp almadığını değerlendirecek, bu güvencelerin olması halinde "kanunun kalitesi" koşulunun sağlandığına hükmedecektir.

[56] *Roman Zakharov v. Rusya*, (GC) BN. 47143/06, 4 Aralık 2015.

[57] *Roman Zakharov v. Rusya*, p. 335.

bb. Ele Alınan Davalar Bakımından Kanunlarla Sağlanması Gereken Sekiz Minimum Güvence[58]

Makalenin konusu olan kitle iletişiminin gözetimi, suçların önlenmesi için istihbarat elde edilmesi amacıyla yapılmaktadır. Kitle iletişiminin gözetimi önlemi, belli bir suç çerçevesinde kişilerin yakalanması ya da yargılanması amacı ile uygulanmamaktadır. Bu sebeple, "Altı Weber Güvencesi" arasında yer alan "müdahale kararı alınabilecek suçların tipleri" ve "iletişimlerine müdahale edilecek kişi kategorilerinin tanımlanması" ya da "makul şüpheye" ilişkin güvencelerin kitle gözetimi alanında uygulaması söz konusu değildir. Buna karşılık, kitle iletişiminin gözetimine izin verilme sebepleri, iletişime toplu müdahalenin kendisine özgü koşulları kanunlarda açıkça ve yeterli ek güvenceler içerecek şekilde düzenlenmelidir.

Özellikle, kitle iletişimine müdahalenin niteliği gereği gizli olması bazı ciddi ihlal risklerini de beraberinde getirmektedir. Ele aldığımız kararlar uyarınca, ulusal kanunlarda kitle iletişiminin gözetiminde ilk aşamadan son aşamaya kadar[59] yeni bazı usul güvencelerin getirilmesi özel hayatın gizliliğinin sağlanması bakımından gereklidir. Buna göre, kitle iletişiminin gözetimine ilişkin izin verilmesi, gözetimin uygulanması ve sona erdirilmesi aşamalarında usule ilişkin güvenceler sağlanmalı ve bu amaçla alınacak kararlar ve uygulama denetlenebilmelidir. Belirtilen kararlar uyarınca, ulusal mevzuatta kitle iletişimine müdahaleye ilişkin önlemlerin, her aşamada orantılılık ve gereklilik bakımından denetlenmesi öngörülmelidir. Keza, mevzuatta iletişime kitlesel müdahaleye yürütmeden bağımsız bir organ tarafından izin verilmesine; her bir operasyonun amacının ve kapsamının tanımlanmasına; bir operasyon sona erdiğinde yürütmeden bağımsız bir organ tarafından denetlenebileceğine ilişkin güvenceler bulunmalıdır. Son olarak, kanunlarda gözetim yapan ülkelerin elde ettikleri verileri, uygun bir zaman sonrasından çalınmasını önlemek için, yok etmeleri de düzenlenmelidir.

---

[58] *Big Brother Watch and Others v. Birleşik Krallık,* p. 365-427; *In Centrum för Rattvisa v. İsveç,* p. 246-374.

[59] Bu çerçevede Büyük Daire, kitle iletişimine müdahalenin aşama aşama (adım adım) gerçekleştiğini belirtmiştir. Bu aşamalar ve müdahale ilerledikçe Sözleşmenin 8. maddesinin ihlali söz konusu olabilir ya da ihlal daha da artabilir. Mahkemeye göre, müdahalenin her bir aşamasında 8. maddenin uygulanması mümkündür. *Big Brother Watch and Others v. Birleşik Krallık,* p. 330.

Bu konuya ilişkin olarak her iki kararda da ortak olan bazı paragrafların değerlendirilmesi gerekir. Öncelikle, kararlarda yer alan "iç hukukta sürecin baştan sona her aşamasında alınacak önlemlerin *gereklilik ve orantılılık* bakımından değerlendirilmesi gerekir. İletişimin toplu gözetimine yürütmeden bağımsız bir organ tarafından izin verilmesi; operasyonun amaç ve kapsamının açıkça tanımlanması, denetime tâbi tutulması ve bağımsız bir *ex post facto* gözden geçirme mümkün olmalıdır."[60] ifadesi çok önemlidir.

Büyük Daire, iletişimin toplu denetlenmesinin kötüye kullanılmasını önlemek için sürecin baştan sona sahip olması gereken güvenceleri belirlemiştir. Bunu yaparken, Mahkeme, yalnızca kitle iletişiminin gözetimine ilişkin kanuni düzenlemeleri kanunun kalitesi açısından değil aynı zamanda sürecin işleyişi ve uygulamayı da değerlendirmelidir. Mahkeme bütün bu güvencelerin olup olmadığına karar verirken rejimin isleyişiyle ilgili tüm hususları dikkate alacaktır, iç hukukun kötüye kullanmaya karşı gerekli garantileri içerip içermediğine ve baştan sona güvencelere sahip olup olmadığına yoğunlaşacaktır. Burada müdahale rejiminin aslında nasıl işlediğine, gerçekte kötüye kullanmanın olup olmadığına bakılacaktır. Bu çerçevede, kitle iletişiminin gözetimine ilişkin yetkinin kullanımı sırasında denge ve denetim mekanizmalarının işleyip işlemediği ve kötüye kullanım iddiaları varsa bunlara ilişkin deliller de değerlendirilecektir.[61]

Keza, Mahkeme davalı devletin dar takdir marjı içinde hareket edip etmediğini değerlendirirken yukarıda belirttiğimiz altı Weber Güvencesinden daha ayrıntılı usul güvenceleri üzerinden bir değerlendirme yapmaktadır. *Lubin*, Mahkemenin altı Weber Güvencesini bu kararlarda reddettiğini ifade etse[62] de kanımızca burada bir redden ziyade altı Weber Güvencesinin geliştirilmesi, toplu gözetime uyarlanması söz konusudur. Mahkeme, "kanuna uygunluk" ve "gereklilik" koşullarını

[60] *Big Brother Watch and Others v. Birleşik Krallık,* p. 361; *In Centrum för Rattvisa v. İsveç,* p. 264.

[61] *Big Brother Watch and Others v. Birleşik Krallık,* p. 360; *In Centrum för Rattvisa v. İsveç,* p. 274.

[62] Lubin, Asaf: ''Introductory Note to Big Brother Watch v. UK (Eur. Ct. H. R. Grand Chamber)'', International Legal Materials, C. 61, S. 4, 2022, s. 605-653.

birlikte değerlendirerek aşağıda belirtilecek güvencelerin iç hukukta açık bir şekilde düzenlenip düzenlenmediğini inceleyecektir.[63]

Kararlarda, "iç hukukta düzenlenen toplu gözetim rejiminin demokratik bir toplumda "gereklilik" ve "öngörülebilirlik" koşullarının sağlanması için içermesi gereken yeterli ve etkin güvenceler ve garantiler,"[64] "Minimum Sekiz Güvence" olarak adlandırılmıştır. Kararlarda ayrıca kanunlarda yer alması gereken her bir güvencenin "gereklilik" ve "orantılılık" koşulları bakımından inceleneceği de belirtilmiştir.

Bu çerçevede kanunlarda sağlanması gereken güvenceler aşağıdaki gibi özetlenebilir.

1. Toplu gözetime hangi sebeplerle izin verilebileceğinin kanunlarda düzenlenmesi gereklidir. İlke olarak izin sebeplerinin geniş tutulması kötüye kullanma potansiyeli artacaktır. Sebeplerin dar ve sıkı bir şekilde tanımlanması halinde ise toplu gözetime ancak bu sebep "gerekli ve orantılı" ise izin verilebilir. Kanunda öngörülen bir sebep çerçevesinde yetkilendirme yapılması halinde yeterli ve etkin güvencelerin söz konusu olduğu kabul edilecektir. Mahkemeye göre, toplu gözetimin sebepleri göreceli olarak geniş düzenlemiş olsa da rejim bir bütün olarak değerlendirildiğinde yeterli güvencelerin sağlanmış olup olmadığı değerlendirilecektir.

2. Hangi durumlarda iletişimin gözetilebileceği;

3. Kitle iletişiminin gözetimine izin verilirken izlenmesi gereken usul;

Toplu gözetime yürütmeden bağımsız bir kurum tarafından izin vermelidir; ancak bu kurumun yargı organı olması şart değildir. İzin alınacak kurum, yürütme tarafından müdahalenin amacı, sağlayıcılar (bearers) ve muhtemelen hangi iletişim rotalarına müdahale edilebileceği konusunda bilgilendirilmelidir. Bu sayede, izin verecek kurum gereklilik ve orantılılık konusunda bir değerlendirme yapabilecektir. Bazı belirteçlerin seçilmesi toplu gözetimin en önemli aşamalarındandır. Bütün belirteçler olmasa bile bu aşamada gözetim sırasında kullanılacak

[63] *Big Brother Watch and Others v. Birleşik Krallık,* p. 361.

[64] *Big Brother Watch and Others v. Birleşik Krallık,* p. 347.

"belirteçlerin tipleri ve kategorileri" belirlenmelidir. İstihbarat servisleri kullanmak istedikleri bütün bu belirteçleri gereklilik ve orantılılık bakımından gerekçelendirmelidir.

4. Müdahale neticesinde edilen verilerin seçilmesi, incelenmesi ve kullanılması sırasında izlenmesi gereken usullerin kanunlarda düzenlemesi;

5. Kitlesel gözetim sonucu elde edilen verilerin diğer ülkelerle (uluslararası örgütlerle) paylaşılması sırasında alınması gereken önlemler bakımından ise alıcı devletlerin bütün bu standartlara tam olarak uyması beklenmemektedir. Bununla beraber, gazetecilik materyalleri gibi özel gizlilik içeren konularda alıcı devletin standartlara uyması beklenebilir; verilerin yabancı istihbarat ortakları ile paylaşılması da bağımsız bir denetime tabi olmalıdır.

6. Kanunlarda, iletişime müdahalenin süresinin sınırlandırılması, elde edilen materyalin depolanması, bu materyalin silinmesi ve yok edilmesi gereken durumların düzenlenmesi gereklidir.

7. Kanunların, yukarıda sayılan güvencelere uyulup uyulmadığının her aşamada bağımsız bir denetim organı tarafından denetlenmesinin sağlaması için usuller ve modeller içermesi gerekmektedir. Keza, hukuka aykırılık iddiaları konusunda yetkili olacak denetim organının ve yetkilerinin ve alınan önlemlerin her aşamada gereklilik ve orantılılık bakımından bağımsız bir otorite tarafından yeterli derecede denetlenmesi için İstihbarat Servislerinin gözetimin her aşamasında detaylı kayıtlar tutmasına ilişkin yükümlülüğünün kanunlarda düzenlenmesi gerekir.

8. Kanunlarda, *ex post facto* hukuka uygunluk denetiminin bağımsız bir organ tarafından yapılmasına yönelik usuller öngörülmeli ve hukuka aykırılık iddiası halinde görevli olacak bu organın yetkileri düzenlenmelidir. İstihbarat servisleri tarafından iletişimine müdahale edildiğinden şüphe duyan herkese bu müdahalenin hukuka ya da Sözleşmeye uygunluğunu denetleyecek etkin bir başvuru yolu sağlanmalıdır. Bu başvuru yolunun yargısal olması şart değildir; ancak yürütmeden bağımsızlığı; keza uygulamaların ve süreçlerin adil olması sağlanmalıdır. *Ex post facto* denetim çerçevesinde mümkün olduğunca çekişmeli bir yargılama yapılmalı; organın kararlarının bağlayıcı ve gerekçeli olması gereği de kanunlarda düzenlenmelidir.

Mahkeme bu güvencelerin iletişimin yalnızca içeriğinin korunmasına yönelik olmasını yeterli görmemektedir; aynı güvenceler ayrıca verilerin toplanması ve metaverinin işlenmesi sırasında da sağlanmalıdır.[65]

2. Müdahalenin Meşru Bir Amaca Ulaşmak için Demokratik Bir Toplumda Gerekli Olması

a. Müdahalenin Meşru Bir Amacı Desteklemesi Koşulu

Sözleşmenin 8. ilâ 11. maddelerinin ikinci paragraflarında yer alan meşru bir amacın varlığını tespit sırasında Mahkeme oldukça kısa ve öz bir değerlendirme yapmaktadır.[66] 8. maddenin 2. fıkrasında madde ile korunan hakların ihlalini haklı kılabilecek meşru amaçlar "ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir önlem olmasıdır." olarak belirtilmiştir. Mahkeme alınan önlemin ya da hakka yapılan müdahalenin meşru bir amacı desteklediğinin davalı Hükümet tarafından gösterilmesini beklemektedir.[67] Ele aldığımız kararlarda da, "müdahalenin meşru bir ya da birkaç amaca ulaşmak için demokratik bir toplumda gerekli olması" koşulu vurgulanmıştır.[68]

---

[65] *Big Brother Watch and Others v. Birleşik Krallık,* p. 342-363-4.

[66] AİHS 8. Madde Rehberi, parag. 18; bkz.: *S.A.S. v. Fransa* [BD], BN. 43835/11, 1 Temmuz 2014, p. 114.

[67] *Mozer v. Moldova Cumhuriyeti ve Rusya* [BD], BN. 11138/10, 2016, p. 194; Mahkeme, örneğin, hükümetin amacı nüfus yoğunluğu nedeniyle emek piyasasını düzenlemekse, göç önlemlerini, düzenin korunmasından ziyade Madde 8 (2) çerçevesinde ülkenin ekonomik refahının sağlanması amacıyla ile meşru olarak kabul edilebileceğini belirtmiştir, *bkz.: Berrehab v. Hollanda*, BN. 10730/84, 21 Haziran 1988, Series A no. 138, p. 26; Mahkeme, ayrıca, bir havalimanının genişletilmesi gibi büyük hükümet projelerini ekonomik refahın korunması bakımından meşru amaç olarak değerlendirmiştir. Bkz.: *Hatton ve Diğerleri v. Birleşik Krallık* [BD], BN. 36022/97, 2003-VIII, p. 121.

[68] *Big Brother Watch and Others v. Birleşik Krallık, p.* 338; *In Centrum för Rattvisa v. İsveç,* p. 246.

b. Müdahalenin "Demokratik Bir Toplumda Gerekli" Olması Koşulu

Demokratik bir toplumda gerekli olma koşulunun değerlendirilmesi sırasında Mahkeme çoğu zaman, başvurucunun 8. madde ile korunan menfaatlerini, üçüncü bir kişinin Sözleşme ve Protokollerin diğer maddeleriyle korunan menfaatleri ile dengelemeye gerek duymaktadır. [69] Mahkeme, özel hayata müdahalenin demokratik bir toplumda gerekli olması koşulunu çeşitli kararlarında vurgulamıştır; ele aldığımız bu kararlarında ise ek olarak demokratik toplumda gerekli olma koşulu çerçevesinde alınacak önlemin ulusal kanunların kalitesinin değerlendirilmesiyle hukukun üstünlüğünün sağlanacağını belirtmiştir.[70]

Bir müdahalenin "demokratik bir toplumda gerekli" olup olmadığını tespiti sırasında Mahkeme, başvurucunun hakları ile Devletin menfaatlerini dengelemektedir. Mahkeme, bu bağlamda "gerekli" ifadesinin "işe yarar", "makul" veya "arzu edilen" ifadelerindeki esnekliğe sahip olmadığını ve belli bir müdahale bakımından "zorunlu bir toplumsal ihtiyacın" varlığının aranması gerektiğini belirtmiştir. Her olay bakımından zorunlu bir toplumsal ihtiyacın olup olmadığına ilişkin değerlendirme öncelikle iç hukukta yetkili makamlar tarafından yapılmaktadır. İç hukuk makamlarının bu konuda takdir yetkisinin olduğu kabul edilmektedir. Ancak, elbette idari kararlar Mahkeme tarafından değerlendirilecektir. Bir hakkın sınırlandırılması, güdülen meşru amaçla orantılı olmadığı sürece "demokratik bir toplumda gerekli" olduğu kabul edilemez.[71]

Mahkeme, önüne gelen önlemlerin "demokratik bir toplumda gerekli" olup olmadığını değerlendirirken, bir bütün olarak dava göz önüne alındığında bu önlemleri meşru kılmak için belirtilen gerekçelerin ilgili ve yeterli; önlemlerin güdülen meşru amaçlarla orantılı olup olmadığını göz önüne alacağını belirtmiştir.[72] Ayrıca, Mahkeme, 8. madde bakımından "gerekliliğin" müdahalenin bir toplumsal ihtiyacın

---

[69] *Big Brother Watch and Others v. Birleşik Krallık,* p. 246-253; *In Centrum för Rattvisa v. İsveç,* p. 246-253.

[70] AİHS 8. Madde Rehberi, parag. 11;26; *Halford v. Birleşik Krallık, BN. 22009/93,* p. 49.

[71] AİHS 8. Madde Rehberi, parag. 22. Bkz. *Dudgeon v. Birleşik Krallık,* p. 51-53.

[72] *Z v. Finlandiya, BN. 22009/93,* p. 94.

karşılaması için zorunlu ve özellikle güdülen amaçla orantılı olması gerektiği anlamına geldiğini ifade etmiştir. Bir müdahalenin "gerekli" olup olmadığını belirlerken Mahkeme kamu kurumlarına verilen takdir yetkisinin kapsamını dikkate alacaktır; ancak müdahalenin toplumsal bir gereksinimin karşılanması bakımından zorunlu olduğunu davalı Devlet gösterecektir.[73]

Mahkeme, gizli gözetim faaliyetlerine ilişkin olan *Klass ve Diğerleri v. Almanya* kararında[74] "günümüzde çok gelişmiş casusluk biçimlerinin ve terörizmin demokratik toplumları tehdit ettiğini; bu tehditlerle etkin şekilde mücadele etmek için Devletin ülkesinde faaliyet gösteren bölücü gruplara karşı gizli gözetim önlemine başvurabilmesi gerektiğini hükme bağlamıştır. Mahkemeye göre, "mektup, posta ve telekomünikasyonun gizli şekilde izlenmesine ilişkin mevzuatın, istisnai durumlarda, ulusal güvenlik ve/veya kamu düzeninin korunması ve suçun önlenmesi için demokratik bir toplumda gerekli olduğu kabul edilmelidir." Ancak, Sözleşme uyarınca, vatandaşların gizli şekilde gözetimine yalnızca demokratik kurumların korunması amacıyla "kesin olarak gerekli" olduğunda izin verilebilir.[75] Buna göre, gizli gözetim önleminin demokratik kurumları korumak genel amacıyla yapılması ya da belli bir operasyon sırasında özel olarak yaşamsal verilerin elde edilmesi kesin olarak gereklilik olarak anlaşılabilir; bunlar söz konusu değilse kamu makamlarına kitle gözetimi konusunda izin verilmesi yetkilerini "kötüye kullanmaları" sonucunu ortaya çıkarır.[76]
Mahkeme, müdahalenin meşru bir amaca ulaşmak için "demokratik bir toplumda gerekli olma" koşulunu değerlendirirken ulusal güvenliğin korunması meşru amacına ne şekilde ulaşılabileceği konusunda ulusal makamların geniş bir takdir marjına sahip olduğunu belirtmiştir. Ancak Mahkeme, takdir marjına ilişkin değerlendirmesini mevzuatı, uygulamayı ve olayın bütün özellikleri dikkate alarak yapmalıdır. Bu çerçevede, alınacak olası önlemlerin kapsamı ve süresi, gerekçeleri, önlemlerin alınması, izin verme, yürütme ve onaylama konusunda yetkili makamlar; kararların ve uygulamanın denetlenmesi ve ulusal hukukta sağlanacak

[73] AİHS 8. Madde Rehberi, parag. 23, bkz. *Piechowicz v. Polonya, BN. 20071/07*, 17 Nisan 2012, p. 212.

[74] *Klass ve Diğerleri v. Almanya*, p. 48.

[75] AİHS 8. Madde Rehberi, parag. 526, bkz.: *Szabó ve Vissy v. Macaristan*, p. 72-73.

[76] AİHS 8. Madde Rehberi, parag. 526.

çözüm yolları göz önüne alınarak bir değerlendirme yapılmalıdır.[77] Örneğin, ulusal güvenliğin korunması amacıyla yapılan gizli gözetim demokratik süreçlerin düzgün bir şekilde işlemesini engelleyebilir. Bütün bu sebeplerle, yetkilerin kötüye kullanılmasına karşı yeterli ve etkin güvenceler sağlanmalıdır.[78]

Mahkeme, Sözleşmede yer alan hakları sınırlayıcı önlemlerin emredilmesini ve uygulanmasını denetlerken "müdahalenin" "demokratik bir toplumda gerekli" olanla sınırlı olup olmadığını değerlendirmektedir.[79]

Öncelikle, her iki kararda da çeşitli müdahalelerin birkaçı birlikte olsa dahi karmaşık yapıdaki suç örgütleri, terörizm ve yabancı devletlerin istihbaratı ile mücadelede iletişimin kitlesel gözetiminin yerini alamayacağı vurgulanmıştır. Büyük Daireye göre, iletişimin kitlesel gözetimi *per se* AİHS'ye aykırı değildir; taraf devletlerin kitle iletişiminin gözetimine ilişkin geniş bir takdir marjları vardır. Devletler ulusal güvenliklerini korumak için gerekli olan kitle gözetim rejimi oluşturabilirler. Başka bir ifadeyle, yalnızca kitle iletişimine müdahalenin çeşitli kanuni düzenlemelerde yer alması ve toplu müdahaleye ilişkin çeşitli uygulamalar 8. maddenin ihlali anlamına gelmemektedir.

c. Gereklilik ve Orantılılık (Ölçülülük) Koşulu

"Gereklilik ve orantılılık" ifadeleri *Big Brother Watch v. Birleşik Krallık* davasında 41, *In Centrum för Ratvisa v. İsveç* davasında ise 7 defa geçmektedir.

Mahkeme, gizli izlemeye izin veren mevzuatın Sözleşmeye aykırılığı iddiasını, müdahalenin hukuka uygun olup olmadığını denetlerken "kanuna uygun olma" ve "gereklilik" koşullarının birlikte ele alınmasının uygun olduğuna hükmetmiştir. Bu çerçevede "hukukun/mevzuatın kalitesi" yalnızca iç hukukun "erişilebilir ve uygulamasının öngörülebilir olması" anlamına gelmemektedir; bunun yanında gizli gözetim önlemleri özellikle kötüye kullanmaya karşı yeterli,

[77] *In Centrum för Rattvisa v. İsveç,* p. 253.

[78] *In Centrum för Rattvisa v. İsveç,* p. 248.

[79] *In Centrum för Rattvisa v. İsveç,* p. 253.

etkin koruma ve garantiler sağlamalı ve yalnızca "demokratik bir toplumda gerekli olduğunda" uygulanmalıdır.[80]

AİHM, kitle gözetiminin kötüye kullanılması riskini en aza indirmek için sürecin "baştan sona bazı güvencelere" tabi olması gerektiği kanaatindedir. Baştan sona sağlanması gereken güvenceler, ulusal düzeyde, sürecin her aşamasında alınan önlemlerin "gereklilik ve orantılılık" konusunda değerlendirme yapılmasını gerektirmektedir. Bu çerçevede, kararlarda operasyonun henüz amacı ve kapsamı tanımlanırken, kitle gözetiminin henüz başında bağımsız bir otoriteden izin alınması ve operasyonun *ex post facto* ve bağımsız denetime tabi olması gerektiği vurgulanmaktadır.[81]

Kararlarda, yetkilendirmeye ilişkin izne ve sürecin denetlenmesine ilişkin güvencelerin, kitle gözetimi konusunda 8. madde çerçevesinde yapılan başvurular bakımından kilometre taşı olduğu belirtilmektedir. Ancak, Büyük Daire, yargı makamları tarafından kitle gözetimine izin verilmesinin "keyfiliği önlemek bakımından önemli bir güvence" olduğunu belirtmekle beraber "zorunlu" olmadığı konusunda Daire ile aynı görüştedir; her halükarda kitle gözetimi konusunda izin verecek kurum yürütmeden bağımsız olmalıdır.[82]

Ayrıca, yetkinin kötüye kullanılmasını önlemek için izin verecek bağımsız kurum, müdahalenin amacı ve müdahale edilebilecek iletişim rotaları ya da iletişim sağlayıcıları konusunda kitle gözetimi konusunda yetki talep eden kurum tarafından bilgilendirilmelidir. Bu sayede, izin verecek bağımsız kurum kitlesel gözetim operasyonlarının ve yapılması düşünülen müdahalenin amacı ile servis sağlayıcıların (bearer) seçiminin gerekli ve orantılı olup olmadığını değerlendirecektir.[83]

Zalnieriute'e göre, kararlarda benimsenen gevşek ve usuli yaklaşım ile kitlesel gözetimin "vazgeçilmezliği" ve tehditlerle mücadele bakımından alternatifinin olmadığı vurgulanırken bu rejimler etkinlik ve orantılılık bakımından sorgulamamıştır. Yazar, kitlesel gözetimin ulusal

[80] *Big Brother Watch and Others v. Birleşik Krallık,* p. 334; *In Centrum för Rattvisa v. İsveç,* p. 248.

[81] *Big Brother Watch and Others v. Birleşik Krallık,* p. 350.

[82] *Big Brother Watch and Others v. Birleşik Krallık,* p. 351.

[83] *Big Brother Watch and Others v. Birleşik Krallık,* p. 352.

güvenliğin sağlanması bakımından gerekli ve etkin olduğunun farz edildiğini belirtmektedir.[84]

III. Mahkemenin Her Bir Davaya İlişkin Hükümleri

Kararlarda öncelikle, özellikle interneti kullanan uluslararası aktörlerden kaynaklanan tehlikelerin arttığından söz edilmiştir; bu sebeple devletlerin ulusal güvenliklerini korumak için seçecekleri gözetim yöntemleri konusunda geniş bir takdir marjına sahip oldukları belirtilmiştir. Bu sebeple, yanızca kitlesel gözetim rejiminin mevcut olması 8. maddenin ihlal edilmesi anlamına gelmemektedir.

A. In Centrum för Ratvisa v. İsveç

Öngörülen sekiz güvenceyi, İsveç'in iletişime kitlesel müdahale rejimine uygulayan Mahkeme, İsveç istihbarat servislerinin Sözleşme kapsamındaki yükümlülüklerini yerine getirmek için büyük özen gösterdiğini ve İsveç toplu dinleme rejiminin temel olarak Sözleşmede yer alan şartları karşıladığını belirtmiştir. Yukarıdaki sekiz güvenceyi değerlendiren Büyük Daire, İsveç'te kitle iletişime müdahaleye ilişkin mevzuatın "öngörülebilirlik" ve "demokratik toplum gerekleri" koşulları açısından, "yeterli" ve "etkin güvenceler" içerdiğine hükmetmiştir.

Mahkeme, İKİM rejimini sekiz güvence bakımından ele alarak ayrıntılı hukuk kuralları içerdiğine ve müdahaleyi açık bir şekilde sınırlamakta, uygun güvenceleri sağlamakta olduğuna hükmetmiştir. Bu çerçevede, kanunlarda, İsveç'te kitle iletişimine müdahaleye hangi sebeplerle izin verilebileceği;[85] keza İsveç'te kitle iletişimine hangi durumlarda müdahale edileceği ve müdahalenin denetimi yeterli açıklıkla düzenlenmiştir.[86] Bunlardan başka, izin alınırken izlenmesi gereken usul, İsveç kanunlarına göre, her istihbarat görevi çerçevesinde FRA tarafından yürütülecek izleme için önceden Dış İstihbarat Mahkemesinden[87] izin alınması gerekmektedir. Hiç şüphe yok ki, Dış İstihbarat Mahkemesi yürütmeden bağımsız olma şartını sağlanmaktadır; kanunda, müdahalenin

[84] Zalnieriute, Monika:''Big Brother Watch and Others v. the UK International Decisions'' American Journal of International Law, C. 116, S. 2, 2022, s. 590.

[85] *In Centrum för Rattvisa v. İsveç,* p. 284-288.

[86] *In Centrum för Rattvisa v. İsveç,* p. 289-294.

[87] Foreign Intelligence Court.

süresi ve denetlenmesi düzenlenmiştir. Müdahale neticesi elde edilen materyalin seçilmesi, incelenmesi ve kullanılması için getirilen usuller de kötüye kullanmaya karşı yeterli güvenceler içermektedir.[88] Keza, kanunlarda, elde edilmiş materyalin diğer devlet kurumlarına, yabancı devletlere ve örgütlere iletilmesi halinde alınması gereken önlemler de düzenlenmiştir.

Buna karşılık, İsveç Hukukunda müdahalenin süresine ilişkin sınırlamalar ve müdahale neticesinde elde edilen materyalin saklanmasına ve bu tür materyallerin silinmesine ve imha edilmesine ilişkin konular düzenlenmemiştir.[89]

Denetim bakımından önemli olan, 8. maddenin orantısız olarak etkilenme riskinin sınırlanması ve iç hukukta gereklerinin uygulanmasını sağlamak için ilke olarak bağımsız bir organın denetim gerçekleştirmesi ve yargısal ön-yetkilendirme usulünün bulunmasıdır. Büyük Daire, İsveç kitle iletişim rejimine müdahale rejiminin kanunun kalitesi (quality of law) koşulunu karşıladığını ve uygulamanın da "demokratik toplum ve gereklilik" sınırları içinde olduğuna karar vermiştir. Bu tespitlerden sonra Büyük Daire, İKİM rejiminde üç temel eksiklik tespit etmiştir. Mevcut güvenceler bu eksiklikleri gidermemiştir ve büyük ölçüde özel hayata saygı yükümlülüğünün ihlaline sebep olabilirler. Mahkeme ele alınan rejimin üç eksiği olduğuna hükmetti; bunlardan ilki, İsveç hukukunda ele geçirilen materyallerin kişisel veri içermemesi halinde imha edilmelerine ve silinmelerine ilişkin açık bir kuralın bulunmamasıdır.[90] İkinci eksiklik, Sinyal İstihbaratı Kanununda ve ilgili diğer mevzuatta istihbarat materyallerinin yabancı ortaklara aktarılmasına ilişkin kararlar alınırken özel hayatın gizliliğinin dikkate alınmasına ilişkin şart/kriter/güvence bulunmamasıdır.[91] İstihbarat değeri çok az olsa dahi haberleşmenin gizliliği ve özel hayatın gizliliği göz ardı edilerek bazı bilgilerin mekanik olarak yabancı istihbarat örgütlerine aktarılmasının bazı kişiler ve kurumlar bakımından çok ciddi sonuçları olabilir, bu şekilde yapılacak aktarımlar 8. madde bakımından orantısız tehlike yaratabilir. Ayrıca kanunlarda, FRA'ya yabancı istihbarat alıcısının kabul edilebilir bir teklif sunup sunmadığını belirlemek ve asgari düzeyde güvenlik önlemlerinin

[88] *In Centrum för Rattvisa v. İsveç,* p. 303-316.

[89] *In Centrum för Rattvisa v. İsveç,* p. 331-344.

[90] *In Centrum för Rattvisa v. İsveç,* p. 369-370.

[91] *In Centrum för Rattvisa v. İsveç,* p. 369.

analiz edilmesi konusunda bağlayıcı bir yükümlülük getirilmemektedir.[92] Son olarak, Mahkeme, iletişime kitlesel müdahaleye ilişkin şikayet ve soruşturmalara verilecek cevapların gerekçeli olması zorunluluğunun olmamasına atıf yaparak bunun temel hakların ihlal edilmesi halinde *ex post facto* denetim mekanizmasını zayıflatacağını belirtmektedir.[93]

Müdahalenin son aşamalarında etkin bir denetim yolunun öngörülmemesi Mahkemenin süreç ilerledikçe 8. maddedeki haklara müdahalenin derecesinin artabileceği yaklaşımı ile bağdaşmamaktadır. Bütün bu sebeplerle, Büyük Daire, İsveç mevzuatının "baştan sona güvence" koşulunu karşılamaması dolayısıyla keyfilik ve kötüye kullanmaya karşı yeterli ve etkin garantiler içermediği gerekçesiyle 8. maddenin ihlaline hükmetmiştir.[94]

B. Big Brother Watch and Others v. Birleşik Krallık

1. 8. Maddenin İhlali İddiasına İlişkin Olarak

Birleşik Krallık kitlesel gözetimi rejiminin Sözleşmenin 8. maddesini ihlal ettiği iddiasına ilişkin olarak; Mahkeme, kitlesel gözetimin Sözleşmeci Devletler bakımından ulusal güvenliklerine yönelik tehditlerin belirlenmesi bakımından hayati önemini kabul ettiğini belirtmektedir. Terörizm Mevzuatı Bağımsız İnceleme Uzmanı[95] da çok sayıda kapalı materyali inceledikten sonra özellikle, teröristler, suçlular ve düşman yabancı istihbarat servisleri ve giderek daha sofistike bir hal alan terörizm ile mücadelede kitlesel gözetiminin önemine dikkat çekmiştir. Internet'in doğası gereği belirli bir iletişimin gideceği yolun son derece belirsiz olması sebebiyle kitlesel gözetimin hedefli müdahale, insan kaynaklarının ve ticari siber savunma ürünlerinin kullanımı gibi alternatiflerinin birkaçı birarada uygulansa dahi kitle gözetiminin yerini alamayacağı anlaşılmaktadır.[96]

Mahkeme, bir bütün olarak bakıldığında, Kanunun 8(4) maddesinde düzenlenen rejimin, yukarıda belirtilen bazı sağlam

[92] *In Centrum för Rattvisa v. İsveç,* p. 371.

[93] *In Centrum för Rattvisa v. İsveç,* p. 354-365.

[94] *In Centrum för Rattvisa v. İsveç,* p. 368.

[95] Independent Reviewer of Terrorism Legislation.

[96] *Big Brother Watch and Others v. Birleşik Krallık,* p. 424.

güvenceleri[97] içerdiği; ancak bunların keyfilik ve suistimal riskine karşı baştan sona yeterli ve etkin güvenceler olmadığı görüşündedir.[98]

Özellikle, söz konusu rejimde aşağıdaki temel eksiklikler tespit edilmiştir: bu eksiklikler, kitlesel gözetimine izin verecek bağımsız bir yetkilendirme kurumunun bulunmaması, seçici kategorilerinin kanunlarda yeterli açıklıkta düzenlenmemesi, izin başvurusuna dahil edilmesi gereken bilgiler ve bireye bağlı seçiciler spesifik hale getirilse de bunun önceden içeride bir denetime tabi tutulmamasıdır. Başka bir deyişle, servis sağlayıcılarından kitlesel metadata elde edilmesi yalnızca ciddi suçlarla mücadele amacı ile sınırlandırılmamakta; ayrıca bağımsız bir denetime tabi tutulmamaları sebebiyle yürütülen programlara ilişkin kanun hükümleri "hukuka uygunluk" koşulunu karşılamamaktadır.[99]

Bu eksiklikler, iletişim içeriklerinin (contents of communications) ve ilgili iletişim verilerinin ele geçirilmesiyle ilgilidir.[100] Mahkemeye göre, İletişimin Dinlenmesi Komiserliği[101] bağımsız ve etkin olarak istihbarat servislerinin faaliyetlerini denetlese; Soruşturma Yetkili Mahkemesi[102] iletişimine gizli servislerce müdahale edildiğini düşünen kişilere önemli bir yargısal başvuru imkanı sunsa da yukarıda belirtilen eksikliklere karşı yeterli güvenceler sağlamamaktadır.[103]

Mahkeme, Kanunun 8(e) bölümünün "kanunun kalitesi" koşulunu karşılamaması sebebiyle müdahalenin demokratik toplum gerekleri çerçevesinde kalmasının mümkün olmadığını belirterek Sözleşmenin 8. maddesinin ihlal edildiğine hükmetmiştir.[104] Kanunun 8(4) maddesi, bazı ciddi güvenceler içerse dahi bir bütün olarak incelendiğinde "kanunun kalitesi" koşulunu karşılamamakta, keyfiliğe ve kötüye kullanmaya karşı baştan sona yeterli ve etkin güvenceler içermemektedir. Bu eksiklikler, kitlesel gözetim rejimi çerçevesinde gerçekleşen "müdahalenin"

[97] *Big Brother Watch and Others v. Birleşik Krallık,* p. 425.

[98] *Big Brother Watch and Others v. Birleşik Krallık,* p. 426.

[99] *Big Brother Watch and Others v. Birleşik Krallık,* p. 518-519.

[100] *Big Brother Watch and Others v. Birleşik Krallık,* p. 416.

[101] Interceptions of Communications Commisioner.

[102] The Investigatory Powers Tribunal (IPT).

[103] *Big Brother Watch and Others v. Birleşik Krallık,* p. 425.

[104] *Big Brother Watch and Others v. Birleşik Krallık,* p. 426.

"demokratik bir toplumda gerekli" olanla sınırlı tutulmadığı anlamına gelmektedir; dolayısıyla, Sözleşmenin 8. maddesi ihlal edilmiştir.[105]

Mahkeme, yabancı istihbarat servislerinden istihbarat elde edilmesi rejiminin "gerekli öngörülebilirlik" koşulunu karşıladığına ve güvenceler içerdiğine hükmetti. Bu çerçevede Mahkemeye göre, istihbarat servisleri, Sözleşmeye taraf olmayan devletlerden dinleme veya dinleme materyali talep etmesine veya bu materyale doğrudan erişmesine izin verilmesi söz konusu ise bağımsız denetime tabi olmalı ve ayrıca bağımsız geriye dönük inceleme mümkün olmalıdır. Mahkeme, incelemesini ABD Ulusal Güvenlik Ajansı'ndan (NSA) talep edilen dinleme materyalinin alınmasıyla ilgili şikayetle sınırlayarak, bu koşulların mevcut davada yerine getirildiğine ve elde edilen dinleme materyali (intercept material) talep etme ve elde etme rejiminin 8. maddeyi ihlal etmediğine hükmetmiştir.[106]

2. 10. Maddenin İhlali İddiasına İlişkin Olarak

İstihbarat servisleri, kitle iletişimini gözetimleri sırasında gazeteciler veya haber kuruluşlarıyla ilgili seçicileri ve arama terimlerini kullandığında bazı gazetecilik materyallerine erişebilir. Burada çok kapsamlı verilere ulaşılabileceği için gazetecilerin kaynaklarını koruması çok zorlaşacaktır. Mahkemeye göre, istihbarat servisleri, gazeteciler ile bağlantılı olduğu bilinen veya gizli gazetecilik materyallerine ulaşmalarını sağlayacak seçici terimleri ya da arama terimlerini kullanmadan önce, bir yargıç ya da bağımsız, tarafsız bir karar organından bu seçicilerin ya da arama terimlerinin kullanılması konusunda izin almalıdır. İzin konusunda bir değerlendirme yapacak olan bu organ, "üstün bir kamu yararının izni gerekli kılıp kılmadığını" ve özellikle "üstün kamu yararına hizmet edebilecek daha az müdahaleci bir önlemin yeterli olup olmayacağını" belirleme yetkisine sahiptir.[107]

Başvuruculara haber yapan kurumlar ve gazeteciler olmalarını dikkate alarak elektronik gözetim sırasında gizli gazetecilik belgelerinin, materyallerinin yeterince korunmamasını Büyük Daire tarafından ifade özgürlüğünün ihlali olarak değerlendirmiştir. Buna göre, gazetecilerin

[105] *Big Brother Watch and Others v. Birleşik Krallık,* p. 276.

[106] *Big Brother Watch and Others v. Birleşik Krallık,* p. 513, 514.

[107] *Big Brother Watch and Others v. Birleşik Krallık,* p. 457.

kaynaklarının ve gizli yazışmalarının korunması için gerekli güvencelere sahip olmaması sebebiyle RIPA II. Bölümde öngörülen rejimin işleyişi "kanuna uygunluk" koşuluna aykırılık gerekçesiyle 10. madde ihlal edilmiştir.[108] Ancak, Mahkeme, yabancı istibarat servislerinden istihbarat elde edilmesinin 10. maddeyi ihlal etmediğine hükmetmiştir.

IV. Kararlara Yönelik Eleştiriler

A. Yargıçlar

Yargıç *Lemmens, Vehabovic ve Bosnyak*,[109] Mahkemenin nadiren toplumların geleceklerini şekillendirecek kararlar verdiğini ve incelediğimiz kararların da bunların örnekleri olduklarını belirtmekte ve kararı yeteri kadar ileri gitmedikleri gerekçesiyle eleştirmektedir. Yargıçlara göre, Mahkeme, eline geçen fırsatı kısmen değerlendirerek kitlesel gözetim sırasında 8. ve 10. maddelerin korunması için kapsamlı ilkeler geliştirmiştir. Ancak, Büyük Dairenin bu davaların incelenmesi sırasında genel olarak özel hayatın gizliliğine ve özel olarak haberleşmenin gizliliğine daha fazla ağırlık vermesi gerekirdi. Yargıçlara göre, Mahkeme ileride önüne gelecek ve kitle iletişimine müdahale sırasında belli bir kişinin haklarının ihlal edilip edilmediğine ilişkin davalarda demokratik toplum düzeninin ve demokratik değerlerin sağlanması yönünde daha ileri ilkeleri benimseyecektir. Keza, kararlar, orantısız müdahalelere ilişkin net maddi güvenceler içermemektedir; örneğin kitle iletişiminin gözetimi öncesinde yargı organından karar alınmasına ilişkin bir düzenleme olmalıdır. Ayrıca, Büyük Dairenin çoğunluğunun aksine, bu üç yargıca ek olarak Yargıç *Ranzoni*, Birleşik Krallık'ın diğer ülkelerin istihbarat servislerinden veri ve istihbarat temin etmesinin de 8. ve 10. maddelerin ihlaline yol açabileceği görüşündedir.[110]

Yargıç *Pinto De Albuquerque* ise karşıt görüşünde, öncelikle kararların dilinin son derece muğlak olmasını eleştiriyor. Muğlak bir dil kullanmak çoğu zaman ilgili devletin kararın uygulanması konusundaki takdir yetkisini arttırırken bazen kararlarda yargıçların tereddütlerini açığa çıkarmaktadır. Böyle bir durum, Mahkemenin otoritesi sarsabilir ve kararlarla oluşturmak istenen standartları da zayıflatabilir. Yargıç,

[108] *Big Brother Watch and Others v. Birleşik Krallık,* p. 522, 528.

[109] Yargıçların kısmi görüşleri (partially concured that).

[110] *Big Brother Watch and Others v. Birleşik Krallık,* Joint partly dissenting opinion of Judges Lemmens, Vehabović, Ranzoni and Bošnjak.

Avrupa'da bazı kötü niyetli gizli servislerin Mahkemenin gevşek bir şekilde formüle ettiği kanuni standartlardan yararlanacağını ve eninde sonunda masum kişilerin bundan zarar göreceğini belirtmektedir.[111] Yargıç, AİHM'in sağladığı korumanın Avrupa Birliği Adalet Divanının sağladığı korumanın dahi gerisinde kaldığını belirtiyor. Keza, kararla kitlesel gözetiminin yararlı olması halinde *fait accompli* haline getirildiğini halbuki "yararlı olmanın" "demokratik toplumda gereklilik" ve "orantılılık" ile aynı anlama gelmediğini belirtmektedir. Bu kararlar, kitle izlenmesi konusunda geliştirilecek hukukun etkileyecektir. Yargıç günümüzde 23 Avrupa ülkesinin açık ya da üstü kapalı olarak hedefli olmayan veri müdahalesini yasakladığını; yalnızca yedi Avrupa Konseyi üyesi ülkede kitlesel müdahaleye ilişkin düzenlemelerin olduğunu belirtmektedir.

B. Doktrindeki Eleştiriler

Hemen belirtelim ki, atıf yapacağımız yazarlar, incelediğimiz kararları çeşitli sebeplerle eleştirmektedirler. *Zalnieriute*, kararları son derece zayıf olmaları ve büyük ölçüde savunmada kaldıkları gerekçesi ile eleştirmektedir. Yazara göre, bağımsız bir kurum tarafından yapılacak *ex post facto* denetim kitlesel müdahale rejiminin temeli olmalıdır; oysa kararlarda sayılan güvencelerin kanunlarda düzenlenmesi halinde rejimin 8. maddeye uygun olacağı belirtilmektedir. Kararlarda maddi hukuka uygun bir uygulamanın denetlenmesinden ya da mevcut rejimin etkinliğinden ziyade kanunlarda usulî güvencelerin mevcut olup olmadığı üzerinde durulmuştur. Yazara göre, Mahkeme açısından usulî güvenceler o kadar önemlidir ki, Mahkemenin bu davalar bakımından tüm yaptığı neredeyse altı Weber güvencesini bir ölçüde genişletmekten ibarettir.[112]

Doktrinde, ayrıca istihbarat verilerinin yabancı ülke istihbarat kurumlarına da verilmesi bakımından insan hakları hukuku bakımından ülke dışılık söz konusu olmasına rağmen kararlarda ülke dışılığa değinilmemesi eleştirilmektedir. *Asaf*, kararlarda ülke dışı uygulamaların ve istihbarat paylaşımı rejimlerinin yeterli bir şekilde incelenmemesini

[111] *Big Brother Watch and Others v. Birleşik Krallık*, partly concurring and partly dissenting opinion of the Judge Pinto de Albuquerque *In Centrum för Rattvisa v. İsveç* concurring opinion of Judge Pinto de Albuquerque.

[112] Zalnieriute, Monika:''Big Brother Watch and Others v. the UK International Decisions'' American Journal of International Law, C. 116, S. 2, 2022, s. 585-592, 589.

eleştirmektedir. Yazara göre, her iki konuda da Mahkemenin yeterli inceleme yapmamasının nedenlerini anlamak güçtür. Özellikle, istihbarat paylaşımı konusunda Büyük Daire, genel ve sınırlı bir çerçeve rejim vurgusu ile yetinmiştir; çerçeve rejim ise ortaya çıkabilecek bütün sorunlara çözüm getirmekten uzaktır. Keza, istihbarat paylaşımı konusunda getirilen çerçeve rejimde "baştan sona güvence" yaklaşımı benimsememiştir.[113]

Milanovic, kararlarla kitlesel gözetimin/kitlesel müdahalelerin normalleştirildiğinden söz etmektedir. Yazar, kararlarda ilgili ükelerde uygulanmakta olan rejimin büyük ölçüde "demokratik toplumda gerekli olma" sınırları içinde kaldığının belirtildiğini; kararların özel hayatın korunması bakımından bir başarı, zafer olarak nitelenemeyeceğini vurgulamaktadır. Keza yazar, özellikle *Big Brother Watch and Others v. Birleşik Krallık* davasında ülke dışılık sorununun ele alınmadığını oysa ki kitlesel müdahalelerin çoğu kez devletlerin ülkeleri dışındaki kişilerin iletişiminden elde edilen verilere ilişkin olduğunu belirtiyor. Yazar, sekiz güvencenin toptan bir orantılılık testine tabi tutulacağına ilişkin paragrafları da eleştiriliyor; bu sayede, bir güvencedeki eksikliğin diğer bir güvence ile kapatılabileceğine ilişkin bir tespitte bulunuyor.[114] Bu görüşte kısmi bir haklılık payı olsa da kararda tam olarak kastedilenin bu olmadığı görüşündeyiz. Kanımızca, kararlarda baştan sona güvenceler öngörülmesi sayesinde ilk aşamadaki eksiklikler sonraki aşamalarda Sekiz Güvencenin sağlanması ve bunların uygulanması ile 8. madde ihlalleri bir ölçüde önlenebilecektir.

Rusinova ise, Mahkemenin kitle iletişimine müdahaleyi teröristlerle ve suçlularla mücadele için toplu gözetim ile rekabet edebilecek bir yöntemin olmadığına ilişkin yaklaşımını eleştiriyor ve bunun tek taraflı bir bakış açısını yansıttığını belirtiyor. Yazar, devletlerin bireylerin verilerinin toplanması ve verilerin analizi konusundaki isteği, iştahı konusunda sessiz kalmasını eleştirmektedir. Yazara göre, 10 yıl evvel büyük verinin depolanması ve işlenmesi bu derece mümkün değilken Mahkeme kararlarında hedefli müdahaleleri ele alıp değerlendirmiş bu kararlarında ise hedefli müdahalelerin kitle

[113] Lubin: s. 606.

[114] Milanovic, Marko: 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rattvisa' (2021) The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa – EJIL: Talk! (ejiltalk.org).

müdahalerine bir alternatif olup olamayacağı konusunda dahi sessiz kalmıştır.[115]

Turanjanin ise, kararlarda kitle iletişiminin gözetimine ilişkin uluslararası alanda basılmış çok sayıdaki eserlerin göz ardı edildiğini belirttikten sonra kararlarda yer alan güvencelerin demokratik toplumun sağlanması için daha da geliştirilmesi gereğine ve bu güvencelerin uygulanması sırasında da bazı sorunların ortaya çıkabileceğine vurgu yapmaktadır.[116]

Massimo, büyük veri çağında ulusal güvenliğin korunması amacıyla yaptığı müdahalelere, saklanması, analiz ve verilerin gözetimi ve metadata konularında üstü kapalı olarak istihbarat servislerine ve hükümetlere gereğinden fazla güvenildiğini vurguluyor. Teknoloji devrimi sonrası ortaya çıkan büyük veri çerçevesinde internette insan haklarının korunması konusunda hedefli gözetim kuralları çerçevesinde hareket edilerek sınırlı bir ilerlemenin sağlandığını belirtiyor. Keza, kitlesel gözetime ilişkin davalarda önemli bir fırsatın kaçırıldığını, gelecekte önüne gelecek davalarda benzeri konuları tekrar ele alacağını ve ilerleyen teknoloji karşısında insan haklarının daha etkin bir biçimde korunmasına yönelik kararların çıkacağını vurguluyor.[117]

SONUÇ

Ele aldığımız davalarda AİHM ilgili ülkelerin kitle gözetim rejimlerinin AİHS'nin 8. ve 10. maddelerine uygunluğunu denetlemiştir. Bu kararların dikkat çeken özelliklerini belli başlıklar altında toplarsak, öncelikle, Mahkeme, davalarda soyut olarak (*in abstantio)* yani herhangi bir somut mağduriyet iddiasında bulunulmadan, başvuruculların iç başvuru

[115] Rusinova, Vera: "European Perspective on Privacy and Mass Surveillance at the Crossroads, Basic Research Program", Working Papers, National Research University Higher School of Economics, Series: LAW WP BRP 87/LAW/ 2019. (https://www.hse.ru/data/2019/03/06/1198896570/87LAW2019.pdf, Erişim: 05.04.2023)

[116] Turanjanin: s.132.

[117] Frigo, Massimo: ''Big Brother Watch v. UK: A Landmark Judgment Missing the Mark', International Commission of Jurists, (Big Brother Watch v. UK: A Landmark Judgment Missing the Mark - Opinio Juris Erişim: 04/06/2021).

yollarını tüketmesini aramadan devletlerin kitle gözetim rejimlerinin, kanunlarının Sözleşmeye uygunluğunu denetlemiştir. Bunun devamında ise, kararlarda kitle iletişiminin gözetimini düzenleyen mevzuatın içermesi gereken minimum güvenceleri belirlemiştir; bunu yaparken önceki bazı kararlarında da ele aldığı üzere "kanunların kalitesi" kavramı üzerinde durmuş, neredeyse davalı devlet yasama organlarına yukarıda belirttiğimiz usule ilişkin bazı minimum güvenceleri dikte etmiştir. Keza, Mahkeme kararlarda 8. maddeye uygunluğu denetlerken sırayla yararlandığı üçlü denetimden bir ölçüde uzaklaşarak "kanunun kalitesi" kavramı ile demokratik devletin gereklerini birlikte değerlendirmiştir.

Mahkeme, kural olarak Sözleşmede yer alan haklarının ihlal edildiğini iddia eden kişi ve kişi gruplarının (mağdurların) başvurularını kabul etmekte; önüne getirilen kanunun Sözleşmeye uygunluğunu soyut olarak denetlememektedir. Söz konusu davalarda ise başvuruculaların *in abstracto* iddiaları ele alındığı için Mahkemenin yaklaşımı diğer davalardan farklı olmuştur. Bunun sebebi hiç kuşkusuz, ele alınan mevzuatın henüz başvuruculara uygulanıp uygulanmadığının bilinmiyor olmasıdır. Uygulama dahi bilinmezken bir mağduriyetin doğup doğmadığını tespit etmek neredeyse imkansızdır. Bu sebeplerle, Mahkemenin iç başvuru yollarını tüketme şartını aramaması devletleri ikincillik ilkesi açısından tedirgin edebilir. 15 nolu Protokolle getirilen ikincillik ilkesinin nedenlerinden biri bu tür kararların engellenmesi iken Mahkeme bu kararlarıyla ikincillik ilkesini kitle gözetimine ilişkin kararlar bakımından bir ölçüde devre dışı bırakmıştır.

Mahkeme önceki kararlarında hedefli gözetimlere ilişkin usulî güvenceleri öngörmüşse de ele aldığımız davalarda kitle iletişiminin gözetimi söz konusu olduğu için eski kararlarıyla bir ölçüde örtüşse de usulî güvenceleri daha da genişleterek yeni bir içtihat yaratma yoluna gitmiştir. Kararlarda kitle gözetimi rejimlerinin içermesi gereken güvenceler ele alınmış ve belirlenmiştir. Davalı devletlerin iletişimin gözetimine ilişkin mevzuatları ele alınarak özellikle 8. maddeye uygunluğun sağlanması için mevzuatın içermesi gereken güvenceler tek tek sayılmıştır. Kararlarda kitle iletişimine müdahale rejimlerinin baştan sona içermesi gereken güvenceler aranmıştır; bunun gerekçesi gözetime ilişkin süreçlerin ilerledikçe daha ağır özel hayat ihlallerinin ortaya çıkabileceği gerçeğidir.

Kararlarda Mahkemenin 8. madde kapsamında yaptığı denetimlerde yararlandığı üçlü denetim yönteminden de bir ölçüde

uzaklaşıldığı görülmektedir. Bu çerçevede, kararlarda demokratik toplum gerekleri koşulu ile kanuna uygunluk koşulunun birlikte değerlendirilmesi dikkat çekmektedir. Başka bir deyişle, kararlarda belirlenen ve açıklanan sekiz usulî güvencenin ilgili kanunlarda bulunması halinde "demokratik toplum gerekleri" koşulu sağlanmış olacaktır. Daha önceki bazı kararlarında da benzeri yöntemi benimseyen Mahkeme ele aldığımız kararlarda özellikle kitle iletişiminin gözetimine ilişkin konularda bu içtihadını geliştirmiştir.

Kararlarda öngörülen sekiz usulî güvence ile kanun yapımında devletin, yasama organlarının takdir marjının bir ölçüde sınırlandığı söylenebilir. Kitlesel gözetimde yürütmenin gücünü kötüye kullanmasını önlemek için kanunlarda bulunması gereken usulî güvencelere ağırlık verilmiştir.

Son olarak, her iki kararda da yer alan en temel paragraflarından birini aşağıda belirtmek istiyoruz.

> "Mahkeme, gizli gözetime izin veren mevzuatın Sözleşmeye aykırılığı iddiasını, müdahalenin hukuka uygun olup olmadığını denetlerken 'kanuna uygun olma' ve 'gereklilik' koşullarının birlikte ele alınmasının uygun olduğuna hükmetmiştir. Bu çerçevede 'kanunun kalitesi' ile yalnızca ilgili kanunların 'erişilebilir ve uygulamasının öngörülebilir olması' aranmamaktadır; bunun yanında gizli gözetim önlemlerinin özellikle kötüye kullanmasının önlenmesi için kanunlarda yeterli, etkin koruma ve garantiler sağlanmalı ve söz konusu önlemler yalnızca 'demokratik bir toplumda gerekli olduğunda' uygulanmalıdır."

Teknoloji geliştikçe insan hakları ile ilişkisinin ve bu konudaki tartışmaların artacağı şimdiden söylebilir. Mahkemenin ileride önüne gelecek teknoloji kullanımına ilişkin benzer davalarda içhihat yaratması, ulusal hukuklar ve Anayasa Mahkemeleri açısından çok değerli olacaktır. Son olarak, bu kararların, ileride daha da tartışmalı hale gelecek bilişim teknolojilerinin istihbarat örgütleri tarafından kullanılması ve insan haklarına etkilerinin düzenleneceği, Avrupa Konseyi bünyesinde yapılacak bir sözleşmeye ön ayak olması çağın gerekleriyle uyumlu olacaktır.

KAYNAKÇA

‘Centrum för Ratvisa v. Sweden’, https://globalfreedomofexpression.columbia.edu/cases/centrum-rattvisa-v-sweden/, erişim tarihi:10.11.2022

Domazet, Siniza/Dinic, Slavica: ‘‘International Legal Aspects of Mass Surveillance and Implications of Privacy’’, Kultura Polisa, C. 19, S. 1, 2022, s. 79-97.

Friedrich, Hannah: ‘‘Protecting Privacy or Enabling Invasion?: Safeguards for Mass Surveillance in Europe’’, Human Rights Brief, C. 25, S. 1, 2021, s. 68-69.

Frigo, Massimo: ‘‘Big Brother Watch v. UK: A Landmark Judgment Missing the Mark’, International Commission of Jurists, (Big Brother Watch v. UK: A Landmark Judgment Missing the Mark - Opinio Juris Erişim: 04/06/2021)

Gerards, Janneke: General Principles of European Court of Human Rights, Cambridge University Press, Cambridge, 2019.

Güzey, Emre: ‘‘AİHM Kararları Çerçevesinde Kitlelerin İstihbarat Maksatlı Gözetimi’’, SAVSAD Savunma ve Savaş Araştırmaları Dergisi, C. 30, S. 2, 2020, s.197-208.

Kaplan, Onur: ““Hukuk Devleti” Bağlamında Kanun Kalitesi, Hukuk ve Adalet Eleştirel Hukuk Dergisi, C. 10, S.23, 2018, s. 83-118.

Kosta, Eleni: ‘‘Algorithmic state surveillance: Challenging the Notion of Agency in Human Rights’’, Regulation & Governance, C.16, S. 1, 2020, s. 212-224.

Lubin, Asaf: ‘‘Introductory Note to Big Brother Watch v. UK (Eur. Ct. H. R. Grand Chamber)’’, International Legal Materials, C. 61, S. 4, 2022, s. 605-653.

Milanovic, Marko: ‘‘Intelligence Sharing in Multinational Military Operations and Complicity under International Law’’, International Law Studies, C. 97, 2021, s. 1269-1403.

Milanovic, Marko: ‘‘The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rattvisa’’ (https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ Erişim: 26/05/2021)

Molu, Benan: ‘‘İHAM Büyük Dairesi’nin Brother Watch v. Birleşik Krallık kararlarının özet çevirisi: Kitlesel dinleme ve iletişim hizmeti sağlayıcılarından iletişim verilerinin alınması rejimi, özel hayatı ve ifade özgürlüğünü ihlal eder.’’,

Anayasa Gündemi, 2021. (https://anayasagundemi.com/2021/06/25/iham-buyuk-dairesinin-big-brother-watch-ve-digerleri-v-birlesik-krallik-kararinin-ozet-cevirisi-kitlesel-dinleme-ve-iletisim-hizmeti-saglayicilarindan-iletisim-verilerinin-alinmasi/ Erişim Tarihi: 25/06/2021)

Rusinova, Vera: "European Perspective on Privacy and Mass Surveillance at the Crossroads, Basic Research Program", Working Papers, National Research University Higher School of Economics, Series: LAW WP BRP 87/LAW/ 2019. (https://www.hse.ru/data/2019/03/06/1198896570/87LAW2019.pdf, Erişim: 05.04.2023)

Sloot, Bart van der/Kosta, Eleni: ''Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance'' European Data Protection Law Review, C. 5, S. 2, 2019, s. 252-261.

Sloot, Bart van der: ''Big Brother Watch and Others v. the United Kingdom & Centrum for Rattvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?'', European Data Protection Law Review, C. 7, S. 2, 2021, s. 319-326.

Sloot, Bart van der: ''The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases'', Journal of Intellectual Property, Information Technology and E-Commerce Law: JIPITEC, C. 11, S. 2, 2020, s. 160-185.

Turanjanin, Veljko: ''When does bulk interception of communications violate the right to privacy? The limits of the state's power and European Court of Human Rights Approach'', International Cybersecurity Law Review, C. 4, S.1, 2023, s.115-136.

Yokuş Sevük, Handan: ''Kolluk Tarafından Suçun Önlenmesine Yönelik Yapılan İletişimin Denetlenmesine İlişkin Değerlendirmeler'', Türkiye Barolar Birliği Dergisi, S.67, 2006, s.41-56.

Zalnieriute, Monika: ''Big Brother Watch and Others v. the UK International Decisions'' American Journal of International Law, C. 116, S. 2, 2022, s.585-592.

AİHM KARARLARI

Berrehab v. Hollanda, BN. 10730/84, 21 Haziran 1988, Series A no. 138.

Big Brother Watch and Others v. the United Kingdom, BN. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

Centrum för Rättvisa v. Sweden, BN. 35252/08 (ECtHR May 25, 2021)

Dragojević v. Hırvatisyan, BN. 68955/11, 15 Ocak 2015.

Dudgeon v. Birleşik Krallık, 22 Ekim 1981, Series A no. 45.

European Court of Human Rights, May 2021, Big Brother Watch and Others v. The UK (GC)-58170/13, 62322/14 and 24960/15, Information Note on the Court's Case-law 251

European Court of Human Rights, May 2021, Centrum för Ratvisa v. Sweden (GC)- 35252/08, Information Note on the Court's Case-law.

Fernández Martínez v. İspanya [BD], BN. 56030/07, 2014.

Halford v. Birleşik Krallık, BN. 22009/93, 25 Haziran 1997.

Hatton ve Diğerleri v. Birleşik Krallık [BD], BN. 36022/97, 2003-VIII.

Huvig v. France, 24 Nisan 1990, Series A no. 176-B.

Kennedy v. Birleşik Krallık, BN. 26839/05, 18 Mayıs 2010.

Klass and Others v. Almanya, BN. 5029/71, 6 Eylül 1978, A 28.

Kruslin v. France, 24 Nisan 1990, Series A no. 176-A.

Mozer v. Moldova Cumhuriyeti ve Rusya [BD], BN. 11138/10, 2016.

Piechowicz v. Polonya, BN. 20071/07, 17 Nisan 2012.

Roman Zakharov v. Rusya, [BD], BN. 47143/06, 2015.

S.A.S. v. Fransa [BD], BN. 43835/11, 1 Temmuz 2014.

Shimovolos v. Rusya, BN. 30194/09, 21 Haziran 2011.

Silver ve Diğerleri v. Birleşik, 25 Mart 1983, Series A no. 61.

Slivenko v. Letonya [BD], BN. 48312/99, 9 Ekim 2003.

Szabó and Vissy v. Macaristan, BN. 37138/14, 12 Ocak 2016

Weber and Saravia v. Almanya , BN.:54934/00, 29 Haziran 2006.

Z v. Finlandiya, BN. 22009/93, 25 Şubat 1997.