Gaziantep Üniversitesi Hukuk Fakültesi Dergisi
Gaziantep University Faculty of Law Journal

E-ISSN: 3023-722X
Yayıncı/Publisher: Gaziantep Üniversitesi

Yıl/ Year: 2 – Sayı/ Volume: 1

Çeviri / Translation

İNSAN HAKLARI AVRUPA MAHKEMESİ GLUKHİN/RUSYA KARARI (BAŞVURU NO: 11519/20), 2023

GLUKHIN/RUSSIA DECISION (APPLICATION NO: 11519/20), 2023 OF EUROPEAN COURT OF HUMAN RİGHTS

Buğra PAKBEŞE[1*]

[1] Araştırma Görevlisi, Gaziantep Üniversitesi Hukuk Fakültesi, İnsan Hakları Hukuku Anabilim Dalı, Gaziantep, Türkiye, av.bugrapakbese@gmail.com.

*Sorumlu Yazar/Corresponding Author

Öz: Rusya Federasyonu aleyhine, İnsan Hakları Avrupa Sözleşmesi'nin 8. ve 10. maddelerinin ihlal edildiği gerekçesiyle Rus vatandaşı olan Bay Nikolay Sergeyevich Glukhin tarafından 31 Ocak 2020 tarihinde İnsan Hakları Avrupa Mahkemesi'ne başvurulmuştur. Mahkeme başvuruyu inceledikten sonra 11519/20 Başvuru Numaralı ve 04 Temmuz 2023 karar tarihli kararında hükümetin yüz tanıma teknolojilerini kullanarak başvuranın Sözleşme'nin 8. ve 10. maddesinde yer alan özel hayata saygı ilkesi ve ifade hürriyetini ihlal ettiğine karar vermiştir.

Anahtar Kelimeler: İnsan Hakları, İnsan Hakları Avrupa Mahkemesi, Yüz Tanıma Teknolojileri, Özel Hayata Saygı İlkesi

Geliş Tarihi/Received: 30.04.2024

Kabul Tarihi/Accepted: 07.06.2024

Yayımlanma Tarihi/ Available Online: 30.06.2024

Abstract: An application was lodged with the European Court of Human Rights on 31 January 2020 by Mr Nikolay Sergeyevich Glukhin, a Russian national, against the Russian Federation alleging violations of Articles 8 and 10 of the European Convention on Human Rights. After examining the application, the Court, in its judgment dated 04 July 2023 and bearing Application No. 11519/20, held that the government had violated the applicant's right to respect for private life and freedom of expression under Articles 8 and 10 of the Convention by using facial recognition technologies.

Keywords: Human Rights, European Court of Human Rights, Facial Recognition Technologies, Right to Private Life.

Atıf/Citation: Pakbeşe, Buğra. "İnsan Hakları Avrupa Mahkemesi Glukhin/Rusya Kararı (Başvuru No: 11519/20), 2023". *Gaziantep Üniversitesi Hukuk Fakültesi Dergisi* 2/1 (Haziran 2024), 59-84.

İNSAN HAKLARI AVRUPA MAHKEMESİ GLUKHIN/RUSYA KARARI

(Başvuru No: 11519/20)

(Karar Tarihi: 04 Temmuz 2023)[*]

İşbu karar, Sözleşme'nin 44 § 2 maddesinde belirtilen koşullar çerçevesinde kesinleşecektir. Bazı şekli düzeltmelere tabi tutulabilir.

Glukhin / Rusya davasında,

İnsan Hakları Avrupa Mahkemesi (Üçüncü Bölüm), aşağıdaki üyelerden oluşan bir Daire olarak görev yapmaktadır:

Pere Pastor Vilanova, *Başkan*,

Jolien Schukking,

Yonko Grozev,

Georgios A. Serghides,

Peeter Roosma,

Andreas Zünd,

Oddný Mjöll Arnardóttir, *yargıçlar*,

ve Milan Blaško, *Bölüm Yazı İşleri Müdürü*,

Aşağıdaki hususları dikkate alarak:

Başvuru (no. 11519/20) Rusya Federasyonu aleyhine, İnsan Hakları ve Temel Özgürlüklerin Korunmasına ilişkin Sözleşme'nin ("Sözleşme") 34. maddesi uyarınca, Rus vatandaşı olan Bay Nikolay Sergeyevich Glukhin ("başvuran") tarafından 31 Ocak 2020 tarihinde Mahkeme'ye sunulmuştur;

Sözleşme'nin 6 § 1 maddesi ile 8. ve 10. maddelerine ilişkin şikâyetlerin Rusya Hükümetine ("Hükümet") bildirilmesine ve başvurunun geri kalanının kabul edilemez ilan edilmesine ilişkin karar;

Davalı Hükümet tarafından sunulan görüşler ve başvuran tarafından sunulan cevap niteliğindeki görüşler;

Bölüm Başkanı tarafından müdahil olmasına izin verilen 19. Madde tarafından sunulan görüşler;

Davalı Hükümetin üçüncü taraf görüşlerine cevaben görüş sunmaması ve Mart 2022'den bu yana davalı Hükümet tarafından herhangi bir bildirimde bulunulmaması;

Bölüm Başkanının, Mahkeme İçtüzüğünün 29 § 2 maddesini kıyasen uygulayarak, Mahkeme'nin görevdeki yargıçlarından birini *ad hoc* yargıç olarak atama kararı (bunun arka planına ilişkin bir açıklama için bkz. *Kutayev v.* Rusya, no. 17912/15, §§ 5-8, 24 Ocak 2023);

[*] İlgili karar İngilizce metin üzerinden çevrilmiştir. İngilizce metin için bkz. https://hudoc.echr.coe.int/tur?i=001-225655.

23 Mayıs ve 13 Haziran 2023 tarihlerinde özel olarak görüştükten sonra,

Son belirtilen tarihte kabul edilen aşağıdaki kararı vermiştir:

GİRİŞ

1. Dava, başvuranın "hızlı bir şekilde (de)monte edilmiş bir nesne" kullanarak tek başına bir gösteri yapma niyetini yetkililere bildirmemesi nedeniyle idari cezaya çarptırılmasıyla ilgilidir. Soruşturma sırasında polis, başvuranın kişisel verilerini işlemek için yüz tanıma teknolojisini kullanmıştır.

OLAYLAR

2. Başvuran 1985 doğumludur ve Moskova'da yaşamaktadır. Moskova'da avukatlık yapan Bay N. Zboroshenko ve Bayan A. Rossius tarafından temsil edilmiştir.
3. Hükümet, başlangıçta Rusya Federasyonu'nun Avrupa İnsan Hakları Mahkemesi nezdindeki eski temsilcisi A. Fedorov ve daha sonra bu görevdeki halefi M. Vinogradov tarafından temsil edilmiştir.
4. Davanın olayları şu şekilde özetlenebilir.
5. Mayıs 2017'de Moskova Belediye Başkanı'nın resmi internet sitesinde Moskova'da 3,500'den fazla CCTV kamerasının kurulduğu bildirilmiştir. Aynı yılın Eylül ayında 3.000'den fazla CCTV kamerası canlı yüz tanıma sistemi (*facial recognition system*) ile donatılmıştır. 2018 baharında Moskova metrosuna yüz tanıma CCTV kameraları yerleştirilmiştir. Moskova Belediye Başkanına göre, canlı yüz tanıma sistemi 2019 yılında test edilmişti. 1 Eylül 2020 itibariyle, -o zamana kadar yaklaşık 175.000 ve 2022'de 220.000'den fazla olmak üzere- Moskova'daki tüm CCTV kameraları canlı yüz tanıma teknolojisi ile donatılmıştır.
6. 12 Ağustos 2019 tarihinde siyasi aktivist olan Bay Konstantin Kotov tutuklanmış ve Rus Ceza Kanunu'nun 212/1 maddesi uyarınca "kamuya açık etkinlikler" ile ilgili kuralları birden fazla kez ihlal etmekle suçlanmıştır. Bay Kotov'un gözaltına alınması ve aleyhindeki cezai kovuşturmalar medyanın ve kamuoyunun büyük ilgisini çekmiş ve halkın tepkisine neden olmuştur.
7. Başvuran, 23 Ağustos 2019 tarihinde, elinde Bay Kotov'un gerçek boyutlu bir karton figürü ve üzerinde şu ifadelerin yer aldığı bir pankartla Moskova metrosunda seyahat etmiştir: "Benimle dalga mı geçiyorsunuz ulan? Ben Konstantin Kotov. Barışçıl protestolar nedeniyle [Madde] 212.1 uyarınca beş yıla kadar [hapis cezasıyla] karşı karşıyayım."
8. 24 Ağustos 2019 tarihli bir polis raporunda, Moskova yeraltı polisinin aşırıcılıkla mücadele birimi ("polis aşırıcılıkla mücadele birimi", "*the police anti-extremism unit*") tarafından yürütülen "internetin izlenmesi" tedbiri sonucunda, bir metro istasyonunda elinde pankart tutan bir insan figürü ile duran bir adamın fotoğrafının ortaya çıktığı anlaşılmaktadır.
9. Daha sonra Polis aşırıcılıkla mücadele birimi, başvuranın bir metro istasyonunda ve bir yeraltı treninin içinde Bay Kotov'un karton figürünü tutarken çekilmiş fotoğraflarını ve bir videosunu içeren herkese açık bir Telegram kanalından ekran görüntüleri almıştır. Paragraf

7'de belirtilen afişte yazılı metin ekran görüntülerinde açıkça okunabilmektedir. Ekran görüntüleri, "İdari Suçlar Kanunu'nun 26. Bölümü uyarınca" ("İSK"; bkz. aşağıdaki 26-27. paragraflar) polis aşırıcılıkla mücadele birimi tarafından basılmış ve saklanmıştır.

10. Polisin 24 Ağustos 2019 tarihli bir başka raporundan, polis aşırıcılıkla mücadele biriminin Chistye Prudy ve Sretenskiy Bulvar metro istasyonlarına yerleştirilen CCTV kameralarından video kayıtları elde ettiği anlaşılmaktadır. Polis aşırıcılıkla mücadele birimi bu kayıtları 27 Ağustos 2019 tarihinde izlemiş, başvuranın görüntüsünün ekran görüntülerini almış, bunların çıktısını almış ve dava dosyasına kaydetmiştir.

11. 26 Ağustos 2019 tarihli polis raporuna göre, polis aşırıcılıkla mücadele birimi, Telegram'da yayınlanan fotoğraf ve videodaki kişinin kimliğini tespit etmek için "operasyonel arama faaliyetleri" yürütmüş, bu kişinin başvuran olduğunu başarıyla tespit etmiş ve ev adresini belirlemiştir.

12. Başvuranın iddiasına göre, 30 Ağustos 2019 tarihinde sabah saat 10 sularında polis aşırıcılıkla mücadele birimi, kendisi evde yokken evine gitmiştir. Başvuran aynı gün saat 11.00 sularında bir metro istasyonunda gözaltına alınmıştır. İddiaya göre polis, başvurana, kendisinin Moskova metrosuna yerleştirilen yüz tanıma CCTV kameraları tarafından tespit edildiğini söylemiştir.

13. Başvuran daha sonra bir polis karakoluna götürülmüş ve burada İSK'nin 20.2 § 5 maddesi uyarınca kamuya açık etkinliklerin yürütülmesi için belirlenen prosedürü ihlal etmekle suçlanmıştır. Suçlamalar, başvuranın 23 Ağustos 2019 tarihinde Chistye Prudy Metro İstasyonu'nda ve metro treninde "hızlı bir şekilde (de)monte edilmiş bir nesne" kullanarak tek başına bir gösteri düzenlediğini ve bunu yapmak için yerel makamlara önceden bildirimde bulunması gerektiğini belirtmiştir.

14. 2 Eylül 2019 tarihli bir mektupta, polis aşırıcılıkla mücadele birimi başkan vekili, Moskova yeraltı güvenlik başkanından, Okruzhnaya Metro İstasyonu'nda kurulu yirmi iki CCTV kamerasından 23 Ağustos 2019 tarihinde saat 8.15 ile 8.35 arasında alınan video kayıtlarının kopyalarını sağlamasını talep etmiştir. Operasyonel Arama Faaliyetleri Yasası'nın (*Operational-Search Activities Act*) 6-3, 7-2(1) ve 15-1. maddelerine (bkz. aşağıdaki 22-23 ve 25. paragraflar) ve Polis Yasası'nın (*Police Act*) 13-1(4). maddesine (bkz. aşağıdaki 29. paragraf) dayanmıştır. Ayrıca, talebin Moskova'da onaylanmış kitlesel halk etkinlikleri sırasında aşırıcılıkla mücadele amacıyla yürütülen bir soruşturma çerçevesinde yapıldığını belirtmiştir. Polisin aşırıcılıkla mücadele birimi, 5 Eylül 2019 tarihinde bu kayıtları izlemiş, başvuranın görüntüsünün ekran görüntülerini almış, bunların çıktısını almış ve dava dosyasında saklamıştır.

15. 23 Eylül 2019 tarihinde, Moskova Meshchanskiy Bölge Mahkemesi tarafından, başvuranın işlediği iddia edilen suçtan suçlu bulunmuştur. Mahkeme, başvuranın sözlü beyanda bulunduğunu ve suçsuz olduğunu iddia ettiğini kaydetmiştir. Ardından, diğerlerinin yanı sıra, Telegram kanalının ekran görüntülerine ve yeraltı güvenlik kameralarından alınan video kayıtlarının ekran görüntülerine dayanarak, başvuranın "hızlı bir şekilde (de)monte edilmiş bir nesne" kullanarak tek başına bir gösteri düzenlediği bulgusunu desteklemiştir. Başvuranın iddiasının aksine, Bay Kotov'un karton figürü "hızlı bir şekilde (de)monte edilmiş bir nesne" olarak kabul edilebilir çünkü bir pervanesi vardır. Mahkeme, başvuranı 20.000 Rus Rublesi ((RUB), yaklaşık 283 Euro) para cezasına çarptırmıştır.

16. Başvuran temyiz yoluna gitmiştir. Başvuran, özellikle, Operasyonel Arama Faaliyetleri Yasası'nın idari suçları soruşturmak için bu tür faaliyetlerin yapılmasına izin vermediğinden kimliğini tespit etmek için yapılan operasyonel arama faaliyetlerinin hukuka aykırı olması nedeniyle şikayetçi olmuştur. Bu nedenle bu şekilde elde edilen deliller kabul edilemez. Ayrıca, dava açan tarafın bulunmamasından dolayı bu durumun tarafsızlık ilkesini ihlal ettiğini iddia etmiştir. Son olarak, tek başına barışçıl bir gösteri yaptığı için mahkûm edilmesinin ifade özgürlüğü hakkını ihlal ettiğini ileri sürmüştür. Gösterinin kamu düzeni veya başkalarının hayatı veya sağlığı için herhangi bir risk oluşturduğu hiçbir zaman iddia edilmemiştir.

17. 30 Ekim 2019 tarihinde Moskova Şehir Mahkemesi, temyiz üzerine, mahkûmiyet kararını onamıştır. Başvuran duruşmaya katılmış ve sözlü beyanlarda bulunmuştur. Mahkeme, gösterinin barışçıl niteliğinin önemsiz olduğunu, çünkü başvuranın kamuya açık etkinliklerin yürütülmesine ilişkin yerleşik prosedürü ihlal etmekten, yani önceden bildirimde bulunmamaktan mahkûm edildiğini tespit etmiştir. Başvuranın karakola götürülmesi ve idari olarak tutuklanması hukuka uygundur. Suç tespit edilmiş ve deliller Polis Kanunu'na uygun olarak polis tarafından toplanmıştır.

İLGİLİ YASAL ÇERÇEVE

I. KAMUYA AÇIK ETKİNLİKLERİN YÜRÜTÜLMESİNE İLİŞKİN PROSEDÜR

18. Kamusal Etkinlikler Yasası (*The Public Events Act,* 19 Haziran 2004 tarihli ve FZ-54 sayılı), göstericinin "hızlı bir şekilde (de)monte edilmiş bir nesne" ("быстровозводимая сборно-разборная конструкция") kullanmayı planladığı durumlar haricinde (bölüm 7(1.1)), tek başına yapılan gösteriler için bildirim gerekmediğini öngörmektedir. Yoldan geçenleri veya trafiği engelleyen böyle bir nesneyi içeren tek başına bir gösterinin bildirimi üç ila dört gün önceden yapılmalıdır (bölüm 7(1)).

19. Yasa tarafından belirlenen süre içinde bildirimde bulunulmaması halinde kamuya açık bir etkinlik düzenlemek yasaktır (bölüm 5(5)).

20. İdari Suçlar Kanunu'nun ("İSK") 20.2 § 5 maddesi, bir katılımcının, herhangi birinin sağlığına veya malına zarar vermeyen kamuya açık etkinliklerin yürütülmesi için belirlenmiş prosedürü ihlal etmesinin 10.000 ila 20.000 RUB para cezası veya kırk saate kadar kamu hizmeti ile cezalandırılmasını öngörmektedir.

II. OPERASYONEL ARAMA FAALİYETLERİ

21. Operasyonel Arama Faaliyetleri Yasası (no. 12 Ağustos 1995 tarihli 144-FZ – "OAFY"), operasyonel arama faaliyetlerinin amaçlarını (a) suçların tespiti, önlenmesi, bastırılması ve soruşturulması ve suç işlemek için komplo kuran, suç işleyen veya işlemiş olan kişilerin kimliklerinin belirlenmesi; (b) adaletten kaçanların ve kayıp kişilerin izinin sürülmesi; (c) Rusya Federasyonu'nun ulusal, askeri, ekonomik veya ekolojik güvenliğini tehlikeye atan olaylar veya faaliyetler hakkında bilgi edinilmesi; ve (d) müsadereye tabi mülkler hakkında bilgi edinilmesi olarak belirlemektedir (OAFY'nin 2. bölümü).

22. Operasyonel arama faaliyetleri sırasında, ilgili kişilerin yaşamına veya sağlığına ya da çevreye zarar vermemek kaydıyla, ses ve görüntü kaydı, fotoğraf, film ve diğer teknik araçlar kullanılabilir (OAFY Bölüm 6-3).

23. Operasyonel arama faaliyetleri, bir suçun işlendiğine, işlenmekte olduğuna veya planlandığına ya da bir suçu işlemek için komplo kuran, işleyen veya işlemiş olan kişiler hakkında bilgi alınmasını takiben, ceza davası açmak için yeterli gerekçe yoksa yürütülebilir (OAFY bölüm 7-2(1)).

24. Anayasa Mahkemesi 14 Temmuz 1998 86-O sayılı kararında, OAFY'nin 7-2(1) bölümünün OAFY'nin 2. bölümüyle birlikte okunması gerektiğine karar vermiştir. Bu nedenle bölüm 7-2(1)'de geçen "suç" terimi "ceza gerektiren suç" anlamına gelecek şekilde yorumlanmalıdır. Operasyonel arama faaliyetleri sırasında soruşturulan suçun ceza gerektiren bir suç olarak sınıflandırılmadığı anlaşılırsa, operasyonel arama faaliyetleri derhal durdurulmalıdır.

25. Operasyonel arama faaliyetleri yürüten birimler belgelere, nesnelere, materyallere ve haberleşmelere el koyabilir (OAFY'nin 15-1. bölümü).

III. İDARİ CEZA DAVALARINDA DELİL TOPLANMASI

26. İSK'nin 26. Bölümüne göre, belgeler, fotoğraflar, ses ve görüntü kayıtları, veri tabanları ve diğer veri türleri, davayla ilgili bilgiler içeriyorsa, idari ceza davalarında delil olarak kullanılabilir. Davadan sorumlu kişi ister hâkim ister başka bir görevli olsun, dava sonuçlanana kadar delilleri korumak için gerekli tüm adımları atmalı ve daha sonra akıbeti hakkında bir karar vermelidir (Madde 26.7).

27. Bir idari ceza davasına bakan hâkim veya başka bir resmi görevli, davayı çözmek için gerekli her türlü bilgiyi talep edebilir. Bu bilgiler, talebin alınmasından itibaren üç gün içinde sunulmalıdır. Bilgi sağlanamazsa, kurum talepte bulunan hâkim veya diğer yetkiliyi üç gün içinde yazılı olarak bilgilendirmelidir (Madde 26.10).

IV. POLİSİN YETKİLERİ

28. Polis Kanunu (07 Şubat 2011 tarihli ve 3-FZ sayılı) polisin yetkisi dahilindeki idari suçları tespit etmek, bastırmak ve soruşturmak için tedbirler almasını öngörmektedir (bölüm 12-1(11)). Ayrıca aşırılık yanlısı faaliyetleri önlemek, ortaya çıkarmak ve bastırmak için de tedbirler almalıdır (bölüm 12-1(16)).

29. Polis, cezai veya idari suçları soruştururken ya da cezai veya idari suçlar veya kazalarla ilgili kayıtlı şikayetleri incelerken, federal yasanın özel bir erişim prosedürü belirlediği bilgiler hariç olmak üzere, Devlet ve belediye makamlarından, kamu derneklerinden, kuruluşlarından, yetkililerinden ve vatandaşlardan, kişisel veriler de dâhil olmak üzere, bilgi, belge veya bunların kopyalarını veya diğer gerekli verileri gerekçeli olarak talep etme ve ücretsiz olarak alma hakkına sahiptir (madde 13-1(4)).

V. KİŞİSEL VERİLERİN İŞLENMESİ

30. Kişisel Verilerin Korunması Kanunu (*The Personal Data Protection Act*, 27 Temmuz 2006 tarihli ve 152-FZ sayılı, söz konusu tarihte yürürlükte olan), kişisel verilerin, diğerlerinin yanı sıra, bir kişinin idari adli işlemlere dâhil olmasıyla bağlantılı olarak ve ayrıca kişisel verilerin bu verilerin öznesi tarafından kamuya açık hale getirilmesi durumunda işlenebileceğini öngörmektedir (madde 6(1)(3) ve (10)).

31. Biyometrik kişisel veriler, bir kişiyi tanımlamak için kullanılabilecek fizyolojik ve biyolojik özelliklerini ortaya koyan bilgiler olarak tanımlanmıştır. Bu veriler, söz konusu bölümde aksi belirtilmedikçe, yalnızca ilgili bireyin yazılı rızası ile işlenebilir (bölüm 11(1)). Biyometrik kişisel veriler, diğer durumların yanı sıra, adaletin idaresi ile bağlantılı olarak ve savunma, güvenlik, terörle mücadele, ulaşım güvenliği, yolsuzlukla mücadele ve operasyonel arama faaliyetleri ile ilgili mevzuatta öngörülen durumlarda veri sahibinin rızası olmaksızın işlenebilir (bölüm 11(2)).

32. Irk, milliyet, siyasi görüş, dini veya felsefi inanç, sağlık durumu veya mahrem hayatı ortaya koyan özel kategorilerdeki kişisel verilerin işlenmesi, söz konusu bölüm tarafından izin verilen haller dışında, genel olarak yasaklanmıştır (bölüm 10(1)). Özel kategorilerdeki kişisel veriler, diğerlerinin aksine, bu verilerin öznesi tarafından kamuya açıklanmış olması halinde; adaletin idaresi ile bağlantılı olarak ve savunma, güvenlik, terörle mücadele, ulaşım güvenliği, yolsuzlukla mücadele, operasyonel arama faaliyetleri ve sivil ve cezai adli yaptırımlara ilişkin mevzuatta öngörülen durumlarda işlenebilmektedir (bölüm 10(2)(2), (6) ve (7)).

VI. MOSKOVA YERALTINDA VİDEO GÖZETİMİ

33. Söz konusu tarihte yürürlükte olan, ulaşım güvenliği gerekliliklerine ilişkin 5 Nisan 2017 tarihli ve 410 sayılı Hükümet Kararnamesi, güvenlik profillerine bağlı olarak metro istasyonlarına teknik ekipman yerleştirilmesi gerekliliğini öngörmektedir. Özellikle, birinci kategorideki (en yüksek güvenlik) yeraltı istasyonlarının, ulaşım güvenliğini sağlayan sistemlerle donatılması gerekmektedir:

- güvenlik bölgesinin ve alt bölgelerinin sınırlarındaki kontrol noktalarında ve yeraltının işleyişi için gerekli olan kısımlarda hedef kişilerin ve araçların video-gözetim sistemleri tarafından tespit edilmesi;

- sınırsız erişimli alt bölgeler, biletli erişimli alt bölgeler ve yeraltının işleyişi için gerekli olan kısımları dâhil olmak üzere yeraltının içinde herhangi bir zamanda ve yerde video-gözetim sistemleri tarafından hedef olayların tespit edilmesi ve tanımlanması;

- yeraltının "sadece personel için" alt bölgelerinde herhangi bir zamanda ve yerde video-gözetim sistemleri tarafından hedef kişilerin ve araçların tespit edilmesi;

- hedef kişilerin ve araçların güvenlik bölgesinin çevresinde belirli bir zamanda ve yerde video-gözetim sistemleri tarafından tespit edilmesi;

- verilerin gerçek zamanlı iletimi;

- verilerin elektronik cihazlarda en az otuz gün süreyle saklanması;

- güvenlik bölgesinin çevresindeki kontrol noktalarının dışında ve yeraltının işleyişi için gerekli kısımlarında yeraltına girmeye çalışan bir suçlunun gerçek zamanlı tespiti;

- biletle girilen alt bölgelerin, "sadece personel için" alt bölgelerin sınırlarını geçen ve yeraltının işleyişi için gerekli kısımlarına erişen personel ve yolcular hakkındaki verilerin kaydedilmesi ve gerçek zamanlı olarak iletilmesi (Madde 6 § 1).

34. Federal Güvenlik Servisi, polis ve Federal Ulaşım Denetleme Servisi'nin yetkili kurumları, ulaşım güvenlik sistemleri tarafından elde edilen verilere erişim hakkına sahip olacaktır (Madde § 5 (10)).

İLGİLİ ULUSLARARASI KAYNAKLAR

I. BİRLEŞMİŞ MİLLETLER

35. Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği'nin 24 Haziran 2020 tarihli "Barışçıl protestolar da dâhil olmak üzere toplantı ve gösteri yürüyüşleri bağlamında yeni teknolojilerin insan haklarının geliştirilmesi ve korunması üzerindeki etkisi" başlıklı raporunun (UN Doc. A/HRC/44/24) ilgili bölümleri aşağıdaki gibidir (dipnotlar çıkarılmıştır):

> "33. Toplantılar bağlamında kişilerin kimliklerini tespit etmek için yüz tanıma teknolojisinin kullanılması, etkili güvenceler olmadığı takdirde, özel hayatın gizliliği, ifade özgürlüğü ve barışçıl toplanma hakları üzerinde önemli olumsuz etkilere sahiptir. Bir kişinin görüntüsü, onu diğer kişilerden ayıran benzersiz özellikleri ortaya çıkardığı için kişiliğinin temel niteliklerinden birini oluşturur. Bir kişinin rızası olmaksızın yüz görüntülerinin kaydedilmesi, analiz edilmesi ve saklanması, kişinin özel hayatının gizliliği hakkına müdahale teşkil eder. Toplantılarda yüz tanıma teknolojisinin kullanılmasıyla, bu müdahaleler kitlesel ve ayrım gözetmeyen bir ölçekte gerçekleşir, çünkü bu, yüz tanıma teknolojisi sistemi ile donatılmış veya bu sisteme bağlı kamera tarafından yakalanan tüm kişilerin yüz görüntülerinin toplanmasını ve işlenmesini gerektirir.
>
> 34. Toplantılar geleneksel olarak katılımcılara tekilleştirilmeye veya teşhis edilmeye karşı belirli bir düzeyde koruma sağlamıştır. Bu koruma, toplantı katılımcılarının rutin olarak görsel-işitsel kayıtlarını yapan birçok Devlet tarafından zaten önemli ölçüde zayıflatılmıştır. Yüz tanıma teknolojisinin yükselişi, görsel-işitsel kayıt uygulamalarına kıyasla bir paradigma değişikliğine yol açmıştır; zira bu teknoloji, bir toplantıdaki tüm veya birçok katılımcıyı otomatik bir şekilde tanımlama kapasitesini önemli ölçüde artırmaktadır. Bu durum özellikle canlı yüz tanıma teknolojisi kullanıldığında, gerçek zamanlı tanımlamanın yanı sıra katılımcıların hedefli gözetim ve takibine de izin verdiğinden sorun yaratmaktadır. Hatalı canlı kimlik tespiti, güvenlik güçlerinin barışçıl toplantılara usulsüz müdahalelerine de yol açabilir. Birleşmiş Milletler insan hakları uzmanlarının da belirttiği gibi, yüz tanıma teknolojisinin barışçıl toplanma hakkı üzerindeki olumsuz etkileri geniş kapsamlı olabilir. Kimliklerinin tespit edilip olumsuz sonuçlara maruz kalabileceklerinden korkan pek çok kişi kamuya açık alanlarda gösteri yapmaktan ve görüşlerini özgürce ifade etmekten çekinmektedir.
>
> 35. Görsel-işitsel kayıt ve yüz tanıma teknikleri yalnızca bu tür tedbirlerin yasallık, gereklilik ve orantılılık olmak üzere üç bölümden oluşan testi karşılaması halinde kullanılmalıdır. Barışçıl protestolar sırasında yüz tanıma teknolojisine başvurulmasının, müdahaleciliği ve ciddi caydırıcı etkileri göz önüne alındığında, gereklilik ve orantılılık testini karşılama olasılığı sorgulanmaktadır. Yetkililer genel olarak gösteriye katılanları kaydetmekten kaçınmalıdır. Orantılılık gerekliliğinin bir gereği olarak, istisnalar sadece ciddi suçların işlendiğine dair somut göstergeler olduğunda ya da şiddet veya ateşli silah kullanımı gibi yakın ve ciddi suç teşkil eden davranışlardan şüphelenmek için bir neden olduğunda değerlendirilmelidir. Mevcut kayıtlar sadece ciddi suç şüphelisi olan toplantı katılımcılarının tespiti için kullanılmalıdır.
>
> 36. Yüz tanıma teknolojisinin barışçıl toplantılar bağlamında kullanılması tavsiye edilmemekle birlikte, bu teknolojiyi kullanmaya devam eden hükümetler, bunu etkin bir şekilde çalışan insan haklarına uygun bir düzenleyici çerçeve de dâhil olmak üzere açık bir yasal zeminde yaptıklarından emin olmalıdır. Buna ek olarak, görsel-işitsel kayıt ve yüz tanıma tekniklerini kullanmaya devam eden yetkililer, yüz görüntüleri ve bunlardan elde edilen veriler de dâhil olmak üzere kişisel verileri etkili bir şekilde

koruyan hükümler içeren bir düzenleyici çerçeveyi uygulamaya koymalıdır. Tedbirler, cezai soruşturmaların yürütülmesi ve şiddet içeren suçların kovuşturulması için gerekli olabilecek belirli bölümler hariç olmak üzere, tüm verilerin derhal silinmesini sağlamalıdır. İlgili tüm kişiler, meşru bir amaç ve yasal bir dayanak olmaksızın saklanan bu tür bilgilere, bu verilerin gerekli olduğu cezai soruşturmaları veya kovuşturmaları engelleyeceği durumlar haricinde, erişme ve bu bilgilerin düzeltilmesini ve silinmesini talep etme hakkına sahip olmalıdır.

37. Bunun yanında, görsel-işitsel kayıt ve yüz tanıma teknolojisinin her türlü kullanımı etkin bir şekilde çalışan ve iyi kaynaklara sahip gözetim mekanizmalarına tabi olmalıdır. Gözetimin bir kısmı bağımsız ve tarafsız veri koruma makamları tarafından gerçekleştirilebilirken, Devletler, yüz tanıma teknolojisi önlemlerinin bir montaj bağlamında kullanılmasına izin vermekten sorumlu, tercihen adli nitelikte bağımsız bir organın katılımı da dâhil olmak üzere ek önlemleri değerlendirmelidir. Her durumda, kayıt ve yüz tanıma teknolojisinin her türlü kullanımı yargı denetimine açık olmalıdır. Her koşulda, yetkililer kayıt ve yüz tanıma teknolojisinin kullanımı konusunda şeffaf olmalı ve halkı, kayıt altına alındıklarında veya alınabileceklerinde ve/veya görüntüleri bir yüz tanıma sisteminde işlenebileceğinde her zaman bilgilendirmelidir.

…

53. Bu bağlamda, Yüksek Komiser Devletlere şu tavsiyelerde bulunur:

…

(h) Devletler, bir toplantıya barışçıl bir şekilde katılanları tespit etmek için asla yüz tanıma teknolojisini kullanmamalıdır;

(i) Katılımcıların ciddi suç faaliyetlerinde bulunduklarına veya bulunacaklarına dair somut belirtiler olmadıkça ve bu tür kayıtlar gerekli sağlam güvencelerle birlikte kanunla sağlanmadıkça, toplantı katılımcılarının görüntülerini kaydetmekten kaçınmalıdır;"

II. AVRUPA KONSEYİ

36. Bakanlar Komitesi'nin polis teşkilatında kişisel verilerin kullanımını düzenleyen R (87) 15 sayılı Tavsiye Kararı (17 Eylül 1987 tarihinde kabul edilmiştir), *diğer hususların yanı sıra*, aşağıdaki hususları belirtmektedir:

"İlke 2- Verilerin toplanması

2.1. Kişisel verilerin polis amaçları doğrultusunda toplanması, gerçek bir tehlikenin önlenmesi veya belirli bir suçun bastırılması için gerekli olanlarla sınırlı olmalıdır. Bu hükme getirilecek her türlü istisna, özel ulusal mevzuatın konusu olmalıdır.

...

2.4. Bireyler hakkında yalnızca belirli bir ırksal kökene, belirli dini inançlara, cinsel davranışlara veya siyasi görüşlere sahip oldukları ya da yasalarca yasaklanmamış belirli hareketlere veya örgütlere mensup oldukları gerekçesiyle veri toplanması yasaklanmalıdır. Bu faktörlere ilişkin verilerin toplanması ancak belirli bir soruşturmanın amaçları doğrultusunda kesinlikle gerekli olması halinde gerçekleştirilebilir."

37. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme'nin (ETS 108) Danışma Komitesi tarafından hazırlanan Yüz Tanıma Kılavuz İlkeleri (2021) aşağıdaki gibidir (dipnotlar çıkarılmıştır):

"Yüz tanıma, bireylerin yüzlerini içeren dijital görüntülerin, yüz şablonları kullanılarak bu bireylerin tanımlanması veya doğrulanması amacıyla otomatik olarak işlenmesidir. Biyometrik nitelikteki bilgilerin hassasiyeti, çağdaşlaştırılmış Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (bundan böyle "108+ sayılı Sözleşme" olarak anılacaktır) 6. maddesinde özel veri kategorileri kapsamına bir kişiyi benzersiz şekilde tanımlayan verilerin dâhil edilmesiyle açıkça kabul edilmiştir. Görüntülerin işlenmesinin bağlamı verilerin hassas niteliğinin belirlenmesi ile ilgilidir; çünkü görüntülerin işlenmesinin tamamı hassas verilerin işlenmesini

içermemektedir. Görüntüler yalnızca bir bireyin benzersiz bir şekilde tanımlanmasına veya kimlik doğrulamasına izin veren belirli bir teknik araçla işlendiğinde biyometrik veri tanımı kapsamına girecektir. Bu kılavuz ilkeler, canlı yüz tanıma teknolojileri de dâhil olmak üzere yüz tanıma teknolojilerinin kullanımını kapsamaktadır. ...

Yüz tanıma teknolojilerinin mevcut gözetim sistemlerine entegre edilmesi, bu teknolojilerin kullanımı her zaman biyometrik verileri bu şekilde işlenen bireylerin farkındalığını veya iş birliğini gerektirmediğinden, özel hayatın gizliliği ve kişisel verilerin korunması haklarının yanı sıra diğer temel haklar açısından da ciddi bir risk oluşturmaktadır. Örneğin, bireylerin dijital görüntülerine internet üzerinden erişme imkânı için durum böyledir. Bu tür ihlalleri önlemek amacıyla, 108+ sayılı Sözleşme'nin tarafları, yüz tanıma teknolojilerinin geliştirilmesi ve kullanımında özel hayatın gizliliği ve kişisel verilerin korunması haklarına saygı gösterilmesini sağlayacak ve böylece Sözleşme'de yer alan ilkeleri yüz tanıma teknolojileri özelinde uygulayarak insan hakları ve temel özgürlükleri güçlendirecektir.

…

Kanunilik

108+ sayılı Sözleşme'nin 6. maddesinde öngörüldüğü üzere, biyometrik veriler gibi özel kategorilerdeki verilerin işlenmesine ancak söz konusu işlemenin uygun bir yasal temele dayanması ve tamamlayıcı ve uygun güvencelerin iç hukukta yer alması halinde izin verilir. Bu güvenceler, ilgili risklere ve korunacak menfaatlere, haklara ve özgürlüklere uyarlanmalıdır. Bazı mevzuatlarda, bu tür işlemlerin yasaklanması bir kuraldır ve uygulanmasına yalnızca istisnai olarak, belirli özel durumlarda (örneğin, bireylerin açık rızası ile, hayati çıkarlarını korumak için veya işlemenin ağır basan kamu yararı nedenleriyle gerekli olduğu durumlarda) ve ilgili risklere uygun güvencelere tabi olarak izin verilir. Yüz tanıma teknolojilerinin kullanımının gerekliliği, amaçla orantılılık ve veri sahiplerinin hakları üzerindeki etki ile birlikte değerlendirilmelidir. Farklı kullanım durumları kategorize edilmeli ve yüz tanıma yoluyla biyometrik verilerin işlenmesine uygulanabilir bir yasal çerçeve mevcut olmalıdır. Bu yasal çerçeve, her bir farklı kullanım için özellikle aşağıdakileri ele almalıdır:

- özel kullanım ve öngörülen amaca ilişkin ayrıntılı bir açıklama;
- kullanılan algoritmanın asgari güvenilirliği ve doğruluğu;
- kullanılan fotoğrafların saklama süresi;
- bu kriterlerin denetlenebilme imkânı;
- sürecin izlenebilirliği;
- güvenlik önlemleri.

…

Belirli kullanımların kanunla kesin olarak sınırlandırılması

Yüz tanımanın müdahalecilik düzeyi ve buna bağlı olarak mahremiyet ve veri koruma haklarının ihlali özel kullanıma göre değişecektir ve iç hukukun, demokratik süreç yoluyla bu karara varıldığı durumlarda kullanımını katı bir şekilde sınırlayacağı veya hatta tamamen yasaklayacağı durumlar olacaktır. Canlı yüz tanıma teknolojilerinin kontrolsüz ortamlarda [kontrolsüz ortam kavramı, alışveriş merkezleri, hastaneler veya okullar gibi kamusal ve yarı kamusal alanlar da dâhil olmak üzere bireylerin serbestçe erişebildiği ve içinden geçebildiği yerleri kapsamaktadır] kullanımı, özel hayatın gizliliği ve bireylerin onuru üzerindeki müdahaleciliği ve diğer insan hakları ve temel özgürlükler üzerindeki olumsuz etki riski ışığında, demokratik bir tartışmaya ve tam bir analiz yapılana kadar bir askıya alma (*moratorium*) olasılığına tabi olmalıdır.

…

Dijital görüntülerin yüz tanıma teknolojilerine entegre edilmesi

Yasa koyucular ve karar alıcılar, dijital formatta mevcut görüntülerin, bu görüntüler başlangıçta başka amaçlarla (örneğin sosyal medyadan) çekilmişse, yeni işleme için belirli bir yasal dayanak olmaksızın

biyometrik şablonları çıkarmak veya biyometrik sistemlere entegre etmek için işlenememesini sağlamalıdır. Dijital görüntülerden biyometrik şablonların çıkarılması hassas verilerin işlenmesini içerdiğinden, aşağıda ele alınan ve farklı sektörlere ve kullanımlara göre değişen olası yasal dayanağın sağlanması gerekmektedir. Özellikle, sosyal medya veya çevrimiçi fotoğraf yönetimi web siteleri de dâhil olmak üzere internete yüklenen veya video gözetim kameraları tarafından çekilen dijital görüntülerin kullanılması, yalnızca kişisel verilerin veri sahipleri tarafından açıkça erişilebilir hale getirilmiş olması temelinde yasal kabul edilemez.

…

Yüz tanıma teknolojilerinin kamu sektöründe kullanımı

İlgili kişiler ile bu makamlar arasındaki güç dengesizliği göz önünde bulundurulduğunda, kamu makamları tarafından gerçekleştirilen yüz tanıma işlemleri için kullanılan yasal zemin kural olarak rıza olmamalıdır.

...

Yasa koyucular ve karar alıcılar, kolluk kuvvetleri amacıyla yüz tanıma teknolojilerinin kullanıldığı biyometrik işlemler için belirli kurallar koymalıdır. Bu kurallar, bu tür kullanımların kesinlikle gerekli ve bu amaçlarla orantılı olmasını sağlayacak ve sağlanması gereken güvenceleri belirleyecektir.

Kolluk kuvvetleri

Kontrollü veya kontrolsüz bir ortamda kimlik belirleme amacıyla yüz tanıma teknolojileri kullanılarak biyometrik veri işleme genel olarak kolluk kuvvetleri amaçlarıyla sınırlandırılmalıdır. Bu işlem yalnızca güvenlik alanında yetkili makamlar tarafından gerçekleştirilmelidir.

Yasalar, temel haklara yönelik potansiyel riskleri dikkate alarak ve bireylerin görüntüleri yasal olarak toplandığı sürece, amacın doğrulama veya kimlik tespiti olmasına bağlı olarak farklı gereklilik ve orantılılık testleri öngörebilir.

Kimlik tespiti amacıyla, hem veri tabanının (izleme listesi) oluşturulmasında hem de (canlı) yüz tanıma teknolojilerinin kontrolsüz bir ortamda kullanılmasında katı gereklilik ve orantılılık gözetilmelidir.

Yasalar, kolluk kuvvetlerinin belirli, meşru ve açık kolluk kuvveti amaçları (örneğin, ağır suç şüphesi veya kamu güvenliği riski) için veri tabanları (izleme listeleri) oluştururken uyması gereken açık parametreler ve kriterler sağlamalıdır.

Bu teknolojilerin müdahaleciliği göz önünde bulundurularak, canlı yüz tanıma teknolojilerinin kontrolsüz ortamlarda konuşlandırılması aşamasında, kanun uygulayıcı makamların bu teknolojilerin konuşlandırılacağı yer ve zamanlama da dâhil olmak üzere çeşitli faktörlerin kullanımların kesin gerekliliğini ve orantılılığını haklı çıkardığını göstermesini sağlamalıdır.

…”

III. AVRUPA BİRLİĞİ

38. Suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı ile ilgili 27 Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi (AB):

“Madde 10 Özel nitelikli kişisel verilerin işlenmesi

Irk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları veya sendika üyeliğini ortaya koyan kişisel verilerin işlenmesine ve genetik verilerin, gerçek bir kişiyi benzersiz bir şekilde tanımlamak amacıyla biyometrik verilerin, sağlıkla ilgili verilerin veya gerçek bir kişinin cinsel yaşamı veya cinsel yönelimi ile ilgili verilerin işlenmesine, yalnızca veri sahibinin hakları ve özgürlükleri için uygun güvencelere tabi olarak kesinlikle gerekli olduğu durumlarda ve yalnızca aşağıdaki hususların gerçekleşmesi halinde izin verilir:

(a) Birlik veya Üye Devlet hukuku tarafından yetkilendirildiği hallerde;

(b) veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için; veya

(c) söz konusu işlemenin veri sahibi tarafından açıkça kamuya açıklanan verilerle ilgili olduğu hallerde."

39. Avrupa Veri Koruma Kurulu'nun 26 Nisan 2023 tarihli kolluk kuvvetleri alanında yüz tanıma teknolojisinin kullanımına ilişkin 05/2022 sayılı Kılavuz İlkeleri aşağıdaki gibidir (dipnotlar çıkarılmıştır):

"36. Biyometrik verilerin her koşulda işlenmesi başlı başına ciddi bir müdahale teşkil eder. Bu, örneğin pozitif eşleşme gibi bir sonuca bağlı değildir. İşleme, biyometrik şablonun polis veritabanında eşleşme sonucu olumsuz çıktıktan hemen sonra silinse bile bir müdahale oluşturur...

43. Şart'ın 52(1) maddesi belirli bir yasal dayanak şartı getirmektedir. Bu yasal dayanak, vatandaşlara, yetkililerin veri toplama ve gizli izleme tedbirlerine başvurma yetkisine sahip olduğu koşullar ve durumlar hakkında yeterli bir fikir verecek şekilde yeterince açık olmalıdır. Demokratik bir toplumda hukukun üstünlüğü çerçevesinde bireylere hak ettikleri asgari koruma derecesini sağlamak için kamu makamlarına verilen ilgili takdir yetkisinin kapsamını ve kullanılma şeklini makul bir açıklıkla belirtmelidir. Ayrıca, kanunilik, özellikle bireyin Şart'ın 8. maddesi kapsamındaki haklarına saygı gösterilmesini sağlamak için yeterli güvenceler gerektirir. Bu ilkeler, YTT [yüz tanıma teknolojisi] sistemlerinin değerlendirilmesi, eğitimi ve daha da geliştirilmesi amacıyla kişisel verilerin işlenmesi için de geçerlidir.

44. Gerçek kişiyi benzersiz olarak tanımlama amacıyla işlenen biyometrik verilerin, LED Madde 10'da (yukarıda 38. paragrafta atıfta bulunulan Veri Koruma Kolluk Kuvvetleri Direktifi) listelenen özel veri kategorilerini oluşturduğu göz önüne alındığında, YTT'nin farklı uygulamaları çoğu durumda, uygulamayı ve kullanım koşullarını açıkça tanımlayan özel bir yasa gerektirecektir. Bu, özellikle suç türlerini ve uygulanabilir olduğu hallerde, diğer hususların yanı sıra, küçük suçları etkin bir şekilde hariç tutmak amacıyla, bu suçların uygun ağırlık eşiğini kapsar ...

51. Avrupa Birliği Adalet Divanı'nın (ABAD) yerleşik içtihadına göre, kişisel verilerin korunmasına ilişkin istisnalar ve sınırlamalar yalnızca kesinlikle gerekli olduğu ölçüde uygulanmalıdır. Bu aynı zamanda, amaca ulaşmak için daha az müdahaleci araçların mevcut olmadığı anlamına gelir. Verilen amaca bağlı olarak ek personel, daha sık polis kontrolü veya ek sokak aydınlatması gibi olası alternatifler dikkatlice belirlenmeli ve değerlendirilmelidir. Yasama tedbirleri, örneğin ciddi suçlarla mücadele gibi amaçlar ışığında, kapsadığı kişileri ayırt etmeli ve belirlemelidir. Böyle bir farklılaştırma, sınırlama veya istisna olmaksızın tüm kişileri genel bir şekilde kapsıyorsa, müdahaleyi yoğunlaştırır. Veri işlemenin nüfusun önemli bir bölümünü kapsaması da müdahaleyi yoğunlaştırır.

52. Şart'ın 8(1) maddesinde yer alan açık yükümlülükten kaynaklanan kişisel verilerin korunması, Şart'ın 7. maddesinde yer alan özel hayata saygı hakkı açısından özellikle önemlidir. Mevzuat, söz konusu tedbirin kapsamını ve uygulanmasını düzenleyen açık ve kesin kurallar koymalı ve verileri işlenen kişilerin kişisel verilerini istismar riskine ve bu verilere yasadışı erişim veya kullanımına karşı etkili bir şekilde korumak için yeterli güvencelere sahip olmalarını sağlayacak güvenceler öngörmelidir. Bu tür güvencelere duyulan ihtiyaç, kişisel verilerin otomatik işlemeye tabi olduğu ve verilere yasa dışı erişim riskinin önemli olduğu durumlarda daha da artmaktadır. Ayrıca, YTT'nin kullanılmasına ilişkin dâhili veya harici -örneğin adli-yetkilendirme de güvence olarak katkıda bulunabilir ve ciddi müdahalelerin söz konusu olduğu bazı durumlarda gerekli olabilir.

53. Belirlenen kurallar, örneğin işlenen veri miktarı, verilerin niteliği ve verilere yasadışı erişim riski gibi özel durumlara uyarlanmalıdır. Bu durum, özellikle söz konusu verilerin bütünlüğünü ve gizliliğini sağlamak amacıyla bunların korunmasını ve güvenliğini açık ve katı bir şekilde düzenlemeye hizmet edecek kurallar gerektirmektedir.

54. Kontrolör ve işleyici arasındaki ilişkiye yönelik, işleyicilerin kişisel verilere uyguladıkları güvenlik düzeyini belirlerken sadece ekonomik mülahazaları dikkate almalarına izin verilmemelidir; bu durum yeterli düzeyde yüksek korumayı tehlikeye atabilir.

55. Bir kanun, yetkili makamların verilere erişiminin ve bunların daha sonra kullanımının sınırlarını belirlemek için maddi ve usule ilişkin koşullar ve objektif kriterler ortaya koymalıdır. Önleme, tespit veya cezai kovuşturma amacıyla, ilgili suçların, örneğin Şart'ın 7. ve 8. maddelerinde yer alan temel haklara yapılan bu müdahalelerin kapsamını ve ciddiyetini haklı çıkaracak kadar ciddi kabul edilmesi gerekir.

56. Veriler, özellikle de koruma ve güvenlik gerekliliklerine uygunluğun bağımsız bir makamın denetimine tabi olacağını belirten Şart'ın 8. maddesinde öngörülenler, AB veri koruma kurallarının uygulanabilirliğini ve etkisini sağlayacak şekilde işlenmelidir. Böyle bir durumda, işlemenin gerçekleştiği coğrafi yer önemli olabilir.

57. Kişisel verilerin işlenmesinin farklı aşamaları ile ilgili olarak, izlenen amacın amaçları için olası yararlılıkları temelinde veya ilgili kişilere göre veri kategorileri arasında bir ayrım yapılmalıdır. İşleme koşullarının belirlenmesi, örneğin saklama süresinin belirlenmesi, müdahalenin kesinlikle gerekli olanla sınırlı olmasını sağlamak için objektif kriterlere dayanmalıdır.

58. Her duruma göre, gereklilik ve orantılılık değerlendirmesinde, Şart'ın 1. maddesi kapsamındaki insan onuru, Şart'ın 10. maddesi kapsamındaki düşünce, vicdan ve din özgürlüğü, Şart'ın 11. maddesi kapsamındaki ifade özgürlüğü ve Şart'ın 12. maddesi kapsamındaki toplanma ve örgütlenme özgürlüğü gibi diğer temel hakların kapsamına giren tüm sonuçlar belirlenmeli ve dikkate alınmalıdır.

59. Ayrıca, verilerin veri sahiplerinin bilgisi olmaksızın sistematik olarak işlenmesi halinde, genel bir sürekli gözetim anlayışının ortaya çıkmasının muhtemel olduğu ciddi bir husus olarak değerlendirilmelidir. Bu durum, ilgili temel hakların bir kısmı veya tamamı bakımından caydırıcı etkilere yol açabilir ...

73. İşleme faaliyeti kişisel verilerin korunmasına yönelik müdahale ve kısıtlamaların mutlak gereklilikle sınırlı olması halinde ancak "kesinlikle gerekli" olarak kabul edilebilir. "Kesinlikle" teriminin eklenmesi, yasa koyucunun özel kategorilerdeki verilerin işlenmesinin yalnızca gereklilik koşullarından daha katı koşullar altında gerçekleşmesini amaçladığı anlamına gelmektedir. Bu gereklilik vazgeçilmez olarak yorumlanmalıdır. Bu, gereklilik testinde kolluk kuvvetlerine tanınan takdir marjını mutlak bir minimumla sınırlandırmaktadır. ABAD'ın yerleşik içtihadına uygun olarak, "kesin gereklilik" şartı, işleme faaliyetinin gerçekleştirilebileceği durum ve koşulları tanımlamak için objektif kriterlerin gerekliliği ile de yakından bağlantılıdır, böylece genel veya sistematik nitelikteki herhangi bir işleme faaliyeti hariç tutulur ...

104. Yüz tanıma teknolojilerinin kullanımı, özel veri kategorileri de dâhil olmak üzere önemli miktarda kişisel verinin işlenmesiyle özünde bağlantılıdır. Yüz ve daha genel olarak biyometrik veriler, bir kişinin kimliğiyle kalıcı ve geri alınamaz bir şekilde bağlantılıdır. Bu nedenle, yüz tanımanın kullanımı, AB Temel Haklar Şartında yer alan ve gizlilik ve veri korumanın ötesine geçebilen insan onuru, hareket özgürlüğü, toplanma özgürlüğü ve diğerleri gibi bir dizi temel hak ve özgürlük üzerinde doğrudan veya dolaylı etkiye sahiptir. Bu durum özellikle kolluk kuvvetleri ve ceza adaleti alanında geçerlidir.

105. Avrupa Veri Koruma Kurulu ("EDPB"), kolluk kuvvetlerinin terör eylemleri ve diğer ciddi suçların faillerini hızlı bir şekilde tespit etmek için mümkün olan en iyi araçlardan yararlanma ihtiyacını anlamaktadır. Ancak, bu tür araçlar yürürlükteki yasal çerçeveye sıkı sıkıya bağlı kalınarak ve sadece Şart'ın 52(1) maddesinde belirtildiği üzere gereklilik ve orantılılık gerekliliklerini karşıladıkları durumlarda kullanılmalıdır. Ayrıca, modern teknolojiler çözümün bir parçası olabilirken, hiçbir şekilde "sihirli değnek" değildir.

106. Yüz tanıma teknolojilerinin bireyler ve toplum için kabul edilemez derecede yüksek riskler ("kırmızı çizgiler") oluşturan belirli kullanım durumları vardır. Bu nedenlerle EDPB ve Avrupa Veri Koruma Denetçisi ("EDPS") bunların genel olarak yasaklanması çağrısında bulunmuştur.

107. Özellikle, kamuya açık alanlarda bireylerin uzaktan biyometrik olarak tanımlanması, bireylerin özel hayatlarına müdahale açısından yüksek risk teşkil etmektedir ve doğası gereği kitlesel gözetimi gerektirdiğinden demokratik bir toplumda yeri yoktur. Aynı şekilde EDPB, bireyleri biyometrik özelliklerine göre etnik köken, cinsiyet, siyasi veya cinsel yönelimlerine göre kümelere ayıran yapay zekâ destekli yüz tanıma sistemlerinin de Şart ile uyumlu olmadığını düşünmektedir. Ayrıca EDPB, gerçek kişinin duygularını tespit edebilmek için yüz tanıma veya benzer teknolojilerin kullanılmasının

son derece istenmeyen bir durum olduğuna ve muhtemelen usulüne uygun olarak gerekçelendirilmiş birkaç istisna dışında yasaklanması gerektiğine inanmaktadır. Buna ek olarak EDPB, kişisel verilerin kitlesel ölçekte ve gelişigüzel bir şekilde toplanmasıyla oluşturulan veri tabanına dayanan kolluk kuvveti uygulaması bağlamında kişisel verilerin işlenmesinin, örneğin çevrimiçi olarak erişilebilen fotoğrafların ve yüz resimlerinin, özellikle de sosyal ağlar aracılığıyla erişilebilir olanların "kazınması" yoluyla, Birlik hukuku tarafından öngörülen katı gereklilik şartını karşılamayacağı görüşündedir."

IV. DİĞER İLGİLİ BULGULAR

40. Bağımsız bir insan hakları medya projesi olan OVD-Info tarafından hazırlanan 17 Ocak 2022 tarihli "Rus devleti protestoculara karşı kameraları nasıl kullanıyor" başlıklı raporun ilgili bölümleri aşağıdaki gibidir:

"Protestocuların olay bittikten sonra gözaltına alınması ya da bizim deyimimizle "*post factum* gözaltılar" 2021'den önce de gerçekleşmiştir. OVD-Info 2018'de Rusya'nın 39 bölgesinde bu tür 219 vaka tespit etti; bunlar çoğunlukla münferit nitelikteydi: bir olayla bağlantılı olarak bir veya iki kişi gözaltına alındı, istisnai durumlarda gözaltına alınanların sayısı ona ulaştı. 2020'de yaygın olarak kullanılmaya başlandı ...

Olay sonrası (*post factum*) gözaltıların sayısındaki artışın, sosyal ağları izleme ve yüz tanıma teknolojilerinin gelişmesine dayandığına inanıyoruz ...

Raporumuz, toplanma özgürlüğünü kısıtlamak için yüz tanıma sistemlerinin kullanımına ayrılmıştır. Araştırmamız Moskova'ya odaklanmış olsa da, verilerimize göre bu olgunun coğrafyası başkentin çok ötesine geçmektedir ...

Yüz tanıma teknolojisinin kullanımı, her şeyden önce, geniş çaplı gözaltılar ve kamuya mal olmamış kişilerin yargılanması ve polis memurlarının sözleri ile kanıtlanmaktadır ...

Protestocuları tespit etmek için yüz tanıma sisteminin kullanılması Ocak 2021 protestolarından sonra medyada geniş yer bulmuş olsa da bu teknolojiden resmi belgelerde nadiren bahsedilmektedir ...

Polis raporlarında, dava dosyalarında ve mahkeme kararlarında yüz tanıma teknolojisinin kullanımına ilişkin doğrudan kanıtların azlığı, polisin ve mahkemelerin bu bilgileri resmi olarak belgelememeyi tercih ettiğini gösteriyor olabilir. Bununla birlikte, bazı belgelerde teknolojinin kullanımına dair dolaylı işaretler bulunmaktadır ...

Polisin protesto olaylarına katıldığından şüphelendiği kişiler işyerinde gözaltına alınmış, üniversite derslerinden çıkarılmış, bir kişi okulda dersten alınmıştır. Kafelerde, sokakta, metroda, tren peronunda ve trende gözaltı vakaları yaşanmıştır...

Peronlarda, kafelerde ve kiralık dairelerde yapılan gözaltılar, protestolara katılanlara karşı şehirdeki hareket takip sistemlerinin kullanıldığına işaret ediyor olabilir. Konut girişlerindeki CCTV kayıtları bu arama için kullanılabilir ...

Bir kişiye karşı işlenen bir suçla ilgili rapor, kişinin bir olayda gözaltına alınmasıyla değil de olaydan sonra düzenlenmişse, bu genellikle kişinin kimliğinin olay yerinde tespit edilmediği anlamına gelir ...Bu nedenle, kolluk kuvvetlerinin videoda yakalanan kişi ile izinsiz bir etkinliğe katıldığı için sorumlu tutmaya çalıştıkları kişi arasındaki kimlik karşılaştırmasının arkasındaki süreci açıklamaları gerekir. Mevcut materyalleri inceleyen OVD-Info, polisin bunu yapmasının iki ana yolu olduğu sonucuna varmıştır:

1. Kişilerin kimlik tespitinin "operasyonel arama faaliyetleri" sırasında gerçekleştiğine dair bir gösterge;

2. Bir polis memurunun daha fazla açıklama yapmadan fotoğraf ve videolarda belirli bir vatandaşı "tespit ettiklerini" belirttikleri bir rapor.

Bu vakaların hiçbirinde polis, yüz tanıma teknolojisinin bir kişinin kimliğini belirlemek için herhangi bir şekilde kullanıldığını "kâğıt üzerinde" kabul etmemektedir. Kolluk kuvvetlerinin, Rus mevzuatının

"gri bölgesinde" yer aldığı için yüz tanıma teknolojisinin kullanımını belgelememeyi tercih ediyor olması mümkündür...

Aynı zamanda, bu tür vakalarda soruşturma faaliyetlerine atıfta bulunulmamakta ve belirli bir kişinin kimliğinin tam olarak nasıl tespit edilebildiği sorusuna da cevap verilmemektedir ...

Protestocuların kimliklerini tespit etmek için güvenlik kameralarından alınan kayıtlar ..., kolluk kuvvetleri tarafından sahada yapılan kayıtlar, internetten alınan fotoğraflar ve videolar (Telegram kanalları, sohbetler, sosyal ağlardaki kişisel sayfalar, YouTube) kullanılmıştır.

Kameraların -örneğin konutların girişlerine veya metroya yerleştirilmiş- bir kişinin idari olarak sorumlu tutulması adına yerini belirlemek için de kullanıldığı durumlar mevcuttur.

Kimlik tespiti için polis, belgelerdeki (iç ve dış pasaportlar, sosyal kartlar) ve sosyal ağlardaki fotoğrafları içeren veri tabanlarını kullanmaktadır ...

Protestolara katılım nedeniyle açılan davalar, gecikmeli olarak, olay sırasında gözaltına alınmaya kıyasla ek zorluklarla ve büyük olumsuz sonuçlarla ilişkilidir. Diğer şeylerin yanı sıra, mahremiyetin ciddi bir şekilde ihlal edilmesi ve insan hayatının diğer alanlarının etkilenmesiyle ilgilidir.

Olay sonrası gözaltı uygulamasında açık bir cezalandırma eğilimi vardır ve toplantıların potansiyel katılımcıları üzerinde korkutucu ve marjinalleştirici bir etkisi bulunmaktadır. İdari Suçlar Kanunu'nun 20.2. maddesinde yer alan en yaygın "miting" suçunun zaman aşımı süresinin bir yıla çıkarıldığı göz önünde bulundurulduğunda, protesto katılımcıları uzun süre olası bir gözaltı için beklemektedir. Olaydan altı aydan fazla bir süre sonra tutanak tutulduğu bilinen vakalar vardır. Son olarak, post factum idari sorumluluk, kolluk kuvvetlerine duruşma zamanlarını manipüle etme fırsatı vererek, ağır yaptırımlarla dolu "tekrarlanan" ve "çoklu" ihlal suçlamalarının (İdari Suçlar Kanunu madde 20.2 Bölüm 8 ve Ceza Kanunu madde 212.1) kullanılmasına zemin oluşturmaktadır ...

Bazı durumlarda mahkemeler, kamu menfaatlerinin korunması bahanesiyle göstericilerin yüz tanıma yöntemiyle tespit edilmesini onaylamaktadır. Öte yandan, bu teknolojinin diğer birçok suç türü için (yanlış yerde karşıdan karşıya geçmek veya kaçak yolcu gibi) kitlesel olarak kullanılmaması, asıl amacın kamu çıkarlarını korumak değil, yetkililerin siyasi muhaliflerine zulmetmek olduğunu göstermektedir.

Protestoları sınırlandırmak için yüz tanıma sisteminin kullanılması için gerekli altyapının oluşturulması ve işleyişi (sokak fotoğrafçılığı ve video kaydı, alınan verilerin depolanması, kişisel kimlik bilgileriyle fotoğrafların veri tabanlarının oluşturulması), polis memurlarının veri tabanlarına erişimi, kişisel verilerin korunması ile ilgili bir dizi konu yeterince düzenlenmemiştir. Kullanımın şeffaf olmaması ve kamu denetiminin eksikliği ile birlikte, bu teknolojinin siyasi amaçlı bir zulüm aracına dönüşmesi mümkündür."

HUKUK

I. YARGI YETKİSİ VE DAVALI HÜKÜMET İLE YAZIŞMALAR

41. Mahkeme, Sözleşme'nin iddia edilen ihlallerine yol açan olayların, Rusya Federasyonu'nun Sözleşme'ye Taraf olmaktan çıktığı tarih olan 16 Eylül 2022'den önce meydana geldiğini gözlemlemektedir. Bu nedenle Mahkeme, mevcut başvuruyu inceleme yetkisine sahip olduğuna karar vermiştir (bkz. *Fedotova ve Diğerleri / Rusya [BD],* no. 40792/10 ve 2 diğerleri, §§ 68-73, 17 Ocak 2023).

42. Mahkeme'nin Sözleşme'nin 58. maddesi uyarınca devam eden yargı yetkisi göz önünde bulundurulduğunda, özellikle 38, 41 ve 46. maddeler ile Mahkeme İç Tüzüğü'nün ilgili hükümleri 16 Eylül 2022 tarihinden sonra da uygulanmaya devam edecektir. Davalı Hükümet'in yargılamalara daha fazla katılmaktan kaçınması, onları Mahkeme ile iş birliği yapma yükümlülüğünden kurtarmaz ve Mahkeme'nin yargı yetkisini sürdürdüğü başvuruları incelemeye devam etmesini engellemez (bkz. *Ukrayna ve Hollanda / Rusya ((dec.) [GC*], no.

8019/16 ve 2 diğerleri, §§ 435-39, 30 Kasım 2022, ve *Svetova ve Diğerleri / Rusya*, no. 54714/17, §§ 29-31, 24 Ocak 2023). Mahkeme, bir tarafın yargılamalara etkin bir şekilde katılmaması veya katılmayı reddetmesinden uygun gördüğü çıkarımları yapabilir (Mahkeme İçtüzüğü'nün 44C maddesi).

43. Mahkeme, Rusya Federasyonu yetkilileriyle iletişim aracı olarak ve önündeki yargılamanın çekişmeli yapısına saygı göstermek amacıyla elektronik güvenlikli Hükümet web sitesini kullanmaya devam ettiğini gözlemlemektedir (Mahkeme Başkanı tarafından 22 Eylül 2008 tarihinde Mahkeme İçtüzüğü'nün 32. maddesi uyarınca yayınlanan ve 29 Eylül 2014 ve 5 Temmuz 2018 tarihlerinde değiştirilen Hükümetler tarafından güvenli elektronik dosyalamaya ilişkin Uygulama Talimatına bakınız). Site güvenli ve davalı Devlet yetkilileri tarafından erişilebilir olmaya devam etmektedir.

II. İÇ HUKUK YOLLARININ TÜKETİLMESİ

44. Hükümet, *Chigirinova / Rusya* ((dec.), no. 28448/16, 13 Aralık 2016) kararına dayanarak, başvuranın Yüksek Mahkeme'ye temyiz başvurusunda bulunmadığı için iç hukuk yollarını tüketmediğini ileri sürmüştür.

45. Mahkeme, Chigirinova'nın (yukarıda atıfta bulunulan) İdari Yargılama Usulü Kanunu kapsamındaki yargılamalarla ilgili olduğunu, mevcut davanın ise İdari Suçlar Kanunu ("İSK") kapsamındaki yargılamalarla ilgili olduğunu belirtmektedir. İSK'de öngörülen inceleme/temyiz prosedürü, tüketilmesi gereken etkili bir hukuk yolu değildir (bkz. *Smadikov / Rusya (dec.)*, no. 10810/15, § 49, 31 Ocak 2017, ve *Ecodefence ve Diğerleri / Rusya*, no. 9988/13 ve 60 diğerleri, § 75, 14 Haziran 2022).

46. Dolayısıyla, Hükümet'in iç hukuk yollarının tüketilmediğine ilişkin itirazı reddedilmelidir.

III. SÖZLEŞME'NİN 10. MADDESİNİN İHLAL EDİLDİĞİ İDDİASI

47. Başvuran, kendisine karşı yürütülen idari ceza yargılamasının Sözleşme'nin 10. ve 11. maddeleri kapsamındaki haklarını ihlal ettiğinden şikayetçi olmuştur. Mahkeme, 11. madde bağlamında ortaya konan genel ilkeleri dikkate alarak, bu şikâyeti Sözleşme'nin 10. maddesi kapsamında inceleyecektir (bkz. *Novikova ve Diğerleri / Rusya*, no. 25501/07 ve 4 diğerleri, § 91, 26 Nisan 2016). Sözleşme'nin 10. maddesi aşağıdaki gibidir:

> "1. Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar. Bu madde, Devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine tabi tutmalarına engel değildir.
>
> 2. Görev ve sorumluluklar da yükleyen bu özgürlüklerin kullanılması, yasayla öngörülen ve demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir."

A. Kabul Edilebilirlik

48. Mahkeme, bu şikâyetin açıkça dayanaktan yoksun olmadığını veya Sözleşme'nin 35. maddesinde belirtilen diğer gerekçelerden dolayı kabul edilemez olmadığını kaydeder. Bu nedenle kabul edilebilir ilan edilmelidir.

B. Esaslar

49. Başvuran, tek başına yaptığı gösteri için önceden bildirimde bulunmaması nedeniyle mahkûm edilmesinin hukuka aykırı olduğunu ileri sürmüştür. Bay Kotov'un karton figürü tek bir karton parçasından oluşmaktaydı ve bu nedenle "hızlı bir şekilde (de)monte edilmiş bir nesne" olarak kabul edilemezdi; bu nedenle, solo gösterisini yetkililere bildirmesi gerekmiyordu. Her durumda, yürürlükteki yasal hükümler "hukukun niteliği" şartını karşılamıyordu. Ayrıca, yerel makamlar başvuranın barışçıl tek başına yaptığı gösteriye karşı sıfır tolerans göstermiştir. Gösteriden birkaç gün sonra tutuklanması, herhangi bir acil toplumsal ihtiyaçla gerekçelendirilmemiştir. Yerel makamlar, bireysel gösterinin yarattığı risklere ilişkin herhangi bir değerlendirme yapmamış veya tutuklanmasının ve mahkûm edilmesinin gerekli olup olmadığını doğrulamamıştır.

50. Hükümet, iç hukukun kamuya açık etkinliklerin önceden bildirilmesini gerektirdiğini ileri sürmüştür. Başvuran, bu gerekliliğe uymadığı için yasal olarak mahkûm edilmiştir. Polis karakoluna götürülmesi ve tutuklanması da hukuka uygun olmuştur.

51. Mahkeme, 10. maddenin korumasının sözlü veya yazılı sözlerle sınırlı olmadığını, fikir ve görüşlerin sözlü olmayan ifade araçlarıyla veya bir kişinin davranışlarıyla da iletilebileceğini yineler (bkz. *Karuyev / Rusya,* no. 4161/13, § 18, 18 Ocak 2022). Başvuranın davranışının niteliği ve bağlamı göz önünde bulundurulduğunda, Mahkeme, başvuranın eylemleriyle, 10 § 2 maddesi kapsamında kısıtlamalar için çok az kapsam bulunan, kamu yararına ilişkin bir konuda görüşlerini ifade etmeye çalıştığı kanaatindedir.

52. Başvuranın polis karakoluna götürülmesi, idari olarak tutuklanması ve idari bir suçtan mahkûm edilmesi, ifade özgürlüğü hakkına bir müdahale teşkil etmiştir (bkz. *Novikova ve Diğerleri,* yukarıda anılan § 106).

53. İlgili genel ilkeler *Novikova ve Diğerleri* (yukarıda anılan, §§ 190-201) ve *Kudrevičius ve Diğerleri/Litvanya* ([GC], no. 37553/05, §§ 108-10, 150-51 ve 155, İHAM 2015) kararlarında özetlenmiştir.

54. "Kanunla öngörülme" kriterine ilişkin olarak, "hızlı bir şekilde (de)monte edilen nesneler" hükmü, bir kişinin ne tür nesnelerin bu hükmün kapsamına girebileceğini öngörmesine olanak tanıyan hiçbir kriter içermemektedir. Başvuranın tek başına yaptığı gösterinin niteliği göz önünde bulundurulduğunda ve ilgili hükümlerin kapsamı ve uygulanma şekline ilişkin olarak yüksek Rus mahkemeleri tarafından daha fazla açıklama yapılmadığı veya başvuranın özel davasında yerel mahkemeler tarafından ayrıntılı bir analiz yapılmadığı göz önünde bulundurulduğunda, Mahkeme, itiraz edilen yasal hükümlerin uygulanma şeklinin söz konusu davadaki nitelik şartını karşılamak için yeterince öngörülebilir olduğundan şüphe etmek için nedenler olduğunu tespit etmiştir (bkz. *Navalnyy / Rusya* [BD], no. 29580/12 ve 4 diğerleri, § 118, 15 Kasım 2018).

55. Bununla birlikte, müdahalenin hukuka uygun olduğu ve "düzensizliğin önlenmesi" ile "başkalarının haklarının korunması" meşru amaçlarını güttüğü varsayılsa bile, aşağıdaki nedenden dolayı "demokratik bir toplumda gerekli" değildir.

56. Başvuranın tek başına yaptığı gösteri, tartışmasız bir şekilde barışçıl ve yıkıcı olmayan bir şekilde gerçekleştirilmiştir. Başvuranın mahkûm edildiği suç, yalnızca tek başına yaptığı gösteriyi yetkililere bildirmemekten ibarettir ve trafiğin engellenmesi, mala zarar verilmesi veya şiddet eylemleri gibi kınanacak herhangi bir eylemle ilgili suçlayıcı başka bir unsur içermemektedir (yukarıda anılan *Kudrevičius ve Diğerleri*, §§ 164-75). Başvuranın eylemlerinin, olağan yaşamda ve diğer faaliyetlerde normal veya kaçınılmaz olanı aşan ölçüde büyük bir aksamaya neden olduğu tespit edilmemiştir. Eylemlerinin kamu düzeni veya ulaşım güvenliği için herhangi bir tehlike arz ettiği de iddia edilmemiştir. Bununla birlikte, yetkililer, başvuranın barışçıl bireysel gösterisine karşı gerekli hoşgörü derecesini göstermemiştir. Yukarıda belirtilen ilgili unsurları dikkate almamışlar ve başvuranın elinde pankart tutan karton bir figür kullanmasının görüşlerinin bir ifadesi olup olmadığını değerlendirmemişlerdir. Konuyla ilgili tek değerlendirme, yasa dışı davranışların cezalandırılması ihtiyacı olmuştur. Bu bağlamda, Sözleşme'nin 10. maddesi açısından, herhangi bir ağırlaştırıcı unsurun bulunmaması yeterli bir değerlendirme değildir (bkz. *Novikova ve Diğerleri*, yukarıda anılan, § 199). Dolayısıyla, mahkemeler, başvuranın ifade özgürlüğü hakkına yapılan müdahaleyi haklı çıkarmak için ilgili ve yeterli gerekçeler sunamamıştır.

57. Dolayısıyla, Sözleşme'nin 10. maddesi ihlal edilmiştir.

IV. SÖZLEŞME'NİN 8. MADDESİNİN İHLAL EDİLDİĞİ İDDİASI

58. Başvuran, yüz tanıma teknolojisinin kullanımı da dâhil olmak üzere, idari suç işlemleri çerçevesinde kişisel verilerinin işlenmesinin özel hayatına saygı hakkını ihlal ettiğinden şikayetçi olmuştur. Başvuran, Sözleşme'nin aşağıda belirtilen 8. maddesine dayanmıştır:

> "1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
>
> 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli tedbir olması durumunda söz konusu olabilir."

A. Kabul Edilebilirlik

59. Mahkeme, bu şikâyetin açıkça dayanaktan yoksun olmadığını veya Sözleşme'nin 35. maddesinde belirtilen diğer gerekçelerden dolayı kabul edilemez olmadığını kaydeder. Bu nedenle kabul edilebilir ilan edilmelidir.

B. Esas

1. Tarafların beyanları Tarafların beyanları

60. Başvuran, Moskova metrosuna yerleştirilen CCTV kameraları tarafından filme alındığını, yüz tanıma teknolojisi ile tespit edildiğini ve daha sonra bu şekilde elde edilen kanıtlara dayanarak

idari bir suçtan mahkûm edildiğini ileri sürmüştür. Kendisine ait video görüntülerinin toplanması, saklanması ve kullanılmasına izin veren herhangi bir yargı kararı bulunmamaktadır. Polis Kanunu ve Kararnamesi no. 410 sayılı Kararname, müdahalenin yasal dayanağı olarak "kanun kalitesi" şartını karşılamamıştır. İlgili düzenlemeler çok muğlaktı ve ne önceden bir yargı izni ne de sonradan herhangi bir yargı denetimi öngörüyordu.

61. Başvuran ayrıca, özel hayatına saygı gösterilmesi hakkına yapılan müdahalenin herhangi bir meşru amaç gütmediğini ve "demokratik bir toplumda gerekli" olmadığını ileri sürmüştür. Başvuranın özel hayatına sadece barışçıl bir gösteri düzenlediği için müdahale edilmiştir.

62. Hükümet, başvuranın idari bir suç işlediğini ve polis tarafından kendisine karşı alınan tüm tedbirlerin yasal ve haklı olduğunu ileri sürmüştür. Başvuranın adı herhangi bir aranan kişiler listesinde yer almamaktadır. Başvurana karşı alınan tedbirlerin yasal bir dayanağı vardır (bkz. yukarıdaki 33-34. paragraflarda atıfta bulunulan mevzuatın özeti).

63. Üçüncü taraf müdahil Madde 19'un, yüz tanıma teknolojisinin azami dikkatle kullanılması ve yeterli yasal güvencelerle desteklenmesi gerektiğini ileri sürmüştür. Özellikle yüz tanıma teknolojisinin kullanıldığı biyometrik kitlesel gözetimin, dijital çağda temel haklara yönelik en büyük tehditlerden birini temsil ettiğini savunmuştur. Bu durum, mahremiyet ve anonimlik hakkını tehdit etmekte ve ifade ve toplanma özgürlüğü hakları üzerinde güçlü bir caydırıcı etkiye sahiptir. İnsanların izlendikleri ve takip edildikleri bilinci, insanları protesto haklarını kullanmaktan ve kamusal alanlarda fikirlerini özgürce ifade etmekten caydırabilir.

2. Mahkeme'nin değerlendirmesi

(a) Bir müdahalenin varlığı

(i) Genel ilkeler

64. Mahkeme, "özel hayat" kavramının kapsamlı bir tanıma elverişli olmayan geniş bir terim olduğunu yineler. Bu kavram, kişinin fiziksel ve sosyal kimliğinin birçok yönünü kapsayabilir. Bireyin dışarıdan müdahale olmaksızın kendi kişisel hayatını yaşayabileceği bir "yakın çevre" ile sınırlı olmayıp, aynı zamanda "özel bir sosyal yaşam" sürme hakkını, yani başkalarıyla ve dış dünyayla ilişki kurma ve geliştirme imkanını da kapsar. Kamusal bağlamda gerçekleşen faaliyetleri dışlamaz. Dolayısıyla, kamusal bağlamda bile olsa, bir kişinin başkalarıyla "özel yaşam" kapsamına girebilecek bir etkileşim alanı vardır (bkz. *López Ribalda ve Diğerleri/İspanya* [BD], no. 1874/13 ve 8567/13, §§ 87-88, 17 Ekim 2019).

65. Bir bireyin özel hayatına ilişkin verilerin yalnızca saklanması, 8. madde anlamında bir müdahale teşkil etmektedir. Saklanan bilgilerin daha sonra kullanılmasının bu bulgu üzerinde hiçbir etkisi yoktur. Bununla birlikte, yetkililer tarafından saklanan kişisel bilgilerin yukarıda belirtilen özel hayata ilişkin hususlardan herhangi birini içerip içermediğini belirlerken Mahkeme, söz konusu bilgilerin kaydedildiği ve saklandığı özel bağlamı, kayıtların niteliğini, bu kayıtların kullanılma ve işlenme şeklini ve elde edilebilecek sonuçları dikkate alacaktır (bkz. *S. ve Marper/Birleşik Krallık* [BD], no. 30562/04 ve 30566/04, § 67, AİHM 2008).

66. İnsanların bilerek veya isteyerek kamuya açık bir şekilde kaydedilen, rapor edilen veya edilebilecek faaliyetlere dâhil oldukları durumlar olduğundan, bir kişinin mahremiyete ilişkin makul beklentileri bu değerlendirmede kesin olmasa da önemli bir faktör olabilir. Bir bireyin eylemlerinin fotoğraf veya video cihazları kullanılarak izlenmesine ilişkin olarak, Sözleşme

kurumları, bir bireyin kamuya açık bir yerdeki eylem ve hareketlerinin görsel verileri kaydetmeyen bir kamera kullanılarak izlenmesinin kendi başına özel hayata müdahale teşkil etmediği görüşünü benimsemiştir. Bununla birlikte, bu tür kişisel verilerin, özellikle de kimliği belirlenmiş bir kişinin resimlerinin sistematik veya kalıcı bir kaydı ortaya çıktığında, özel hayata ilişkin hususlar ortaya çıkabilir. Bir kişinin görüntüsü, kişinin benzersiz özelliklerini ortaya koyduğu ve kişiyi benzerlerinden ayırdığı için kişiliğinin başlıca niteliklerinden birini oluşturur. Dolayısıyla, her bir kişinin imajını koruma hakkı, kişisel gelişimin temel bileşenlerinden biridir ve bu imajın kullanımını kontrol etme hakkını gerektirir. Çoğu durumda, bu tür bir kullanımı kontrol etme hakkı, bireyin görüntüsünün yayınlanmasını reddetme olasılığını içermekle birlikte, bireyin görüntüsünün başka bir kişi tarafından kaydedilmesine, muhafaza edilmesine ve çoğaltılmasına itiraz etme hakkını da kapsar (bkz. López Ribalda ve Diğerleri, yukarıda anılan, § 89, daha fazla referansla birlikte).

67. Mahkeme daha önce, yetkililer tarafından belirli kişiler hakkında veri toplanmasının ve depolanmasının, bu veriler yalnızca kişinin kamusal faaliyetleriyle ilgili olsa bile, örneğin hükümet karşıtı gösterilere katılım (bkz. *Association "21 December 1989" and Others/Romania*, no. 33810/07 ve 18817/08, § 170, 24 Mayıs 2011, ve *Catt/Birleşik Krallık,* no. 43514/15, § 93, 24 Ocak 2019), bu kişilerin özel hayatlarına müdahale teşkil ettiğine karar vermiştir (bkz. *Amann/İsviçre* [BD], no. 27798/95, §§ 65-67, AİHM 2000-II, ve *Rotaru/Romanya* [BD], no. 28341/95, §§ 43-44, AİHM 2000-V). Mahkeme ayrıca, kamuya açık bir yerde veri toplanmasına ilişkin aşağıdaki örneklerin kişilerin özel hayatlarına müdahale teşkil ettiğini tespit etmiştir: bir polis karakolunun kamuya açık bir alanında bir sorgunun kaydedilmesi (*P.G. ve J.H. / Birleşik Krallık,* no. 44787/98, §§ 56-60, AİHM 2001-IX); halka açık bir yerde CCTV kameraları tarafından kayıt yapılması ve daha sonra video görüntülerinin medyaya ifşa edilmesi (bkz. *Peck/Birleşik Krallık*, no. 44647/98, §§ 57-63, AİHM 2003-I); bir polis karakolunda video görüntülerinin kaydedilmesi ve daha sonra ceza yargılamalarında kullanılması (bkz. *Birleşik Krallık*, no. 63737/00, §§ 36-43, AİHM 2003-IX (alıntılar); bir kişinin arabasına takılan GPS cihazı aracılığıyla o kişinin kamusal alanda bulunduğu yer ve hareketlerine ilişkin verilerin toplanması ve depolanması (bkz. 35623/05, §§ 51-53, AİHM 2010 (alıntılar), ve *Ben Faiza/Fransa*, no. 31446/12, §§ 53-55, 8 Şubat 2018); bir kişinin adının, o kişinin tren veya hava yoluyla yaptığı hareketlere ilişkin bilgileri otomatik olarak toplayan ve işleyen bir polis veri tabanına kaydedilmesi (bkz. *Shimovolos/Rusya*, no. 30194/09, § 66, 21 Haziran 2011); ve bir devlet üniversitesindeki üniversite amfitiyatrolarının video ile gözetlenmesi (bkz. *Antović ve Mirković/Karadağ*, no. 70838/13, §§ 40-45 ve 55, 28 Kasım 2017).

(ii) Mevcut davaya uygulanması

68. Mevcut davada, internetin rutin olarak izlenmesi sırasında polis, başvuranın herkese açık bir Telegram kanalında yayınlanan tek başına bir gösteri düzenlerken çekilmiş fotoğraflarını ve bir videosunu keşfetmiştir. Polis, Telegram kanalının ekran görüntülerini almış, bunları saklamış ve iddiaya göre başvuranın kimliğini tespit etmek için bunlara yüz tanıma teknolojisi uygulamıştır. Videodaki yerin Moskova metrosunun istasyonlarından biri olduğunu tespit eden polis, bu istasyonda ve başvuranın geçiş yaptığı diğer iki istasyonda bulunan CCTV güvenlik kameralarından da video kayıtları toplamıştır. Bu video kayıtlarının ekran görüntülerini almışlar ve bunları saklamışlardır. Ayrıca, iddiaya göre, Moskova metrosuna yerleştirilen canlı yüz tanıma CCTV kameralarını, birkaç gün sonra başvuranı idari bir suçla

suçlamak amacıyla yerini tespit etmek ve tutuklamak için kullanmışlardır. Telegram kanalının ve CCTV güvenlik kameralarından alınan video kayıtlarının ekran görüntüleri daha sonra başvuran aleyhindeki idari suç yargılamalarında delil olarak kullanılmıştır (bkz. yukarıdaki 7-15. paragraflar).

69. Hükümet, yukarıda açıklanan olgusal koşulların, başvuranın Sözleşme'nin 8. maddesi kapsamındaki özel hayatına saygı gösterilmesi hakkına bir "müdahale" teşkil ettiğine itiraz etmemiştir. Özellikle, Mahkeme'nin konuyla ilgili özel sorusuna rağmen, başvuranın yüz tanıma teknolojisinin, ilk olarak, Telegram'da yayınlanan fotoğraflardan ve videodan kimliğini tespit etmek ve ikinci olarak, Moskova metrosunda seyahat ederken yerini tespit etmek ve tutuklamak için kullanıldığına dair iddiaları hakkında yorum yapmamıştır. Mahkeme, başvuranın iddialarını kanıtlamakta karşılaştığı zorlukların farkındadır. Gerçekten de Mahkeme'nin elindeki iç mevzuat, polisin yüz tanıma teknolojisini kullanırken bir kayıt tutmasını ya da ilgili kişiye otomatik olarak ya da talep üzerine böyle bir kayda erişim hakkı vermesini gerektirmemektedir (bkz. herhangi bir resmi kayıt tutmadan yüz tanıma teknolojisini kullanma uygulamasını anlatan yukarıdaki 40. paragraf).

70. Başvuranın kimliğinin Telegram'da yayınlanan fotoğraf ve videodan tespit edilmesine ilişkin olarak, Mahkeme, söz konusu fotoğraf ve videonun başvuranın kimliğinin tespit edilmesine izin veren herhangi bir bilgi içermemesine rağmen, başvuranın kimliğinin iki günden kısa bir süre içinde tespit edildiğini kaydetmektedir. Polis raporu (bkz. yukarıdaki 11. paragraf), başvuranın kimliğini tespit etmek için hangi operasyonel arama tedbirlerinin alındığını açıklamamıştır. Başvuranın bu tedbirlerin hukuka uygunluğuna itiraz etme girişimi, mahkemelerin özetle şikâyetlerini reddetmesi nedeniyle başarısız olmuştur (bkz. yukarıdaki 16-17. paragraflar). Bu koşullar altında, başvuranın, davasında yüz tanıma teknolojisinin kullanıldığını varsayması mantıksız değildir. Hükümet bunu açıkça reddetmemiş veya başvuranın kimliğini tespit etmek için kullanılan önlemlere ilişkin herhangi bir açıklama yapmamıştır. Son olarak, Mahkeme, Rusya'daki protesto etkinliklerine katılanların kimliklerinin belirlenmesi için yüz tanıma teknolojisinin kullanıldığı çok sayıda vakaya ilişkin kamuya açık bilgileri dikkate almaktadır (bkz. yukarıdaki 40. paragraf).

71. Ayrıca, başvurana göre, polis, Moskova metrosunda seyahat ederken kendisini tutuklamak için canlı yüz tanıma CCTV kameralarını kullandığını kabul etmiştir (bkz. yukarıdaki 12. paragraf). Hükümetin, Moskova metrosuna hedef kişilerin video-gözetim sistemleri tarafından tespit ve teşhis edilmesini sağlayan CCTV kameralarının yerleştirilmesini öngören kararname de dâhil olmak üzere geçerli yasal dayanağa atıfta bulunması, mevcut davada canlı yüz tanıma teknolojisinin kullanıldığının zımni bir kabulü olarak yorumlanabilir (bkz. yukarıdaki 33. paragraf).

72. Bu arka plan karşısında ve iç hukukun yüz tanıma teknolojisinin kullanımına ilişkin resmi bir kayıt veya bildirim öngörmemesi nedeniyle başvuranın iddialarını kanıtlamasının zorluğunu, başvuranın kimliğinin hızlı bir şekilde tespit edilmesine ilişkin başka bir açıklama bulunmamasını ve Hükümet tarafından canlı yüz tanıma teknolojisinin kullanıldığının zımnen kabul edilmesini göz önünde bulundurarak Mahkeme, davanın özel koşullarında yüz tanıma teknolojisinin kullanıldığını kabul etmektedir. Mahkeme daha önce, fotoğrafların polis tarafından saklanmasının ve bu fotoğraflara yüz tanıma teknikleri uygulanmasının özel yaşam hakkına müdahale teşkil ettiğine karar vermiştir (bkz. *Gaughran / Birleşik Krallık,* no. 45245/15, §§ 69-70, 13 Şubat 2020).

73. Mahkeme, başvuranın kişisel verilerinin, yüz tanıma teknolojisinin kullanılması da dâhil olmak üzere -ilk olarak, Telegram'da yayınlanan fotoğraflardan ve videodan kimliğini belirlemek ve ikinci olarak, daha sonra Moskova metrosunda seyahat ederken yerini tespit etmek ve tutuklamak için- aleyhindeki idari suç işlemleri çerçevesinde işlenmesinin, Sözleşme'nin 8 § 1 maddesi anlamında özel hayatına saygı hakkına bir müdahale teşkil ettiği sonucuna varmıştır.

(b) Müdahalenin gerekçelendirilmesi

(i) Genel ilkeler

74. Mahkeme, herhangi bir müdahalenin hukuka uygun olması, ancak 8. maddenin 2. paragrafının atıfta bulunduğu meşru amaçlardan bir veya daha fazlasını izlemesi ve demokratik bir toplumda bu tür bir amaca ulaşmak için gerekli olması halinde müdahalenin 8 § 2 maddesi kapsamında haklı görülebileceğini yineler (bkz. *Roman Zakharov / Rusya* [BD], no. 47143/06, § 227, AİHM 2015).

75. Kişisel verilerin korunması, Sözleşme'nin 8. maddesi ile güvence altına alındığı üzere, bir kişinin özel hayatına ve aile hayatına saygı gösterilmesi hakkından yararlanması bakımından temel öneme sahiptir. İç hukuk, kişisel verilerin bu maddenin güvencelerine aykırı olabilecek şekilde kullanılmasını önlemek için uygun güvenceler sağlamalıdır. Bu tür güvencelere duyulan ihtiyaç, otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda, özellikle de bu tür veriler polisiye amaçlarla kullanıldığında (bkz. yukarıda anılan *S. ve Marper*, § 103) ve özellikle de mevcut teknolojinin sürekli olarak daha sofistike hale geldiği durumlarda (bkz. yukarıda anılan *Catt*, § 114; yukarıda anılan *Gaughran*, § 86; ve yukarıda anılan *Uzun*, § 61) daha da artmaktadır. Modern bilimsel tekniklerin ceza adaleti sisteminde kullanılmasına ne pahasına olursa olsun ve bu tür tekniklerin yaygın kullanımının potansiyel faydalarını özel hayatın önemli menfaatleri karşısında dikkatli bir şekilde dengelemeden izin verilmesi halinde, Sözleşme'nin 8. maddesinin sağladığı koruma kabul edilemez bir şekilde zayıflayacaktır (bkz. yukarıda anılan *S. ve Marper*, § 112).

76. Barışçıl protestolara katılımla ilgili bilgiler gibi siyasi görüşleri ortaya koyan kişisel veriler, yüksek düzeyde korumadan yararlanan özel hassas veri kategorilerine girmektedir (bkz. *Catt*, yukarıda anılan, §§ 112 ve 123).

77. Bu nedenle, kişisel verilerin toplanması ve işlenmesi bağlamında, tedbirlerin kapsamını ve uygulanmasını düzenleyen açık ve ayrıntılı kuralların dışında, diğerlerinin yanı sıra, süre, saklama, kullanım, üçüncü tarafların erişimi, verilerin bütünlüğünü ve gizliliğini koruma usulleri ve imha usullerine ilişkin asgari güvencelerin bulunması ve böylece kötüye kullanım ve keyfilik riskine karşı yeterli güvencelerin sağlanması esastır (bkz. yukarıda anılan *S. ve Marper*, § 99, ve P.N. / Almanya, no. 74440/17, § 62, 11 Haziran 2020).

(ii) Mevcut davaya uygulanması

78. Mahkeme, mevcut davada, kanunilik ve meşru bir amacın varlığı sorularının, müdahalenin "demokratik bir toplumda gerekli" olup olmadığı sorusundan ayrı tutulamayacağı kanaatindedir (bkz. yukarıda anılan *S. ve Marper*, § 99; *Nemtsov / Rusya*, no. 1774/11, § 75, 31 Temmuz 2014; ve *Elvira Dmitriyeva / Rusya*, no. 60921/17 ve 7202/18, § 77, 30 Nisan 2019). Bu nedenle, aşağıda bunları birlikte inceleyecektir.

79. Yerel makamlara ve Hükümete göre, başvuran aleyhinde alınan tedbirlerin İSK, OAFY, Polis Yasası ve 410 sayılı Kararname'de yasal dayanağı bulunmaktadır.

80. Mahkeme, operasyonel arama faaliyetlerinin yalnızca iç hukukta "suç" olarak sınıflandırılan bir suçla bağlantılı olarak gerçekleştirilebileceğini belirterek başlayacaktır (bkz. yukarıdaki 24. paragraf). Dolayısıyla, OAFY, idari bir suçla ilgili olan mevcut davada alınan tedbirler için yasal dayanak teşkil edemez.

81. Hem İSK hem de Polis Kanunu polise idari suçları soruşturma ve kişisel verileri içeren deliller de dâhil olmak üzere delil toplama yetkisi vermiştir (bkz. yukarıdaki 26-29. paragraflar). 410 sayılı Kararname, Moskova metrosuna polisin erişebileceği canlı yüz tanıma CCTV kameralarının yerleştirilmesini sağlamıştır (bkz. yukarıdaki 33-34. paragraflar). Dolayısıyla Mahkeme, başvurana karşı alınan tedbirlerin iç hukukta yasal bir dayanağı olduğunu kabul etmektedir.

82. Başvuranın, iç hukukun "hukuk kalitesi" gerekliliğini karşılamadığını iddia ettiği ölçüde, Mahkeme, yüz tanıma teknolojisinin uygulanması bağlamında, tedbirlerin kapsamını ve uygulanmasını düzenleyen ayrıntılı kuralların yanı sıra kötüye kullanım ve keyfilik riskine karşı güçlü güvencelere sahip olmanın gerekli olduğunu düşünmektedir. Canlı yüz tanıma teknolojisinin kullanımı söz konusu olduğunda, güvencelere duyulan ihtiyaç daha da artacaktır.

83. Mahkeme, iç hukuk hükümlerinin "kanun kalitesi" şartını karşıladığına dair güçlü şüphelere sahiptir. Mahkeme, özellikle, iç hukukun biyometrik kişisel verilerin "adaletin idaresi ile bağlantılı olarak" işlenmesine izin verdiğine dikkat çekmektedir (bkz. yukarıdaki 31. paragraf). Bu yasal hüküm geniş bir şekilde formüle edilmiştir. Hükümetin, bu hükmün Yüksek Mahkemeler veya Anayasa Mahkemeleri tarafından yapılan herhangi bir yetkili yorumuna atıfta bulunmadığı veya idari ve adli uygulamada kısıtlayıcı yorum ve uygulamasına ilişkin herhangi bir örnek sunmadığı dikkate alındığında, herhangi bir adli işlemle bağlantılı olarak biyometrik kişisel verilerin- yüz tanıma teknolojisi yardımıyla da dâhil olmak üzere- işlenmesine izin verdiği görülmektedir. İç hukuk, yüz tanıma teknolojisinin kullanımına yol açabilecek durumların niteliği, amaçlanan hedefler, hedef alınabilecek kişi kategorileri veya hassas kişisel verilerin işlenmesine ilişkin herhangi bir sınırlama içermemektedir. Ayrıca, Hükümet, Rusya'da yüz tanıma teknolojisinin kullanımına eşlik eden yetkilendirme prosedürleri, elde edilen verilerin incelenmesi, kullanılması ve saklanması için izlenecek prosedürler, denetim kontrol mekanizmaları ve mevcut çözüm yolları gibi herhangi bir usuli güvenceye atıfta bulunmamıştır.

84. Mahkeme ayrıca, itiraz edilen tedbirlerin suçun önlenmesi gibi meşru bir amaç güttüğü varsayımından hareket edecektir.

85. Mahkeme, günümüz Avrupa toplumlarının karşılaştığı zorluklardan biri olan suçla ve özellikle de organize suç ve terörizmle mücadelenin, büyük ölçüde modern bilimsel soruşturma ve kimlik belirleme tekniklerinin kullanımına bağlı olduğunu tartışmasız bulmaktadır. Ancak, suçun tespiti ve soruşturulmasında bu tür tekniklerin önemini kabul etmekle birlikte, Mahkeme, incelemesinin kapsamını sınırlandırmalıdır. Sorun, biyometrik kişisel verilerin yüz tanıma teknolojisi ile işlenmesinin genel olarak Sözleşme kapsamında haklı görülüp görülemeyeceği değildir. Mahkeme tarafından değerlendirilmesi gereken tek

konu, mevcut davada başvuranın kişisel verilerinin işlenmesinin Sözleşme'nin 8 § 2 maddesi kapsamında haklı olup olmadığıdır (karşılaştırınız *S. ve Marper*, yukarıda anılan, §§ 105-06).

86. Mahkeme, başvuranın kişisel verilerinin işlenmesinin "demokratik bir toplumda gerekli" olup olmadığını belirlerken, öncelikle özel hayata saygı hakkına yapılan fiili müdahalenin düzeyini değerlendirecektir (bkz. yukarıda anılan *P.N. / Almanya*, §§ 73 ve 84). Mahkeme, polisin başvuranın dijital görüntülerini toplayıp sakladığını ve bunları yüz tanıma teknolojisi yardımıyla başvuranın biyometrik kişisel verilerini çıkarmak ve işlemek için kullandığını kaydeder: ilk olarak, Telegram'da yayınlanan fotoğraflardan ve videodan kimliğini tespit etmek ve ikinci olarak, Moskova metrosunda seyahat ederken yerini tespit etmek ve tutuklamak. Mahkeme, özellikle canlı yüz tanıma teknolojisi söz konusu olduğunda, bu tedbirlerin bilhassa müdahaleci olduğunu düşünmektedir (bkz. yukarıdaki 37. paragraf). Bu nedenle, bu tedbirlerin "demokratik bir toplumda gerekli" olarak kabul edilebilmesi için yüksek düzeyde bir gerekçe gerekmekte; canlı yüz tanıma teknolojisinin kullanımı için ise en yüksek düzeyde gerekçe gerekmektedir. Ayrıca, işlenen kişisel veriler, başvuranın barışçıl bir protestoya katılımı hakkında bilgi içermekte ve dolayısıyla siyasi görüşünü ortaya koymaktadır. Bu veriler, yüksek seviyede koruma gerektiren özel hassas veri kategorilerine girmektedir (bkz. yukarıdaki 76. paragraf).

87. Soruşturmalar bağlamında kişisel verilerin işlenmesinin "demokratik bir toplumda gerekliliği" değerlendirilirken, söz konusu suçların niteliği ve ağırlığı dikkate alınması gereken unsurlardan biridir (bkz. *mutatis mutandis*, *P.N. / Almanya*, yukarıda anılan, § 72). İç hukuk, niteliğine ve ağırlığına bakılmaksızın, herhangi bir suçun soruşturulması ve kovuşturulmasıyla bağlantılı olarak biyometrik kişisel verilerin işlenmesine izin vermektedir.

88. Mahkeme, başvuranın önceden bildirimde bulunmadan tek başına gösteri düzenlemekten ibaret küçük bir suçtan -iç hukukta cezai değil idari suç olarak sınıflandırılan bir suçtan- yargılandığını gözlemlemektedir. Başvuran, gösteri sırasında trafiğin engellenmesi, mülke zarar verilmesi veya şiddet eylemleri gibi kınanacak herhangi bir eylemde bulunmakla suçlanmamıştır. Eylemlerinin kamu düzeni veya ulaşım güvenliği için herhangi bir tehlike oluşturduğu da iddia edilmemiştir. Mahkeme, başvuran aleyhindeki idari ceza yargılamasının ifade özgürlüğü hakkını ihlal ettiğini tespit etmiştir (bkz. yukarıdaki 57. paragraf). Mahkeme, barışçıl protesto eylemlerine katılanları tespit etmek ve tutuklamak için son derece müdahaleci yüz tanıma teknolojisinin kullanılmasının, ifade ve toplanma özgürlüğü hakları açısından caydırıcı bir etkiye sahip olabileceğini düşünmektedir.

89. Bu koşullar altında, Telegram'da yayınlanan fotoğraf ve videolardan başvuranın kimliğini tespit etmek için yüz tanıma teknolojisinin kullanılması -*a fortiori* (dolayısıyla) Moskova metrosunda seyahat ederken yerini tespit etmek ve tutuklamak için canlı yüz tanıma teknolojisinin kullanılması- "acil bir sosyal ihtiyaca" karşılık gelmemiştir.

90. Yukarıdaki tüm değerlendirmeler ışığında Mahkeme, başvuranın Sözleşme'deki ifade özgürlüğü hakkını kullanması bağlamında son derece müdahaleci yüz tanıma teknolojisinin kullanılmasının, Sözleşme'nin korumak ve geliştirmek için tasarlandığı hukukun üstünlüğü ile yönetilen demokratik bir toplumun idealleri ve değerleri ile bağdaşmadığı sonucuna varmıştır. Başvuranın kişisel verilerinin idari suç yargılamaları çerçevesinde yüz tanıma teknolojisi kullanılarak işlenmesi -ilk olarak, Telegram'da yayınlanan fotoğraflardan ve videodan kimliğini tespit etmek ve ikinci olarak, Moskova metrosunda seyahat ederken yerini tespit etmek ve tutuklamak- "demokratik bir toplumda gerekli" olarak kabul edilemez.

91. Bütün bu gerekçelerle, Sözleşme'nin 8. maddesi ihlal edilmiştir.

V. SÖZLEŞME'NİN 6. MADDESİNİN İHLAL EDİLDİĞİ İDDİASI

92. Başvuran, Sözleşme'nin 6. maddesi uyarınca, aleyhindeki idari ceza yargılamasının, davacı taraf olmaması nedeniyle adil olmadığından şikayetçi olmuştur. Davanın olaylarını, tarafların beyanlarını ve 8. ve 10. maddeler uyarınca yaptığı tespitleri göz önünde bulunduran Mahkeme, 6. madde kapsamındaki şikâyetin kabul edilebilirliği ve esası hakkında ayrı bir karar vermeye gerek olmadığı kanaatindedir (bakınız *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 156, ECHR 2014).

VI. SÖZLEŞME'NİN 41. MADDESİNİN UYGULANMASI

93. Sözleşme'nin 41. maddesi şu şekildedir:

> "Eğer Mahkeme bu Sözleşme ve Protokollerinin ihlal edildiğine karar verirse ve ilgili Yüksek Sözleşmeci Taraf'ın iç hukuku bu ihlalin sonuçlarını ancak kısmen ortadan kaldırabiliyorsa, Mahkeme, gerektiği takdirde, zarar gören taraf lehine adil bir tazmin verilmesine hükmeder."

A. Zarar

94. Başvuran, manevi tazminat olarak 15,000 Euro (EUR) talep etmiştir.

95. Hükümet, talebin aşırı olduğunu ileri sürmüştür.

96. Mahkeme, başvurana manevi tazminat olarak 9,800 Euro (EUR) ve buna eklenebilecek her türlü verginin ödenmesine karar vermiştir.

B. Masraf ve harcamalar

97. Başvuran, avukatlık ücret sözleşmelerine ve avukatları tarafından sunulan zaman çizelgelerine dayanarak, yerel mahkemeler ve Mahkeme önünde yapılan avukatlık ücretlerine ilişkin olarak 6,400 Euro talep etmiştir.

98. Hükümet, şarta bağlı ücret sözleşmelerinin icra edilemez olması nedeniyle, başvuranın avukatlık ücretlerine ilişkin talebinin reddedilmesi gerektiğini ileri sürmüştür.

99. Mahkeme'nin içtihadına göre, bir başvuran, masraf ve harcamaların geri ödenmesine ancak bunların gerçekten ve zorunlu olarak yapıldığı ve miktar bakımından makul olduğu gösterildiği ölçüde hak kazanır. Mahkeme, başvuran tarafından imzalanan avukatlık ücret sözleşmelerinin şarta bağlı olmadığını kaydeder. Elindeki belgeleri ve yukarıdaki kriterleri göz önünde bulunduran Mahkeme, tüm başlıklar altındaki masrafları ve başvurana yüklenebilecek her türlü vergiyi kapsayan 6,400 Euro'ya hükmetmeyi makul bulmaktadır.

BU NEDENLERLE, MAHKEME, OYBİRLİĞİYLE,

1. 16 Eylül 2022 tarihinden önce meydana gelen olaylarla ilgili oldukları için başvuranın şikâyetlerini ele almaya yetkili olduğuna karar verir;

2. Özel hayata saygı ve ifade özgürlüğü haklarının ihlal edildiği iddialarına ilişkin şikâyetlerin kabul edilebilir olduğuna karar verir;

3. Sözleşme'nin 8. maddesinin ihlal edildiğine karar verir;

4. Sözleşme'nin 10. maddesinin ihlal edildiğine karar verir;

5. Sözleşme'nin 6. maddesi kapsamındaki şikâyetin ayrıca incelenmesine gerek olmadığına karar vermiştir;

6. Mahkeme;

(a) Davalı Devlet'in, Sözleşme'nin 44 § 2 maddesi uyarınca kararın kesinleştiği tarihten itibaren üç ay içinde başvurana, karar tarihinde geçerli olan kur üzerinden davalı Devlet'in para birimine çevrilmek üzere aşağıdaki tutarları ödemesine,

(i) Manevi tazminat olarak 9,800 Euro (dokuz bin sekiz yüz Euro), artı uygulanabilecek her türlü verginin;

(ii) masraf ve harcamalar için 6,400 Euro (altı bin dört yüz Euro) artı başvuru sahibinden talep edilebilecek her türlü verginin;

(b) yukarıda belirtilen üç aylık sürenin bitiminden uzlaşmaya kadar, yukarıda belirtilen tutarlar üzerinden, temerrüt süresi boyunca Avrupa Merkez Bankası'nın marjinal borç verme oranına eşit bir oranda artı yüzde üç puan basit faiz ödenmesine;

Karar verir.

7. Başvuranın adil tazmin talebinin geri kalanını *reddeder*.

İngilizce olarak hazırlanmış ve Mahkeme İç Tüzüğü'nün 77 §§ 2 ve 3. maddeleri uyarınca 4 Temmuz 2023 tarihinde yazılı olarak tebliğ edilmiştir.

Milan Blaško — Pere Pastor Vilanova

Yazı İşleri Müdürü — Başkan