HAFIZA MERKEZİ

HAKİKAT ADALET HAFIZA MERKEZİ
TRUTH JUSTICE MEMORY CENTER

GÖZETİM TEKNOLOJİLERİNİN TOPLANTI VE GÖSTERİ HAKKI ÜZERİNDEKİ ETKİSİ: TÜRKİYE ÖRNEĞİ

IRMAK ERDOĞAN

POLİTİKA BELGESİ

Meydan

GÖZETİM TEKNOLOJİLERİNİN TOPLANTI VE GÖSTERİ HAKKI ÜZERİNDEKİ ETKİSİ: TÜRKİYE ÖRNEĞİ

IRMAK ERDOĞAN

POLİTİKA BELGESİ

HAKİKAT ADALET HAFIZA MERKEZİ
Ömer Avni Mahallesi İnönü Caddesi
Akar Palas No: 14 Kat: 1
Beyoğlu 34427 İstanbul / Türkiye
0212 243 32 27
info@hafiza-merkezi.org
www.hakikatadalethafiza.org

HAZIRLAYAN
Irmak Erdoğan

TASARIM
Ekin Sanaç

PROJE KİMLİK TASARIMI
Baht. Design Studio

e-ISBN: 978-625-95069-8-2

Bu yayın ***Meydan*** projesi kapsamında **Avrupa Birliği** desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla **Hafıza Merkezi**'ne aittir ve **Avrupa Birliği**'nin görüşlerini yansıtmamaktadır.

Avrupa Birligi tarafindan finanse edilmektedir

GÖZETİM TEKNOLOJİLERİNİN TOPLANTI VE GÖSTERİ HAKKI ÜZERİNDEKİ ETKİSİ: TÜRKİYE ÖRNEĞİ

IRMAK ERDOĞAN

POLİTİKA BELGESİ

HAKİKAT ADALET HAFIZA MERKEZİ
TRUTH JUSTICE MEMORY CENTER

HAFIZA MERKEZİ

Meydan

Giriş

Barışçıl toplantı ve gösteri yürüyüşü hakkı, bireylerin ve toplulukların görüşlerini ifade etmesi, kolektif deneyimlerini paylaşması ve özellikle kamu politikalarının şekillendirilmesinde merkezi bir rol oynamaktadır[1].

Toplanma ve kitlesel hareketler, sadece anlık eylemlerden ibaret değildir. Bireylerin birlikte hareket etme iradesinin vücut bulduğu eylemler, genellikle çok katmanlı bir sürecin ürünüdür. Bu süreçte, bireyler bir araya gelebilmeli, iletişim kurabilmeli, eylemlilik öncesi ortak karar alabilecek araçlara sahip olmalıdır. Bu bağlamda, toplantı ve gösteri yürüyüşleri lojistik planlama, koordinasyon, güven ilişkisi kurulması gibi unsurlara dayanan örgütlenme faaliyetlerini içermektedir[2]. Dolayısıyla, kolektif eylemin ortaya çıkmasını mümkün kılan süreçlere yönelik müdahaleler -özellikle güvenli iletişim ve örgütlenme ilişkilerini zedeleyen uygulamalar- toplantı ve gösteri yürüyüşü hakkının kullanımını doğrudan etkilemektedir[3].

Toplantı ve gösteri yürüyüşleri söz konusu olduğunda, toplanma özgürlüğü, ifade özgürlüğü ve özel hayatın gizliliği haklarının büyük ölçüde kesiştiği ve iç içe geçtiği görülür[4]. Kimi zaman yargı kararlarında mahkemeler bağlantılı haklardan birinin ihlal edildiğine karar verdiklerinde, diğer haklar bakımından ayrıca inceleme yapmamaktadır. Nitekim Avrupa İnsan Hakları Mahkemesi, protestoların öncesinde, sırasında veya hemen sonrasında gerçekleşen gözaltılar ya da toplantıların haksız biçimde kısıtlanması gibi durumlarda olası ihlalleri toplanma hakkı kapsamında incelerken[5] gözetim teknolojileriyle toplanma hakkını mümkün kılan iletişim kanallarının tıkanmasını çoğunlukla yalnızca özel hayatın gizliliği çerçevesinde incelemektedir[6].

---

[1] United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, A/HRC/44/24 (24 Haziran 2020), s. 1, para. 4, https://docs.un.org/en/A/HRC/44/24.

[2] Amory Starr, Luis A. Fernandez, Randall Amster, Lesley J. Wood, ve Manuel J. Caro, "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis," *Qualitative Sociology* 31 (2008): 251–270, ss. 259, 260.

[3] A.g.e., s. 268.

[4] Ilia Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications," *International Review of the Red Cross* 102, Sayı: 913 (2020): 181–198, s. 189.

[5] Örneğin, AİHM kararlarında bkz. *Navalnyy v. Rusya,* Başvuru no. 29580/12 ve diğerleri, Karar Tarihi: 15.11.2018; *Éva Molnár v. Macaristan*, Başvuru no. 10346/05, Karar Tarihi: 07.10.2008; *Balçık ve Diğerleri v. Türkiye*, Başvuru no. 25/02, Karar Tarihi: 29.11.2007.

[6] "Mahkeme, yukarıda 8. maddenin ihlal edildiği sonucuna varmış olması ışığında, başvurucuların Sözleşme kapsamındaki diğer şikâyetlerini incelemeyi gerekli görmemektedir.", *Gillan ve Quinton v. Birleşik Krallık*, Başvuru no. 4158/05, 12.01.2010, para. 90

Bununla birlikte, gözetim faaliyetleri ve internet iletişimine yönelik müdahalelerin demokratik katılımın köşe taşı olan barışçıl toplantılar üzerinde doğurduğu özgün risklere dikkat çekmek önemlidir. Dijital çağda toplanma özgürlüğüne ilişkin çeşitli kararlar, raporlar ve belgelerde gözetim teknolojilerinin bu hak üzerindeki etkileri daha fazla ele alınmakla birlikte[7], söz konusu teknolojilerin toplanma özgürlüğüne doğrudan ve dolaylı etkilerini tüm boyutlarıyla ortaya koymak için daha fazla araştırmaya ve bu araştırmalarla beslenen kanun ve kararlara ihtiyaç bulunmaktadır. Bu rapor, Türkiye örneğini temel alarak ve karşılaştırmalı örnekleri de göz önünde bulundurarak, bu konuda yapılan ve yapılacak araştırmalara katkı sağlamayı amaçlamaktadır.

Bu çerçevede, rapor kapsamında öncelikle kullanımı gittikçe yaygınlaşan çevrim içi ve çevrim dışı gözetim teknolojileri tanıtılacak, ardından söz konusu teknolojilerin bireysel ve kolektif haklar üzerindeki caydırıcı ve bastırıcı etkileri analiz edilecektir. Nitekim bu teknolojiler aracılığıyla gerçekleştirilen müdahalelerin toplantılar üzerindeki etkisinin incelenmesi, hem toplanma özgürlüğünün kendine özgü niteliğinin korunması hem de protestolar sırasında uygulanan tedbirleri düzenlenmesi ve denetlenmesi bakımından büyük önem taşımaktadır[8]. Sonraki bölümlerde ise gözetim teknolojilerine ilişkin karşılaştırmalı hukuk düzenlemeleri incelenerek bu düzenlemeler Türkiye'deki hukuki çerçeve ile karşılaştırılacaktır. Son bölümde tartışılan örnekler ve karşılaştırmalı normlar ışığında kanun koyucular, uygulayıcılar, avukatlar ve sivil toplum örgütlerine yönelik önerilerle tamamlanacak; toplumda farklı aktörlerin toplantı hakkının kullanımına sunabileceği katkılar ele alınacaktır.

[7] Bu alanda önemli Birleşmiş Milletler raporları ve kararları için bkz. United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, A/HRC/44/24 (24 Haziran 2020), https://docs.un.org/en/A/HRC/44/24, toplanma hakkının çevrimiçi ortamda da korunmasının gerekliliğine dair bkz. UN Human Rights Council (HRC) Resolution A/HRC/RES/38/11 (6 Temmuz 2018), https://digitallibrary.un.org/record/1640460/files/A_HRC_RES_38_11-EN.pdf

[8] Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications", s. 190.

Gözetim Teknolojileri ve Toplanma Hakkı: Küresel Bir Sorun

Gözetim teknolojileri, bireylerin davranışlarını, hareketlerini ve kişisel verilerini sistematik bir biçimde izleyen, kaydeden ve analiz eden araçlar bütünüdür[9]. Bu teknolojilerin örnekleri olan biyometrik kimlik sistemleri, kapalı devre kameralar ve dijital veri kayıt mekanizmaları gündelik yaşamın sıradan bir parçası haline gelmiştir. Yine bilgisayar, cep telefonu, kredi kartı kullanımı aynı zamanda bireylerin günlük faaliyetlerini izlenebilir kılmaktadır[10]. Kişilere dair farklı kollardan elde edilen verilerin geniş veri havuzlarına dahil edilmesiyle gündelik yaşam pratikleri izlenir, yönlendirilebilir ve belirli sınırlar içinde tutulabilir hale gelmiştir[11].

Gözetim teknolojileri güvenliği sağlama ve suçu önleme amacıyla meşrulaştırılmakta, aynı zamanda risk yönetimi ve toplumsal kontrol işlevi görmektedir. "Suçtan arınmış toplum" hedefi doğrultusunda, bireylere dair hem sıradan hem de özel bilgilerin devletler ve özel kurumlar eliyle toplanması[12], kişisel verilerin korunması, özel hayatın gizliliği kadar toplanma hakkı üzerinde de derin etkiler yaratmaktadır. Söz konusu teknolojilerin artan kullanımıyla, bu toplum hedefinin adeta sessiz ve çatışmasız bir yapı olarak kurgulandığını söylemek yanlış olmayacaktır.

Bununla birlikte, dijital teknolojiler ikircikli bir yapıya sahiptir; gözetim amacıyla kullanılabildikleri gibi, barışçıl toplantıların gerçekleştirilmesine imkân tanıyan bir potansiyel de barındırırlar. Örneğin, #MeToo (#BenDe) hareketi çevrim içi platformlar aracılığıyla yayılarak kadınları yaşadıkları cinsel taciz ve saldırılara karşı harekete geçirmiştir[13]. Daha yakın zamanlı bir örnek olarak, Brexit'in iptali için başlatılan bir dilekçe 6 milyondan fazla insanı bir araya getirmiş ve parlamentoya sunulan en geniş çaplı dilekçeyi oluşturmuştur[14]. Tüm bu örneklerde, sosyal medya ve internet, milyonlarca bireyin aynı amaç çerçevesinde bir araya gelmesinde önemli birer araç olmuştur.

---

9 Selma Arslantaş Toktaş, Mutlu Binark, Ergin Şafak Dikmen, Işık Barış Fidaner ve Elif Küzeci, "Dijital Gözetim Olgusuna Kuramsal ve Kavramsal Bakış," *Türkiye'de Dijital Gözetim: T.C. Kimlik Numarasından E-Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi* (İstanbul: Alternatif Bilişim Derneği, 2012), s. 16.

10 A.g.e., s.17.

11 A.g.e.

12 A.g.e.

13 Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications," s. 182.

14 Cameran Ashraf, "Artificial Intelligence and the Rights to Assembly and Association," *Journal of Cyber Policy* 5, no. 2 (2020), s. 167, https://doi.org/10.1080/23738871.2020.1778760.

Bununla birlikte, internet ağları barışçıl protestoları gözetlemek, sansür ve baskı uygulamak için de kullanılmaktadır. İnternete veya belli sitelere erişimi engelleme, protestolara ilişkin içerikleri filtreleme, kişilerin sosyal medya hesaplarını izleme, sahte hesaplarla grup içi tartışmalara müdahale etme gibi yöntemler bu tür amaçlara hizmet etmektedir[15].

Oysa güvenli ve gizliliği korunan iletişim ağlarının varlığı, barışçıl protestoların planlanması ve yürütülmesinde hayati bir öneme sahiptir. Gözetim teknolojileri, çevrim içi ortamda, tüm sosyal medya paylaşımları takip edilebilecek, bir toplantıya ilişkin bilgi paylaşmış veya online arama yapmış kişileri tespit edebilecek düzeye ulaşmıştır. Dahası, protestocuların sosyal medya hesaplarına veya cihazlarına sızmak için hackleme yöntemleri kullanılmakta ya da virüslü yazılımlar aracılığıyla mobil cihazlardaki rehber listeleri, mesajlar, fotoğraflar, videolar ve diğer tüm kişisel verilere erişim sağlanabilmektedir[16].

Protestolar sırasında genel ve ayrım gözetmeksizin yürütülen gözetim daha da yoğunlaşmaktadır. Örneğin, baz istasyonlarını taklit eden "yalancı istasyonlar", toplantı çevresindeki tüm telefon sinyallerini takip etmeyi mümkün kılabilir. Her telefon ve SIM kart için benzersiz olan IMSI ve IMEI numaralarını topladıkları için "IMSI yakalayıcı" olarak adlandırılan bu cihazların, ABD'de polis şiddeti sonucu hayatını kaybeden George Floyd'un ardından gerçekleştirilen protestolarda kullanıldığı iddia edilmiştir[17]. IMSI yakalayıcılar, bağlandıkları telefonlardaki arama içeriklerini, mesajları ve internet aktivitelerini engelleyebilir veya kaydedebilir; böylece binlerce kişinin mobil faaliyetlerini izlemek veya yönlendirmek mümkün hâle gelmektedir[18]. Bu tür cihazlar karşısında, protestocuların kimliğini gizli tutma olanağı ciddi şekilde kısıtlanmaktadır.

Ağ trafiği verilerinin kolaylıkla kaydedilebilmesiyle ortaya çıkan bir diğer gözetim biçimi ise sosyal ağ analizidir. Bu teknolojiler ile telefon görüşmeleri, e-postalar ve internet kullanımı sırasında oluşan trafik verilerine dayanarak kimlerin, ne sıklıkla ve hangi

---

[15] Giulia Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights," *European Journal of Risk Regulation* 16, no. 2 (2025): 514–541, s. 520.

[16] Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications, s. 185.

[17] Privacy International, "IMSI Catchers: Facilitating Indiscriminate Surveillance of Protesters," 19 Haziran 2020, https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters.

[18] Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications", s. 185.

ağlar üzerinden iletişim kurduğunu ortaya koyan kapsamlı kayıtlar üretilmektedir[19]. Bu veriler çoğu zaman iletişimin içeriğini kapsamasa da, bireyler arasındaki ilişkileri ve sosyal bağlantıların haritasını çıkarabilmek için yeterli olmaktadır. Kurulan bağlantı ağları, yalnızca kişinin doğrudan iletişim kurduğu kişileri değil, aynı zamanda bu kişilerin bağlantıda olduğu diğer bireyleri de takip altına almaktadır[20]. Bu tür analizler suç örgütü üyelerini ve kurucularını tespit etmek gibi amaçlarla kullanılmakta, ancak suç ile ilişkili olmayan çok sayıda bireyin de dolaylı biçimde gözetim kapsamına girmesine ve potansiyel risk olarak değerlendirilmesine yol açmaktadır[21]. Bu tür uygulamaların, bir toplantı veya gösteri yürüyüşü ile ilişkili olacağı iddiasıyla pek çok kişiyi "ağ haritası" kapsamına alması durumunda, örgütlenme hakkı açısından ciddi tartışmalara yol açacağı açıktır.

Protestolarda katılımcıların kimliklerini gizlemelerini büyük ölçüde engelleyen bir diğer önemli uygulama da yüz tanıma teknolojileridir. Bu sistemler, kamusal alanlara yerleştirilen kameralar aracılığıyla bireylerin yüz verilerini toplayarak bunları veritabanlarında yer alan bilgilerle karşılaştırmakta ve kişilerin kimliğini otomatik olarak tespit edebilmektedir[22]. Son yıllarda 179 ülkeyi kapsayan araştırmada, 2012–2022 yılları arasında en az 78 ülkede kamusal alanlarda yüz tanıma teknolojilerinin kullanıldığı ortaya konulmuştur. Ayrıca bu durumun yalnızca otoriter rejimlerle sınırlı olmadığı; liberal demokrasilerde de bu tür teknolojilerin giderek yaygınlaştığı görülmektedir[23]. Özellikle gerçek zamanlı yüz tanıma uygulamaları, protestolara katılan bireylerin anlık olarak izlenmesine, takip edilmesine ve hatta hedef alınmasına olanak sağlamaktadır. Örneğin, Hong Kong'daki protestolar sırasında Çin hükümeti tarafından, 'Black Lives Matter' protestoları sırasında ise Amerikan hükümeti tarafından yüz tanıma teknolojilerinin kullanıldığı, hatta tüm protesto görüntülerinin yüz tanıma yazılımlarıyla tarandığı iddia edilmiştir[24]. Bu süreçte yalnızca şüpheli görülen kişiler değil, protesto alanında bulunan herkesin verisi ayrım gözetmeksizin işlenmektedir. Üstelik sistemlerin

---

19 Katherine J. Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," *Boston College Law Review* 49, Sayı: 3 (2008), s. 756, 757.

20 A.g.e., s. 757.

21 Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," s. 758.

22 United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, s. 9, para. 30.

23 Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights", s. 518.

24 Heather Kelly ve Rachel Lerman, "America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police", Washington Post (3 Haziran 2020) <https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/> Erişim Tarihi: 29 Mart 2026, Monika Zalnieriute, *Protests and Public Space Surveillance: From Metadata Tracking to Facial Recognition Technologies* (8 Temmuz 2021), submission to the thematic report to the 50th session of the UN Human Rights Council, SSRN, https://ssrn.com/abstract=3882317, 5.

hata payı, yanlış kimlik eşleştirmeye yol açarak kişilerin güvenlik güçlerinin gereksiz ya da orantısız müdahalelerine maruz kalmasına neden olabilmektedir[25]. Bazı örneklerde, yüz tanıma teknolojilerinin doğrudan belirli grupları da hedef alacak şekilde kullanıldığı görülmektedir. Çin'de Uygurların fiziksel görünümlerine dayanarak izlenmesi ve hareketlerinin kayıt altına alınması tür bir uygulamanın çarpıcı bir örneğidir[26].

Türkiye'de Gözetim Teknolojileri

Türkiye'de gözetim altyapısı, hukuki düzenlemelerle ve aynı zamanda gelişmiş ağ izleme teknolojileriyle desteklenen bütüncül bir kontrol rejimi olarak şekillenmektedir. Bu bağlamda en kritik araçlardan biri olan Derin Paket İnceleme (DPI)[27] teknolojisi, veri paketlerinin içeriğini analiz ederek kullanıcıların çevrimiçi faaliyetlerinin ayrıntılı biçimde izlenmesine olanak tanımaktadır[28]. Türkiye'de DPI kullanımı, kamu kurumları ile uluslararası teknoloji şirketleri arasındaki iş birlikleri üzerinden şekillenmektedir. Örneğin, ABD merkezli Procera Network şirketinin geliştirdiği DPI sistemleri[29], Türk Telekom'un ağ altyapısına entegre edilmiş[30], bu sistemler aracılığıyla kullanıcıların yalnızca internet trafiği değil; ziyaret ettikleri siteler, IP adresleri ve şifrelenmemiş veri akışları da izlenebilir hale gelmiştir. Dolayısıyla DPI teknolojisi, ağ yönetimi amacıyla kullanılan bir araç olmanın ötesine geçerek, doğrudan gözetim kapasitesini artıran bir mekanizma haline gelmiştir[31].

Bu teknolojilerin Türkiye'ye aktarımı çoğu zaman doğrudan değil, aracı şirketler üzerinden gerçekleşmektedir. Procera örneğinde de söz konusu sistemlerin Ankara merkezli bir firma olan Sekom aracılığıyla entegre edildiği görülmektedir[32]. Bu tür aracı yapılar teknik

---

25 United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, s. 9, para. 34.

26 A.g.e. s. 5, para. 12.

27 İngilizce'de "Deep Packet Inspection" şeklinde ifade edilmektedir.

28 İhsan Yılmaz, Ali Mamouri, Nicholas Morieson ve Muhammad Omer. 2025. "The Transnational Diffusion of Digital Authoritarianism: From Moscow and Beijing to Ankara." European Center for Populism Studies (ECPS), 12 Mayıs 2025.

29 Teknoloji şirketleri isim değişikliği veya birleşme ve devralma süreçlerinden geçmekte, bu durum izlerini takip etmeyi güçleştirmektedir. Örneğin, Procera ile Sardvine şirketlerinin birleştiği belirtilmelidir, Scott Bicheno, "Sandvine and Procera announce network intelligence merger", 17 Temmuz 2017, https://www.telecoms.com/enterprise-telecoms/sandvine-and-procera-announce-network-intelligence-merger, Erişim Tarihi: 30 Mart 2026.

30 Bilge Yeşil, Efe Kerem Sözeri, "Online surveillance in Turkey: Legislation, technology and citizen involvement". Surveillance & Society, Cilt: 15, Sayı: 3/4, 2017, s. 546.

31 Thomas Brewster, "Is an American Company's Technology Helping Turkey Spy on its Citizens", https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan, 25 Ekim 2016, Forbes, Erişim Tarihi: 30 Mart 2026.

32 Turkish Minute, "Forbes says Türk Telekom hacking Turkish citizens via US firm", 25 Ekim 2016, https://www.turkishminute.com/2016/10/25/forbes-says-turk-telekom-hacking-turkish-citizens-via-us-firm/,

süreci kolaylaştırsa da, aynı zamanda sorumluluğun dağılmasına ve sürecin şeffaf bir şekilde takibinin güçleşmesine neden olmaktadır.

Gözetim teknolojilerinin ihracatı, geniş bir uluslararası yayılma sürecinin parçası olarak değerlendirilmelidir. Sandvine/Procera gibi Batılı şirketlerin yalnızca Türkiye'ye değil, birçok Orta Doğu ülkesine benzer gözetim teknolojileri sağladığı bilinmektedir. Bu şirketler, teknik altyapı sunmanın yanı sıra gözetim pratiklerinin kurulmasını kolaylaştırıcı bir rol de oynamaktadır[33]. Bu durum, dijital gözetim kapasitesinin yerel politikalarla ve küresel teknoloji ticaretiyle şekillendiğini göstermektedir.

Türkiye'de gözetim teknolojilerine yapılan yatırımın zamanlaması da dikkat çekicidir. Özellikle 2013 Gezi Parkı protestoları sonrasında bu yatırımların hız kazandığı görülmektedir. Bu durum, dijital gözetim araçlarının salt teknik bir gelişmenin sonucu olmadığını, toplantı ve gösterilere yönelik kontrol ihtiyacının bir yansıması olduğunu göstermektedir[34].

Gözetim kapasitesinin bir diğer önemli boyutunu, hedef odaklı izleme imkânı sağlayan casus yazılımlar (spyware) oluşturmaktadır. Bu kapsamda öne çıkan araçlar arasında, İtalya merkezli Hacking Team tarafından geliştirilen Remote Control System (RCS) ile Gamma International/FinFisher tarafından üretilen FinSpy yer almaktadır. Söz konusu yazılımlar, klasik ağ izleme tekniklerinden farklı olarak doğrudan kullanıcı cihazlarını hedef almakta ve cihazın içerisine sızdıktan sonra tamamen kontrol sağlamaktadır[35]. Cihaza sızılmasının ardından kullanıcılarının anlık konum bilgileri takip edilebilmekte; telefon görüşmeleri, mesajlaşmalar ve e-posta içerikleri kaydedilebilmekte; ayrıca cihazın mikrofonu ve kamerası uzaktan aktif hale getirilerek fiziksel ortam da gözetim kapsamına dahil edilebilmektedir. Bu yönüyle casus yazılımlar, yalnızca dijital iletişimi değil, bireyin tüm özel yaşam alanını kapsayan bütüncül bir gözetim imkânı sunmaktadır[36].

Erişim tarihi: 30 Mart 2026.

33 İhsan Yılmaz, Ali Mamouri, Nicholas Morieson ve Muhammad Omer, "The Transnational Diffusion of Digital Authoritarianism: From Moscow and Beijing to Ankara." *European Center for Populism Studies (ECPS)*, 12 Mayıs 2025, https://www.populismstudies.org/the-transnational-diffusion-of-digital-authoritarianism-from-moscow-and-beijing-to-ankara/, Erişim Tarihi: 30 Mart 2026.

34 A.g.e.

35 Bilge Yeşil, Efe Kerem Sözeri, "Online surveillance in Turkey: Legislation, technology and citizen involvement", s. 546.

36 European Center for Constitutional and Human Rights, "Surveillance software 'made in Germany' for Turkish authorities? Public Prosecutor's Office charges FinFisher executives", https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher, Erişim Tarihi: 30 Mart 2026, Bilge Yeşil & Efe Kerem Sözeri. (2017). *Online surveillance in Turkey: Legislation, technology and citizen involvement.* Surveillance & Society, 15(3/4). https://doi.org/10.24908/ss.v15i3/4.6637 546

Türkiye bağlamında bu teknolojilerin kullanımına ilişkin en çarpıcı örneklerden biri, FinSpy yazılımının 2017 yılında muhalif bir hareketle bağlantılı gözüken sahte bir internet sitesi üzerinden yayılmasıdır. Orijinalinde protesto katılımcılarının iletişim kurmasını kolaylaştırmayı amaçlayan bir platformun taklit edilmesiyle oluşturulan bu site, ziyaretçilerini bir uygulama indirmeye yönlendirmiş; uygulama aracılığıyla cihazlara casus yazılım bulaştırılmıştır. Bu yöntem, gözetim faaliyetlerinin pasif veri toplama ile sınırlı kalmadığını, aktif olarak hedef seçme ve yanıltma tekniklerini de içerdiğini göstermektedir[37]. Ayrıca, Birleşik Krallık tarafından Türkiye'ye IMSI yakalayıcı ihraç edildiğine dair veriler, mobil verilerin de gözetimin kapsamına alındığını göstermektedir[38].

Bu tür uygulamalar, dijital gözetimin doğrudan muhalefeti hedef alabilecek şekilde kullanılabildiğini ortaya koymaktadır. Özellikle gazeteciler, aktivistler, sivil toplum örgütleri ve protestocuların hedef alınması, gözetim teknolojilerinin kamusal güvenlik gerekçesinin ötesine geçerek siyasal kontrol aracı haline geldiğine işaret etmektedir. Bu bağlamda casus yazılımlar, yalnızca teknik bir araç olmanın ötesine geçerek, aynı zamanda izleme, caydırma ve bastırma stratejilerinin merkezinde yer alan bir unsur olarak değerlendirilebilir[39].

İnternet trafiğini filtreleme ve yönlendirme teknolojileri de yaygın biçimde kullanılmaktadır. Örneğin, PacketShaper gibi sistemler belirli içeriklerin engellenmesine ve kullanıcı davranışlarının analiz edilmesine imkân tanımaktadır[40]. Asoto, Netclean ve Nokia Siemens Networks gibi şirketlerin sağladığı kitlesel gözetim hizmetlerinin Türkiye'de çeşitli kamu kurumları tarafından kullanıldığına dair bulgular mevcuttur. Bu durum, gözetim teknolojilerinin çok aktörlü bir yapı içinde tedarik edildiğini göstermektedir[41]. Yine bant daraltma *(throttling)* tekniği, özellikle acil durumlarda ve protesto dönemlerinde bilgi dolaşımını sınırlamak amacıyla kullanılmaktadır. İnternet servis sağlayıcıları düzeyinde uygulanan bant daraltma uygulamaları, sosyal medya

---

37 Reporters Without Borders, "Spyware exports in Turkey: RSF Germany denounces the German company FinFisher", 09.10.2019, https://rsf.org/en/spyware-exports-turkey-rsf-germany-denounces-german-company-finfisher, Erişim Tarihi: 30 Mart 2026.

38 Joseph Cox, "The UK Granted Spy Tech Export to Turkey Amid Its Massive Crackdown on Dissent" 19 Temmuz 2017, https://www.vice.com/en/article/the-uk-granted-spy-tech-export-to-turkey-amid-massive-crackdown/, Erişim Tarihi: 30 Mart 2026.

39 Morgan Marquis- Boire, Bill Marczak, Claudio Guarnieri, John Scott- Railton, "For Their Eyes Only: The Commercialization of Digital Spying", Citizen Lab, 1 Mayıs 2013, https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf , Erişim Tarihi: 30 Mart 2026, ss. 95, 112-114.

40 Bilge Yeşil, Efe Kerem Sözeri, "Online surveillance in Turkey: Legislation, technology and citizen involvement", s. 546.

41 Bilge Yeşil, Efe Kerem Sözeri, ve Emad Khazraee, "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" *Internet Policy Observatory*, 2017, s. 10.

platformlarına erişimi yavaşlatarak kullanıcıların iletişim kurmasını zorlaştırmaktadır[42]. Bu tür müdahaleler, söz konusu teknolojilerin kolektif eylemleri engelleme potansiyelini göstermektedir.

Sosyal medya platformları bu gözetim ve kontrol ekosisteminin önemli bir parçasıdır. Türkiye, içerik kaldırma talepleri açısından küresel ölçekte en üst sıralarda yer almakta; Facebook, Google ve Twitter gibi platformlara yapılan yoğun talepler, dijital alan üzerindeki müdahale kapasitesini ortaya koymaktadır. Bu durum, platformların içerik denetiminin giderek merkezileştiğini göstermektedir[43].

Yine son yıllarda Türkiye'de yüz tanıma sistemleri ve akıllı şehir teknolojilerinin hızla yaygınlaştığı görülmektedir. Bu yaygınlaşma büyük ölçüde kamu ihaleleri aracılığıyla gerçekleşmekte; emniyet birimlerine yüz tanıma özellikli kameralar, internet izleme ve analiz yazılımları ile açık kaynak istihbaratı sistemleri tedarik edilmektedir. Nitekim 2024 yılında 30 ilde kullanılmak üzere yüz tanıma sistemlerinin kurulmasına yönelik teknolojileri alınmış,[44] 2025 yılında İstanbul, Tokat ve diğer illerde de alımlar yapılmıştır[45]. Bu kapsamda binlerce yüz tanıma kamerasının yanı sıra, sunucu ve ağ takibi altyapı ekipmanının da temin edilmesi[46], gözetim kapasitesinin arttırılarak merkezi ve entegre bir yapıya kavuşturulduğunu göstermektedir.

---

[42] Beyza Nur Demir, "İnternet Özgürlüğü ve Erişim Engelleme: İfade Özgürlüğü Bağlamında Bir Değerlendirme", Bilişim Hukuku Dergisi, Cilt 7, Sayı: 1, 2025, s. 393. 6 Şubat Depremleri sonrasında bant daraltma uygulanması, bu tür uygulamalara örnek teşkil etmektedir. Bu yönteme başvurulduğunda, gerekçesi çoğu zaman açıklanmamaktadır, bkz. Demir, s.396; dipnot 75.

[43] Bilge Yeşil, Efe Kerem Sözeri, and Emad Khazraee, "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" *Internet Policy Observatory*, 2017, s.11. Ayrıca platformların içerik kaldırma gerekçelerini açık biçimde raporlamaması ve düzenleyici kurumların bu süreçleri "ticari sır" kapsamında gizlemesi, dijital denetimin kamuoyu tarafından izlenmesini zorlaştırmaktadır, bkz. İfade Özgürlüğü Derneği, *Dijital İtaat Rejimi: Türkiye'de Sosyal Ağ Sağlayıcıları ve Şeffaflık Yanılsaması*, 13 Ocak 2026, https://ifade.org.tr/basin-bultenleri-ve-duyurular/sosyal-medya-raporu/, Erişim Tarihi: 2 Nisan 2026.

[44] İlgili ihaleler, Elektronik Kamu Alımları Platformu üzerinden takip edilebilir. İçişleri Bakanlığı Emniyet Müdürlüğü tarafından 30 ilde yüz tanıma teknolojisi alımı için bkz. İhale Kayıt No: 2024/1227117, İlan Tarihi: 25.10.2024, https://ekapv2.kik.gov.tr/ekap/search/2024_1227117.

[45] İstanbul Emniyet Müdürlüğü İhtiyacında Kullanılmak Yüz Tanıma Sistemi malzeme alımına ilişkin, İhale Kayıt No: 2025/332877, İlan Tarihi: 09.05.2025, https://ekapv2.kik.gov.tr/ekap/search/2025_332877, Tokat Valiliği Emniyet Müdürlüğü Hikvision Ids-2cd7a86g2-Izhs 8-32mm veya dengi Yüz Tanıma Sistemi Kamerası, İhale Kayıt No: 2025/378827, İlan Tarihi: 25.04.2025.

[46] *Sistem ve Siber Tehdit İstihbarat Yazılım Lisansı ile Açık Kaynak İstihbaratı Uygulama Projesi*, Başkanlık ve Hizmet Birimleri Düzenleyici ve Denetleyici Kurumlar Kişisel Verileri Koruma Kurumu, İhale Kayıt No: 2025/1846300, İlan tarihi 04.11.2025; *8 adet yazılım, internet içeriği çıkartma, Magnet Axiom yazılım güncellemesi hizmet alımı*, İçişleri Bakanlığı Jandarma Genel Komutanlığı Ankara Jandarma Tedarik Merkezi Komutanlığı, İhale Kayıt No: 2021/665475, İlan Tarihi: 25.10.2021, https://ekapv2.kik.gov.tr/ekap/search/2021_665475; *Xways Dongle Ve İnternet İçeriği Çıkartma Yazılımı Güncellemesi*, İçişleri Bakanlığı Jandarma Genel Komutanlığı, İhale Kayıt No: 2021/502042, İhale Tarihi: 12.10.2021, https://ekapv2.kik.gov.tr/ekap/search/2021_502042.

Bu teknolojik altyapı, protestoların izlenmesi ve sonrasında katılımcıların tespit edilmesi süreçlerinde kendini göstermektedir. Nitekim birçok protestocunun eylem sırasında değil, eylemlerin hemen ardından evlerine düzenlenen sabah baskınlarıyla gözaltına alındığı görülmektedir. Ekrem İmamoğlu'nun gözaltına alınmasının ardından 19 Mart'tan 25 Mart'a kadar gerçekleşen gösterilerde yapılan resmî açıklamalara göre 1418 kişi gözaltına alınmıştır[47]. Bu durum, hepsi olay yerinde gerçekleştirilmeyen bu gözaltılar açısından, güvenlik güçlerinin bireyleri kısa sürede nasıl tespit edebildiği sorusunu gündeme getirmektedir. Bu bağlamda güçlü açıklamalardan biri, yüz tanıma teknolojilerinin aktif biçimde kullanılmasıdır[48]. Resmî olarak açıkça kabul edilmese de, sabıka kaydı bulunmayan bireylerin dahi kimliklerinin hızlı biçimde belirlenebilmesi, biyometrik veri temelli izleme sistemlerinin devrede olduğuna dair şüphe uyandırmaktadır[49]. Nitekim kimi iddianamelerde de benzer yönde izler bulunmaktadır. Bu çalışma kapsamında incelenen bir iddianamede, kanuna aykırı toplantı ve gösteri yürüyüşlerine katıldıkları ve ihtara rağmen dağılmadıkları iddia edilen çok sayıda kişinin "deşifresine yönelik" yapılan çalışmalar sonucunda açık kimlik bilgileri ile adreslerinin tespit edildiği görülmekte; ancak söz konusu tespit sürecinin yöntemine ilişkin açıklamaya yer verilmemektedir. Bu şüpheleri güçlendiren bir diğer unsur ise sahadan gelen görseller ve tanıklık verileridir. Protestolar sırasında polislerin, göstericilerin maskelerini indirmelerini talep ederek yakın plan görüntüler kaydettiği yönündeki bulgular, bunun yanı sıra, 29 Mart'ta İstanbul Maltepe'de düzenlenen eylemler sırasında, Çin merkezli Hikvision şirketi tarafından üretilen yüz tanıma kameralarını gösteren görüntüler[50] yüz tanıma sistemlerinin kullanılmış olma ihtimalini güçlendirmektedir. Bu noktada, Hikvision kameralarının Çin'de Uygur vatandaşlarını tespit etme ve tutuklama amacıyla kullanıldığı[51] ve Avrupa Birliği Parlamentosu tarafından insan hakları ihlallerine sıkça karışan bu şirketin kameralarının kullanılmaması yönünde karar alındığı da vurgulanmalıdır[52].

---

47 BBC Türkçe, "İçişleri Bakanı Yerlikaya: Altı günlük eylemlerde 1418 gözaltı", 26 Mart 2025, https://www.bbc.com/turkce/articles/c70edn829z3o, Erişim Tarihi: 30 Mart 2026.

48 Ylenia Gostoli, "Turkey's AI-Powered Protest Crackdown", New Lines Magazine, 5 Haziran 2025, https://newlinesmag.com/spotlight/turkeys-ai-powered-protest-crackdown/, Erişim Tarihi: 30 Mart 2026.

49 Levent Kenez, "Turkey Expands Facial Recognition to Identify Protesters after Arrest of Erdogan's Political Rival", Nordic Monitor, 11 Nisan 2025, https://nordicmonitor.com/2025/04/turkey-expands-facial-recognition-to-identify-protesters-after-arrest-of-erdogans-political-rival/, Erişim Tarihi: 30 Mart 2026.

50 Eylem sırasında görüntülenen Hikvision kamerası için bkz. Ylenia Gostoli, "Turkey's AI-Powered Protest Crackdown", New Lines Magazine, 5 Haziran 2025, https://newlinesmag.com/spotlight/turkeys-ai-powered-protest-crackdown/, Erişim Tarihi: 30 Mart 2026.

51 Bethany Allen-Ebrahimian, "Report: Hikvision cameras help Xinjiang police ensnare Uyghurs", 14 Haziran 2022, https://www.axios.com/2022/06/14/report-hikvision-cameras-xinjiang-police-uyghurs, Erişim Tarihi: 30 Mart 2026.

52 Charles Rollet, "EU Parliament Removes Hikvision, Citing Human Rights Abuses" IPVM, 29 Nisan 2021, https://ipvm.com/reports/hik-eu, Erişim Tarihi: 30 Mart 2026.

2025 yılında gözetim teknolojilerinin alımı ve kullanımında bir artış gözlense de, bu gelişmelerden önce 2023 yılında kamuoyuna yansıyan ve yerli bir uygulama olarak tanıtılan Kişisel İletişim Mobil (KİM) uygulaması, daha önceki bir süreçte de hukuki zemini oldukça tartışmalı gözetim teknolojilerinin kullanımının bir örneğini sunmaktadır. Dönemin İçişleri Bakanı Süleyman Soylu'nun bir röportajında, bir kişinin fotoğrafını çekerek saniyeler içinde kimlik ve adres bilgilerine ulaşılabileceğini ifade etmesi, biyometrik veritabanlarının ne ölçüde entegre edildiğini ve belirli bir suç şüphesi dahi gerektirmeden erişilebilir hâle geldiğini göstermektedir[53].

Bu gelişmeler, Türkiye'de gözetim teknolojilerinin pasif izleme araçları olmadığını, protesto sonrası takibi, kimlik tespitini ve müdahaleyi mümkün kıldığını göstermektedir. Yüz tanıma sistemleri, kamera ağları, internet takip teknolojileri ve biyometrik veritabanlarının entegrasyonu sayesinde bireyler artık yalnızca eylem anında değil, sonrasında da tespit edilebilir hale gelmektedir. Bu durum, fiziksel ve dijital gözetim alanlarında genişlemenin özellikle anonimlik sayesinde korunan ve güçlenen kolektif eylem pratiklerini dönüştürebilecek bir niteliğe büründüğünü ortaya koymaktadır.

Gözetim Teknolojilerinin Toplanma Hakkı Üzerindeki Etkisi

Toplanma Hakkının Kullanılmasında Caydırıcı Etki

Yüz tanıma teknolojileri ve genel olarak kitlesel gözetim araçlarının kullanımı, son yıllarda kamusal alanlardaki eylemler bağlamında ciddi hukuki tartışmalara yol açmıştır. Örneğin, Birleşik Krallık'ta görülen *Bridges* davasında Mahkeme, polis tarafından otomatik yüz tanıma sistemlerinin kullanımını, yeterince açık ve öngörülebilir bir yasal çerçeveye dayanmadığı ve kişisel verilerin korunması ile ayrımcılık yasağı yükümlülüklerine aykırılık teşkil ettiği gerekçesiyle hukuka aykırı bulmuştur[54]. Bununla birlikte, bu teknolojilerin kamusal alanlarda ve protestolar sırasında kullanımı genellikle doğrudan toplanma hakkı çerçevesinde ele alınmamaktadır.

Oysa gözetim teknolojileri, bireylerin kimliklerinin tespit edilmesini kolaylaştırarak toplantı ve gösteri yürüyüşlerine anonim katılımı adeta imkânsız hale getirmektedir[55].

---

[53] Merve Kara Kaşka, "KİM uygulaması: Süleyman Soylu'nun telefonundaki uygulama hakkında neler biliniyor?", BBC Türkçe, 8 Mayıs 2023, https://www.bbc.com/turkce/articles/cd1rmnrjggyo, Erişim Tarihi: 30 Mart 2026.

[54] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, Monika Zalnieriute, "Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State", *Columbia Science & Technology Law Review* 22, Sayı: 2 (2021), s. 287.

[55] Zalnieriute, "Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State", s. 299.

Gözetim teknolojilerinin etkisi yalnızca anlık değildir; farklı veri toplama yöntemlerinin bir araya gelmesiyle, protestolara katılan bireylerin sonradan teşhis ve takip edilmesi de mümkün hâle gelmektedir. Üstelik bu süreç, herhangi bir suç şüphesi bulunmayan kişileri de içerecek şekilde işletilmektedir. Bu durum, toplantıya katılan tüm bireylerin yalnızca eylem sırasında değil, sonrasında da potansiyel sonuçlarla karşılaşabileceği anlamına gelir[56].

Öte yandan, sanal ortamda kullanılan teknolojiler de doğrudan toplanma hakkına müdahale etmektedir. Sosyal medya ve diğer iletişim araçları üzerinden protesto örgütleyen kişilerin hedef alınması; bazı durumlarda yalnızca çevrim içi toplantı organize etme faaliyetleri nedeniyle soruşturma ve kovuşturma başlatılması; toplantı ve gösteri yürüyüşlerine ilişkin içeriklerin kaldırılması; sosyal medya kısıtlamaları ve toplanmalar sırasında internet kesintileri, toplanma hakkına yönelik müdahalelere örnek teşkil etmektedir[57].

Görüldüğü gibi, kişisel verilerin korunması, özel hayatın gizliliği ve barışçıl toplanma hakkı arasında önemli bir bağ mevcuttur. Bununla birlikte, tüm bu gelişmeler, kamusal alanda mahremiyetin var olup olmadığı sorusunu yeniden gündeme getirmektedir[58]. Geleneksel yaklaşım, kamusal alanda bulunan bireylerin başkaları tarafından gözlemlenebileceğini ve bu nedenle mahremiyet beklentisinin sınırlı olduğunu kabul eder[59]. Ancak modern gözetim teknolojileri yalnızca "görme" ile sınırlı değildir; bireyleri tanımlama, sınıflandırma, geçmiş verilerle eşleştirme ve uzun vadeli analizlere tâbi tutma kapasitesine sahiptir[60]. Dolayısıyla, toplantı gösteri yürüyüşleri sırasında kamusal alanda bulunan kişilerin neredeyse otomatik olarak kimlikleri tespit edilebilir hale gelmiştir. Bu durumda, başkaları tarafından görülebilir olmak ile devlet tarafından teşhis edilip sürekli izlenebilir olmak arasında önemli bir ayrım bulunduğunun altı çizilmelidir[61].

Bu ayrım, toplanma özgürlüğü açısından kritik önem taşır. Toplumsal hareketler ve protestolar, her ne kadar kamusal alanda gerçekleşse de, bireylerin belirli bir ölçüde anonim kalabilmesine dayanır. Nitekim özel hayatın korunması yalnızca bireyin mahrem

---

56 Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications", 194.

57 A.g.e.

58 Valerie Aston, "State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives," *European Journal of Law and Technology* 8, no. 1 (2017), 3.

59 A.g.e., 5.

60 Deven R. Desai, "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding," *Notre Dame Law Review* 90 (2014): 623.

61 Bu hakkı, bir nevi "kamusal özel hayat" olarak ifade etmek mümkündür. A.g.e., 623.

alanıyla sınırlı olmayıp, kamusal alanda kurulan sosyal ilişkileri de kapsar. Dolayısıyla kamusal alanda gerçekleştirilen bir eylem, bireyin mahremiyet beklentisini tamamen ortadan kaldırmaz[62].

Kamusal alanda belirli oranda bir mahremiyetin sağlanması, protestonun işlevselliği açısından kurucu bir unsurdur. Bu mahremiyet alanı, kişilerin hayatlarındaki özel, profesyonel ve politik alanları birbirinden ayırabilmesine imkân tanır. Bu sayede bireyler, toplumda yaygın olmayan görüşlerini iş yaşamlarında, yakın ilişkilerinde veya devlet nezdinde olası olumsuz sonuçlardan çekinmeksizin ifade edebilirler[63].

Bu bağlamda, hem geriye dönük verilerle karşılaştırma hem de eylem anından görüntü ve diğer verileri kaydedebilmeyi mümkün kılan gözetim uygulamaları, bireyler üzerinde kaçınılmaz bir baskı yaratır. Eyleme katılan kişiler yalnızca o anda izlenip izlenmediklerini değil, geçmişteki faaliyetlerinin ne zaman ve nasıl analiz edileceğini de öngöremez. Bu belirsizlik, bireylerin davranışlarını otosansürle şekillendirmelerine, hâkim görüşlerden sapmamalarına ve yalnızca çoğunluk tarafından kabul gören eylemlerde bulunmalarına yol açacaktır[64]. Bu durum, literatürde "caydırıcı etki" *(chilling effect)* olarak tanımlanmakta ve demokratik katılımı zayıflatarak kamusal alanı fikir ayrılığına yer bırakmayacak şekilde dönüştüren bir unsur olarak değerlendirilmektedir[65].

Devletlerin bireyleri izleme kapasitesindeki niteliksel dönüşüm, hukukun kapsayıcılığının yeniden değerlendirilmesini gerektirmektedir. Geriye dönük ve her an erişilebilen veri temelli gözetim, geleneksel, makul şüpheye dayalı ve ileriye dönük uygulanan tedbirlerle elde edilen sınırlı bilginin ötesine geçilmesine olanak tanımaktadır[66]. Devletin bireyler hakkında genelleştirilmiş ve belirli bir şüpheye dayanmayan veri toplama kapasitesi, adeta genel arama yetkisine benzer şekilde geniş ve belirsiz müdahalelere

---

62 Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights," s. 529.

63 A.g.e., ss. 529, 530.

64 Desai, "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding," s. 623.

65 Zalnieriute, "Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State", s. 299. Zalnieriute bu bağlamda PEN America'nın çarpıcı araştırmasına yer vererek, devletin doğrudan ya da üçüncü taraflar aracılığıyla bilgi toplama kapasitesinin, yazarların bir araya gelme ve ifade faaliyetleri üzerinde caydırıcı bir etki yarattığını bulgularla göstermektedir. Bu araştırma ile katılımcıların önemli bir kısmının sosyal medya kullanımını sınırladığı veya belirli konulardan kaçındığı; bazılarının yazma, konuşma, internet araması yapma ya da tartışmalı görülebilecek kişilerle iletişim kurma konusunda çekindiği; yine bir kısmının ise dijital izlerini gizlemek için ek önlemler aldığı ortaya konulmuştur.

66 Desai, "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding," *Notre Dame Law Review* 90 (2014), s. 581

yol açabilmektedir[67]. Bu bağlamda, bireylerin okudukları kaynaklar, gittikleri yerler ve kurdukları ilişkiler gibi verilerin özel şirketler veya internet hizmet sağlayıcıları gibi üçüncü kişilerden temin edilmesi mümkündür. Söz konusu durum, yalnızca mahremiyet hakkını değil, aynı zamanda bireylerin iletişim kurma, örgütlenme ve kamusal alanda bir araya gelme süreçlerini de doğrudan etkilemektedir[68]. Toplanma hakkına yönelik müdahaleler değerlendirilirken eylem anı ve sonrası ile sınırlı kalınmamalı; bireylerin nasıl bir araya geldiği ve hangi koşullar altında örgütlenebildiği de dikkate alınmalıdır. Gözetim teknolojileri tam da bu altyapıyı hedef alarak, kamusal alana henüz taşınmamış düşünceleri ve kolektif eylemleri en başından bastırma potansiyeline sahiptir[69]. Bu nedenle, demokratik bir hukuk düzeninde gözetim faaliyetlerinin açıkça düzenlenmesi ve sınırlamalara tâbi tutulması gerekmektedir. Özellikle veri toplamanın belirli amaçlarla sınırlandırılması, saklama sürelerinin kısıtlanması ve veriye erişimin denetlenmesi gibi güvenceler toplanma hakkının kullanılabilmesinin de ön koşullarını oluşturmaktadır.

Ayrımcılık Yasağı Bağlamında "Seçici Gözetim Riski"

Makine öğrenimi ve derin öğrenme tekniklerindeki ilerlemeler ve bunları besleyen veri kapasitesinin hızla artışı gözetim teknolojilerinin gelişimini sağlasa da, bu sistemlerin hâlâ hata paylarının bulunduğu göz ardı edilmemelidir. Hata oranları; bu sistemlerin kullanım koşulları, kullanıldıkları ortam ve amaca göre değişebilmektedir. Örneğin, yüz tanıma teknolojilerinin vardıkları sonuçların doğruluk oranı kontrollü ortamlarda daha yüksekken, bu oran kamusal alanlar gibi kontrolsüz ortamlarda çok daha düşük olabilmektedir.[70] Işık, gölge ve aydınlatma gibi çevresel faktörler ile yüzün görüntülenme açısı, yüz tanıma teknolojilerinin doğruluğunu önemli ölçüde etkilemekte ve bu sistemlerin, parmak izi gibi diğer biyometrik yöntemlere kıyasla daha yüksek hata oranına sahip olmasına neden olmaktadır[71]. Yoğun kalabalığın görüldüğü kamusal alanlarda, %0,01 gibi çok düşük hata oranlarının dahi yüzlerce kişinin yanlış kimlik bilgileriyle eşleştirilmesine yol açabileceği dikkate alınmalıdır[72].

---

67 A.g.e., s. 614.

68 Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance", s. 744.

69 Desai, "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding", s. 592.

70 Giulia Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights", s. 519.

71 Zafer İçer, Elif Dönmez, "Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku Ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları", *Ceza Hukuku Dergisi*, Cilt : 15, Sayı : 43, ss. 421-461, 429, 430.

72 European Union Agency For Fundamental Rights, *Facial recognition technology: Fundamental rights Considerations in the Context of Law Enforcement*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdfM, s. 9, Giulia Gabrielli, "The Use of Facial Recognition Technologies in the Context

Ayrıca bu sistemlerin eğitildiği veri setleri çoğu zaman toplumun tüm kesimlerini dengeli biçimde yansıtmamaktadır. Bu nedenle, özellikle kadınlar, gençler ve siyah bireyler bu sistemler tarafından daha yüksek oranlarda yanlış tanımlanma riski taşımaktadır. Bu durum, bireylerin haksız şekilde kolluk müdahalesine ve hak ihlallerine maruz kalmasına açabilir. Veritabanlarının çeşitlendirilmesi yoluyla önyargı azaltılabilse de, biyometrik tanıma sistemleri hâlâ belirli grupları cinsiyet, etnik köken veya engellilik durumuna göre yüksek oranda hedef alma riski taşımaktadır[73].

Ayrımcılık riski yalnızca yüz tanıma teknolojileriyle sınırlı değildir; daha geniş ölçekli algoritmik sistemler de benzer sorunlar üretebilmektedir. Suç tahmini, sosyal yardım dağıtımı veya kamu hizmetlerine erişim gibi alanlarda kullanılan otomatik karar alma sistemleri çoğu zaman geçmiş verilere dayanır. Ancak bu veriler, tarihsel olarak daha fazla takip ve yaptırıma maruz kalmış kişi ve grupların bilgilerini içerir ve toplumsal eşitsizlikleri yansıtır. Dolayısıyla, bu tür verilerle beslenen algoritmaların bu eşitsizlikleri yeniden üretmesi tesadüf değildir. Algoritmik sistemlerin ayrımcılık üretme riski, kolluk faaliyetleri bağlamında özellikle önemli bir boyut kazanmaktadır. Günümüzde birçok ülkede polis teşkilatları, suçun nerede ve kim tarafından işlenebileceğini öngörmek amacıyla "öngörücü polislik" *(predictive policing)* sistemlerinden yararlanmaktadır. Bu sistemler, suç kayıtları, istatistikler ve mahallelerin demografik yapısı gibi çok sayıda veriyi bir araya getirerek analiz etmektedir. Ancak veri setleri çoğu zaman mevcut sınıfsal, politik veya etnik önyargıları yansıtır ve teknolojiler, genellikle zaten yoğun biçimde denetlenen, dezavantajlı bölgelerde uygulanır; uygulama sırasında bu bölgelerden elde edilen veriler sisteme yeniden dahil edilir. Böylece gözetim, belirli bölgeleri ve grupları hedefleyen seçici bir nitelik kazanır. Bu nedenle, söz konusu sistemler görünüşte tarafsız olsa da, uygulamada belirli gruplar üzerinde orantısız etkiler doğurabilmektedir[74].

İngiltere'deki *"Gangs Violence Matrix"* (Çete Şiddeti Matrisi) veritabanı bunun somut bir örneğidir. Sistem, bireyleri ırk, yaş, cinsiyet ve sosyoekonomik durum gibi ölçütlere göre değerlendirir. Veritabanına kayıtlı kişilerin yaklaşık %78'i siyahtır, oysa suça sürüklenen çocukların yalnızca %27'si bu gruba dahildir. Bu sistemin vardığı sonuçlar, kolluk kuvvetlerinin ötesinde iş bulma kurumları, konut idareleri ve eğitim kurumlarıyla

of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights," *European Journal of Risk Regulation* 16, no. 2 (2025), 519, 520.

[73] Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights", s. 520.

[74] United Nations Human Rights Council Special Rapporteur, "Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis", A/GRC/44/57, 18 Haziran 2020, s. 11, para. 35.

paylaşılmış ve bireylerin barınma, istihdam ve polis faaliyetleri gibi alanlarda haksız muameleye maruz kalmasına yol açmıştır[75].

Benzer bir durum ABD'deki PredPol sisteminde görülmektedir. Sistem, geçmiş suç verilerini analiz ederek belirli yer ve zamanlarda suç işlenme ihtimalini tahmin etmeyi amaçlar. Ancak kullanılan veriler, zaten yoğun polis denetimine tâbi tutulan siyah ve Latin kökenli topluluklardan gelmektedir. Sonuç olarak sistem, gözetimin aynı grupların yaşadıkları mahalleler üzerine yoğunlaşmasına ve mevcut eşitsizliklerin yeniden üretilmesine yol açmaktadır[76].

Kamu otoritelerinin bu teknolojileri kullanırken sistemlerin ayrımcı etkiler doğurup doğurmadığını, görünüşte tarafsız olan bir teknolojinin farklı gruplar üzerindeki etkilerini araştırma yükümlülüğü bulunmaktadır[77]. Bununla birlikte bu yükümlülüğün yerine getirilmesi kolay değildir. Özellikle söz konusu teknolojilerin özel şirketler tarafından geliştirilmesi, yazılımların ve eğitildikleri veritabanlarının ticari sır veya fikrî mülkiyet hakları kapsamında korunması, bu sistemlerin çalışma modelinin anlaşılmasını ve bağımsız denetimini zorlaştırmaktadır. Ancak ticari gizlilik gerekçesi kamu otoritelerinin vatandaşlara karşı sorumluluğunu ortadan kaldırmayacaktır. Bu nedenle, kamu otoritelerinin şeffaf ve bağımsız denetime açık şekilde tasarlanmış sistemleri tercih etmesi gerekmektedir[78].

Toplanma hakkı ve ayrımcılık yasağını ihlal etme riski oldukça yüksek olan gözetim teknolojilerinin kullanımı, yalnızca teknik veya idari bir mesele olarak ele alınamaz. Bu araçların hangi koşullarda ve sınırlar içinde kullanılabileceği hukuki düzenlemelerle belirlenmelidir. Nitekim uluslararası insan hakları hukuku, ifade özgürlüğü, özel hayatın gizliliği ile toplantı ve örgütlenme özgürlüğüne yönelik her türlü müdahalenin kanunla öngörülmüş, meşru bir amaca dayanması ve demokratik bir toplumda gerekli ve orantılı olması gerektiğini açıkça ortaya koymaktadır[79]. Bu bağlamda, yüz tanıma teknolojisine ilişkin verdiği kararlarda AİHM de "kanunla öngörülme" şartının, yalnızca bir yasal

---

75 A.g.e., s. 11, para. 36.

76 A.g.e., s. 11, para. 37.

77 Zalnieriute, "Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State", s. 295.

78 A.g.e., s. 302.

79 Avrupa İnsan Hakları Sözleşmesi'nin 8, 10 ve 11. maddeleri ile Türkiye Cumhuriyeti Anayasası 20, 26, 34. maddeleri bu hakların ne şekilde sınırlandırabileceğini açıkça göstermektedir, yine bu yönde bkz. Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights", s. 526.

dayanağın varlığını değil, aynı zamanda düzenlemelerin erişilebilir, öngörülebilir olmasını ve keyfî müdahalelere karşı yeterli güvenceleri içermesini gerektirdiğini belirtmektedir[80].

Barışçıl toplanma hakkı bağlamında gözetimin sınırlarını belirleyen kanunlar, somut ve ciddi bir suç şüphesine dayanma, belirli hedeflere yönelme ve etkili yargısal denetime tâbi olma gibi temel güvenceleri içermelidir. Ayrımcılık teşkil edebilecek seçici nitelikte hedeflemelerin yanı sıra, kitlesel ve ayrım gözetmeksizin herkesi kapsayan gözetim uygulamaları da yasaklanmalıdır[81].

Bu çerçevede, gözetim teknolojilerinin yol açtığı hak ihlalleri ve yapısal riskler, bu teknolojilerin kullanımının ayrıntılı ve bağlayıcı bir hukuki rejime tâbi kılınmasını gerekli kılmaktadır. Bir sonraki bölümde, biyometrik veri işleme, yapay zekâ sistemleri ve yüz tanıma teknolojilerine ilişkin düzenlemeler başta olmak üzere, bu alandaki güncel Avrupa düzenlemeleri, Türkiye ile karşılaştırmalı olarak ele alınacaktır.

Gözetim Teknolojileri ve Yapay Zekâya İlişkin Hukuki Düzenlemeler

Avrupa Birliği Kapsamında Düzenlemeler

Yapay Zekâ Yasası

Avrupa Birliği Yapay Zekâ Yasası[82] yapay zekâ sistemlerini kapsamlı biçimde düzenlemeye yönelik yürürlüğe girmiş dünyadaki ilk düzenlemedir. Bu düzenleme, tüm yapay zekâ sistemlerine yönelik genelgeçer kurallar getirmek yerine, sistemleri taşıdıkları risklere oranla gruplandıran bir yaklaşımı esas almakta ve risk arttıkça daha fazla kural ve yükümlülük öngörmektedir. Bu doğrultuda yapay zekâ sistemleri, kabul edilemez risk,

80 İlgili davada Mahkeme, biyometrik kişisel verilerin "yargı faaliyetleriyle bağlantılı olarak" işlenmesine izin veren bir düzenleme bulunduğuna, ancak düzenlemenin oldukça geniş ve belirsiz şekilde ele alınması sebebiyle gerçek anlamıyla sınırlandırıcı bir kanun niteliği taşımadığına değinmiştir. Mahkeme, ilgili mevzuatta yüz tanıma teknolojisinin hangi durumlarda kullanılabileceğine, hangi amaçlara hizmet edeceğine, hangi kişi gruplarını hedef alabileceğine veya hassas verilerin nasıl işleneceğine ilişkin herhangi bir sınırlama öngörülmediğine işaret etmiştir. Söz konusu detaylar, haklara yoğun müdahale içeren tüm tedbirler açısından dikkate alınmalıdır. Bununla birlikte, özel hayatın gizliliğinin ihlal edildiğine karar veren Mahkeme, toplanma hakkı açısından ayrıca bir değerlendirme yapmamıştır; bkz. AİHM, *Glukhin v. Rusya*, Başvuru no. 11519/20, Karar Tarihi: 04.10.2023.

81 United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, s. 8, para. 26.

82 Artificial Intelligence Act (Yapay Zekâ Yasası), Regulation (EU) 2024/1689, http://data.europa.eu/eli/reg/2024/1689/oj.

yüksek risk, sınırlı risk ve minimal risk olmak üzere dört kategoriye ayrılmış ve her bir kategori için farklı yükümlülükler öngörülmüştür[83].

Yapay Zekâ Yasası'nın klasik bir insan hakları düzenlemesi olmadığını özellikle vurgulamak gerekir. Düzenleme, insan haklarına yönelik risklere dikkat çekmekle birlikte, öncelikle Avrupa'da iç pazarın işleyişini kolaylaştırmak için yapay zekâya ilişkin normları uyumlu hâle getirmeyi hedeflemektedir[84]. Bu nedenle, klasik kamu hukuku denetiminden farklı bir sorumluluk sistemi öngörmektedir.

Geleneksel insan hakları hukukunda dışsal, bağımsız ve çoğu zaman yargısal denetim ön plandayken ve hakları koruma yükümlülüğü devlete aitken, Yapay Zekâ Yasası kapsamında yükümlülükler farklı aktörlere dağıtılmıştır. İlk aşamada sistemin hukuka uygunluğunu ve risk derecesini değerlendiren bizzat bu sistemi geliştiren şirketlerin veya kamu kurumlarının kendisidir. Ancak bu durum, tamamen denetimsiz bir alan yaratmamaktadır. Bununla birlikte, üye devletler tarafından belirlenen piyasa gözetim otoriteleri ve kişisel verileri koruma kurulları, sistemlerin sonradan denetlenmesi, şikâyetlerin incelenmesi ve gerektiğinde yaptırım uygulanması konusunda yetkilidir[85].

Yapay zekâ sistemlerini geliştiren ve sağlayanların, Yasa'da öngörülen hukuki yükümlülükleri yorumlayarak teknik standartlara çevirmeleri beklenmektedir. Teknik standartların büyük ölçüde insan haklarını yorumlama konusunda bilgi ve tecrübe sahibi olmayan özel sektör ve standardizasyon kuruluşları tarafından belirlenmesi, risklere karşı hakların korunmasının ne denli etkili olacağına dair tartışmaları beraberinde getirmektedir[86].

---

[83] Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act", *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703, 685.

[84] Nitekim ilgili düzenleme, AB'nin iç pazarının işleyişini kolaylaştırma amacıyla öngörülen Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın (TFEU) 114. maddesine dayanmaktadır.

[85] Lilian Edwards, *The EU AI Act: A Summary of its Significance and Scope*, Ada Lovelace Institute, Nisan 2022, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf, s. 22.

[86] Teknik standartları belirleme süreci ve standartları belirleme yetkisine sahip kurumlara dair, bkz. Natalia Giorgi, "Standardising AI – a Trade Union Perspective" in Aida Ponce Del Castillo (ed), *Artificial Intelligence, Labour and Society* (ETUI, Brussels, 2024). Yapay zekâ sistemlerinin üreticileri, yapay zekâ yasasının gerektirdiği standartlara uyumlu teknoloji ürettiklerini ya kendi iç değerlendirmeleri sonucu ya da özel standart belirleme kuruluşları tarafından sertifika almak yoluyla gösterebilirler. İkinci durumda, üreticiler Yapay Zekâ Yasası'na uygunluk karinesinden yararlanır. Bu kolaylık, dolaylı olarak Avrupa standartizasyon kuruluşları tarafından belirlenen standartları kabul etmeye yönelik teşvik sağlamaktadır. Ancak bu kuruluşların, insan haklarının korunmasından ziyade kâr amacı güden ve büyük ölçüde büyük teknoloji şirketleri tarafından şekillendirilen yapılar olduğu göz önünde bulundurulmalıdır, bkz. Corporate Europe Observatory, "Bias Baked in: How Big Tech sets its own AI Standards", 09.01.2025, https://corporateeurope.org/en/2025/01/bias-baked, Erişim Tarihi: 30 Mart 2026.

Bu kapsamda üretici veya "sağlayıcılar" olarak adlandırılan şirketler, özellikle yüksek riskli yapay zekâ sistemleri bakımından kapsamlı yükümlülüklere tâbidir. Yüksek risk içeren teknolojiler bakımından bir risk yönetim sistemi kurulması, veri setlerinin güncel, doğru ve belirli kaliteye erişmiş olması, sürece dair belge ve kayıt tutulması gibi önemli yükümlülükler öngörülmüştür[87]. Yapay Zekâ Yasası'nın önemli katkılarından biri de, sistemi üreten ve sağlayanların, sistemlerin doğruluğu ve güvenliği ile bunların içerdiği riskleri sürekli olarak değerlendirmek ve bu hususlarda kullanıcıyı bilgilendirmekle yükümlü olmasıdır[88]. Bu çerçevede, örneğin özel bir şirketin bir kamu kurumuna yapay zekâ teknolojisi temin etmesi hâlinde, söz konusu teknolojinin hangi amaçla geliştirildiğini, farklı amaçlarla kullanılması durumunda performansının nasıl etkileneceğini, ayrımcılık yasağı ve temel haklar bakımından doğurabileceği riskleri ile hata oranını şeffaf bir şekilde açıklaması beklenmektedir. Aksi takdirde, potansiyel kullanıcıların (örneğin kolluk kuvvetlerinin veya adli makamların) sistemin üçüncü kişiler bakımından doğurabileceği riskleri anlamaları ve buna dayanarak bilinçli karar vermeleri mümkün olmayacaktır.

Yasa'da, kullanıcıların yüksek riskli sistemleri kullanmadan önce bu sistemlerin temel haklara etkisine ilişkin değerlendirme yapmaları öngörülmektedir. Bu kapsamda kullanıcılar, söz konusu sistemlerin müdahale edebileceği haklar bakımından hukuka uygunluk, gereklilik ve orantılılık ilkeleriyle uyumlu olup olmadığını değerlendirmek zorundadır[89]. Bunun yanında kullanıcılar, kullanım sırasında sistemin işleyişini izlemek, ortaya çıkan riskleri üreticilere bildirmek ve ciddi ihlalleri raporlamakla yükümlüdür[90].

Önceki bölümlerde tartışılan akıllı gözetim teknolojilerinin Avrupa'da kullanımı hâlinde hukuki statülerini değerlendirmede[91] Yasa'nın getirdiği yasaklanan uygulamalar[92] ile yüksek riskli sistemler[93] ayrımı belirleyici bir rol oynamaktadır. Nitekim düzenleme, risk temelli yaklaşım çerçevesinde bazı uygulamaları tamamen yasaklarken, bazılarını ise sıkı yükümlülüklere tâbi tutarak yüksek riskli olarak sınıflandırmaktadır.

---

87 Yapay Zekâ Yasası, md. 9-12.

88 Yapay Zekâ Yasası, md. 14.

89 Haklara yönelik riskin değerlendirmesi kapsamında ele alınması gereken temel noktalar için bkz. Yapay Zekâ Yasası, md. 27.

90 Lilian Edwards, *The EU AI Act: A Summary of its Significance and Scope*, Ada Lovelace Institute, Nisan 2022, s. 22.

91 Elbette, bu yasanın yer ve kişi bakımından uygulama kapsamı sınırlıdır. Yapay Zekâ Yasası'nın ikinci maddesi gereği ilgili düzenleme AB içindeki üreticiler ve sistemi kullananlar ile Avrupa pazarına bu sistemi sunan üçüncü ülke üreticileri ve dağıtıcılarını kapsar. Bunun yanı sıra bir şirket AB dışında olsa bile, ürettiği yapay zekâ sisteminin çıktıları AB'de kullanılacaksa, düzenlemenin yükümlülüklerine tâbidir.

92 Yapay Zekâ Yasası, md.5.

93 Yapay Zekâ Yasası, md. 6 ve Ek Madde III.

Bu kapsamda, örneğin, gerçek zamanlı ve uzaktan biyometrik kimlik tespitini mümkün kılan sistemlerin kamusal alanda kolluk faaliyetleri kapsamında kullanımı yasaklanmıştır[94]. Bununla birlikte, bu tür sistemlerin kullanımı, hürriyetinden yoksun kılınan *mağdurların* tespiti, suç işlediğinden şüphelenilen belirli kişinin yerini ve kimliğini tespit gibi sınırlı amaçlarla ve ancak bağımsız bir denetim mekanizmasına tâbi olmak kaydıyla mümkün kılınmıştır. Başka bir deyişle, Avrupa Yapay Zekâ Yasası, geniş ölçekli CCTV ağlarının yüz tanıma yazılımlarıyla birleştirilerek, sınırsız sayıda kişinin genel önleyici amaçlarla tespit edilmesini kesin bir şekilde yasaklamaktadır[95].

Buna karşılık, tamamen yasaklanmayan ancak ciddi riskler barındıran teknolojiler, yüksek riskli yapay zekâ sistemleri olarak sınıflandırılmaktadır. Bu kategori, özellikle kolluk faaliyetleri, sınır yönetimi ve adalet sisteminde kullanılan yapay zekâ uygulamalarını kapsamaktadır. Örneğin, mahkemelerde dava dosyalarını analiz ederek benzer karar örneklerini öneren yapay zekâ yazılımları bu kapsamdadır. Bu tür sistemler, doğrudan yasaklanmak yerine; risk yönetimi, veri kalitesi, şeffaflık, insan denetimi ve temel haklar üzerindeki etkilerin değerlendirmesi gibi bir dizi yükümlülüğe tâbi tutulmaktadır[96].

Sonuç olarak, Avrupa Yapay Zekâ Yasası, genel olarak gözetim teknolojilerini tamamen yasaklayan bir çerçeve sunmamakta; aksine bu teknolojileri belirli koşullar altında mümkün kılan, onları sınıflandıran, sınırlandıran ve kısmen denetime tâbi tutan bir düzenleme modeli benimsemektedir. Bu yönüyle, bir yandan piyasa entegrasyonunu hedefleyen bir iç pazar aracı olarak işlev görürken, diğer yandan özellikle yasaklanan uygulamalar, şeffaflık yükümlülükleri ve denetim mekanizmaları aracılığıyla gözetim teknolojilerinin kontrol altına alınması bakımından önemli bir adım teşkil etmektedir[97].

---

94 Gerçek zamanlı uzaktan biyometrik kimlik tespit sistemi, biyometrik verilerin elde edilmesi, karşılaştırılması ve kişinin kimliğinin belirlenmesi işlemlerinin *önemli bir gecikme olmaksızın* gerçekleştiği biyometrik kimlik tespit sistemidir; bu kavram yalnızca *anlık tespiti* değil, aynı zamanda *sınırlı ve kısa gecikmeleri* de kapsar (Yapay Zekâ Yasası, md. 3/42). Buna karşılık, uzun bir ara sonrasında ve geriye yönelik yapılan biyometrik kimlik tespiti sistemleri tamamen yasaklanmamış, yüksek riskli yapay zekâ sistemleri kapsamında değerlendirilmiştir. Bu sistemler esasen önceden kaydedilmiş görüntülerin sonradan analiz edilmesine dayanır. Her ne kadar bu rapor kapsamında ayrıntılı olarak incelenmese de, kimlik tespit işlemlerin daha sonra gerçekleştirilmemesinin, bu sistemlerin temel haklara müdahale bakımından doğurduğu riskleri ortadan kaldırmadığı; bu nedenle "gerçek zamanlı" ve "gerçek zamanlı olmayan" sistemler arasındaki ayrımın öğretide eleştiriye konu olduğu belirtilmelidir, bkz. EDRI, "Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces", 2022, https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf, Alice Giannini ve Sarah Tas, "AI Act and the Prohibition of Real-Time Biometric Identification:Much ado about nothing?", *Verfassungsblog*, 10 Aralık 2024, https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification, Erişim Tarihi: 27 Mayıs 2026.

95 Michael Veale, Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International,* Cilt: 4, 2021, s. 101.

96 Yapay Zekâ Yasası, md. 9-22, md. 27.

97 Gözetim teknolojilerinin düzenlenmesinde, Yapay Zekâ Yasası'nın yanı sıra, Avrupa Komisyonu tarafından düzenlenen kılavuzlar (örneğin *Commission Guidelines on Prohibited Artificial Intelligence Practices*, Regulation

Kişisel Verilerin Korunmasına Dair Düzenlemeler

Kişisel verilerin korunması, modern gözetim teknolojilerinin -özellikle de yüz tanıma sistemleri, sosyal ağ analizleri ve derin paket inceleme (DPI) gibi araçların- sınırsız veri işleme kapasitesine karşı temel bir güvence işlevi görmektedir. Veri koruma hukuku, verilerin toplanmasına, saklanmasına, paylaşılmasına ilişkin önemli sınırlar getirerek pek çok hakka yönelik ağır müdahale içeren teknolojilerin kullanımına karşı önemli bir kalkan teşkil etmektedir.

Avrupa Birliği'nde bu alandaki temel düzenleme Genel Veri Koruma Tüzüğü'dür (GDPR)[98]. GDPR; suçların önlenmesi, soruşturulması, tespiti veya cezaların infazı gibi amaçlarla yetkili makamlar tarafından gerçekleştirilen kişisel veri işlemeyi kapsam dışında bırakmıştır[99]. Bu önemli alanlardaki boşluk, kolluk ve ceza yargılamaları alanında kişisel veri işlenmesini düzenleyen 2016/680 sayılı Direktif[100] ile doldurulmuştur. Direktifin uygulanması için iki şartın bir arada gerçekleşmesi gerekir: kişisel veriler yukarıda sayılan amaçlarla işlenmeli ve işleyen merciler suçla mücadele, soruşturma, kovuşturma ve infaz alanlarında yetkili merciler olmalıdır[101]. Bu durumda, kolluk kuvvetleri suçla mücadele amacıyla veri işlediğinde Direktif uygulanırken, suçla mücadelede yetkili olmayan özel şirketlere GDPR hükümleri uygulanacaktır.

Her iki düzenlemede öngörülen ilkeler üç temel amaca hizmet etmektedir: hukuka uygunluk, gereklilik ve orantılılık[102]. Veri işlemenin yalnızca meşru bir amaca dayanması yeterli olmayıp, aynı zamanda demokratik bir toplumda gerekli ve ölçülü olması gerekir.

-(EU) 2024/1689, C(2025) 5052, 2025), Avrupa Veri Koruma Kurulu tarafından yayımlanan görüşler (*EDPB Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models*, 2024) ve Avrupa Veri Koruma Denetçisi'nin rehberliği (*EDPS, Generative AI and the EUDPR: Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems*, 2025), sürekli gelişen bu alanda yol gösterici olup, hukuki belirliliğe önemli katkı sağlamaktadır.

98 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

99 GDPR, md. 2/(2)(d).

100 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016.*

101 Yetkili merciler 2016/380 sayılı Direktif, md. 3/f. 7'de tanımlanmıştır.

102 Bu ilkeler, GDPR kapsamında veri işlemenin hukuka uygun, adil ve şeffaf olması; belirli, açık ve meşru amaçlarla işlenmesi; amaçla bağlantılı, sınırlı ve ölçülü olması ile verilerin doğru ve güncel tutulması şeklinde düzenlenmiştir (GDPR, md. 5). Benzer ilkeler, 2016/680 sayılı Direktif'in 4. maddesinde de öngörülmüştür.

Bu çerçevede, Avrupa Birliği Temel Haklar Şartı ve Avrupa İnsan Hakları Sözleşmesi'nin özel hayatın korunmasına ilişkin hükümleri de belirleyici rol oynamaktadır[103].

Özellikle otomatik karar alma ve profilleme sistemleri bakımından gerek GDPR md. 22 ile gerekse Direktif md. 11 ile önemli güvenceler sunmaktadır. Bu hükümler, bireylerin yalnızca otomatik veri işleme süreçlerine dayanılarak haklarında hukuki veya benzer şekilde önemli sonuçlar doğuran kararlara tâbi tutulmalarına karşı önemli haklar öngörmektedir. Böylece, bireylerin algoritmik sistemler tarafından "nesneleştirilmesi" ve insan denetiminden bağımsız kararlara katlanmak zorunda kalması engellenmek istenmiştir[104].

Gözetim teknolojilerinin en yoğun müdahale alanlarından biri olan biyometrik veriler ise GDPR ve Direktif kapsamında özel nitelikli kişisel veri olarak kabul edilmekte[105] ve kural olarak işlenmeleri yasaklanmaktadır. Yüz tanıma teknolojileri gibi uygulamalar, bireylerin biyometrik verilerinden yola çıkarak kimliklerini doğrudan tespit etmeye imkân tanıdığı için, bu verilerin işlenmesi ancak istisnai hallerde ve sıkı güvenceler altında mümkündür. Bu bağlamda ilgili maddelerde sayılan hukuki bir zeminin bulunması, asgari veri işleme ve veri güvenliği şartlarının sağlanması büyük önem taşımaktadır. Örneğin verilerin şifrelenerek kaydedilmesi, mümkünse anonim hale getirilmesi, yalnızca gerekli olan özel nitelikli verilerin işlenmesi ve gerekli olmayan verilerin derhal silinmesi, gözetilmesi gereken hususlardır[106].

Bu nedenle, kolluk faaliyetleri bakımından biyometrik verilerin işlenmesi, genel nitelikte düzenlemelere dayanılarak meşrulaştırılamaz. Avrupa Veri Koruma Denetçisi (EDPS), yüz tanıma teknolojilerine ilişkin kılavuzunda, bu tür uygulamalara ilişkin düzenlemelerde, hangi amaçla veri işleneceğinin açıkça belirtilmesi, özel nitelikte verilerin nasıl, hangi koşullar altında saklanacağını ve ne zaman yok edilmesi gerektiğinin detaylı bir şekilde ele alınması gerektiğini belirtmektedir[107]. Bu nedenle, biyometrik verilerin işlenmesine ilişkin düzenlemelerin yalnızca kanuni bir dayanağa sahip olması yeterli olmayıp, aynı

---

[103] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Publications of European Union, 2014, ss. 64-67.

[104] Şehriban İpek Aşıkoğlu, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayınevi, İstanbul, 2018, s. 153.

[105] Özel nitelikli kişisel veriler GDPR md. 9 ve Direktif md. 10 kapsamında düzenlenmektedir.

[106] 29. Madde Çalışma Grubu. (2011). *Advice paper on special categories of data ("sensitive data")*, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, Erişim Tarihi: 23 Haziran 2023, s. 11

[107] EDBP, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 26 Nisan 2023, https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf, para. 68-72. Erişim Tarihi: 31 Mart 2026.

zamanda bu dayanağın teknolojiye özgü riskleri karşılayacak düzeyde ayrıntılı olması gerekmektedir. Aksi halde bireylerin hangi koşullarda bu tür yoğun gözetim tedbirlerine tâbi tutulacağını öngörmesi mümkün olmayacak ve veri işleme faaliyetleri keyfiliğe açık hale gelecektir. Bu tür bir korumanın, yalnızca biyometrik verileri işleyen teknolojiler açısından değil, kişilerin dinî inançları, politik görüşleri, ırk ve cinsel yönelimleri gibi özel nitelikte diğer verilerini kaydeden tüm teknolojiler açısından geçerli olduğu unutulmamalıdır[108].

Kitlesel gözetim uygulamalarının bir diğer boyutunu ise açık kaynak istihbaratı (OSINT) ve internet üzerinden veri çekme *(web scraping)* teknikleri oluşturmaktadır. Bu konuda, internette kamuya açık şekilde paylaşılan verilerin sınırsızca toplanabileceği yönünde hatalı bir kanı bulunmaktadır. Oysa bir kişiyi ayırt edilebilir kılan tüm bilgiler, herkese açık şekilde paylaşılmış olsa dahi kişisel veri niteliğini korumaya devam etmektedir. Dolayısıyla kamuya açık şekilde paylaşılan verileri yeniden işleyen adli ve idari birimler ile ticari şirketlerin, kişisel verilerin korunması hususunda sorumlulukları devam etmektedir. Nitekim Avrupa'da pek çok ülkenin Kişisel Verileri Koruma Kurulları tarafından yaptırıma tâbi tutulan Clearview AI şirketi örneğinde, tüm internet kullanıcılarının sosyal medya ve diğer platformlarda paylaştığı fotoğrafların toplanarak biyometrik veritabanları oluşturulması, kişisel verilerin korunması hakkının ihlali olarak tespit edilmiştir. İnternette verilerini paylaşan kişilerin, bu verilerin Clearview AI ve benzeri şirketler tarafından kitlesel şekilde işleneceğini öngörmesi neredeyse imkânsızdır. Bu veriler, haklarında hiçbir suç şüphesi bulunmayan kişilerin bilgisi dahi bulunmadan biyometrik yüz tanıma sistemlerini besleyerek kolluk kuvvetleriyle paylaşılmıştır. Hukuki dayanağı olmayan ve kitlesel, orantısız müdahaleler içeren bu uygulamalar kuşkusuz ki hukuka aykırıdır[109].

Sınırsızca kişisel veri toplamaya elverişli teknolojiler açısından diğer bir sorun da veri doğruluğu ve güvenilirliği ilkelerinin karşılanmamasıdır. Bilgi kaynağının güvenilirliğinin değerlendirilmemesi ve verilerin bağlamından koparılarak işlenmesi, hatalı sonuçlara ve bireyler hakkında hukuka aykırı takip ve soruşturmalara yol açabilmektedir. Bu durum, özellikle pek çok farklı veritabanının birleştirilmesi ve güncel olmayan verilerle sistemlerin beslenmesi ile katlanarak artan riskler doğurmaktadır[110].

---

[108] EDBP, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 26 Nisan 2023, para. 72.

[109] CNIL Clearview Kararı, 17 Ekim 2022, Délibération de la formation restreinte n° SAN-2022-01917 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859?isSuggest=true. Erişim Tarihi: 31 Mart 2026, para. 64-67.

[110] EDPS, *Opinion 41/2023 on the Proposal for a Regulation on European Union labour market statistics on businesses*, 25 Eylül 2023, https://www.edps.europa.eu/system/files/2023-09/2023-0799_opinion_en.pdf, s.8, para. 18, Erişim Tarihi: 31 Mart 2026.

Çoğunlukla kişilerin haberi olmadan toplanan veriler, özellikle yapay zekâ destekli gözetim sistemlerinde uzun süre fark edilmeden kullanılabilmektedir. Bu durum, IMSI yakalayıcılar gibi araçlarla sınırsız veri toplanmasının, hatalı profillerin, yanlış veri eşleşmelerinin önüne geçmeyi zorlaştırır. Bu nedenle, bireylerin veri işleme faaliyetlerinden haberdar olmasını ve bu süreçleri denetleme imkânına sahip olmasını sağlayacak mekanizmalar, gözetim teknolojilerine karşı önemli bir koruma katmanı oluşturmaktadır. Veri işleyen kurumlara ve veri koruma otoritelerine bilgi alma ve şikayet amaçlı başvuru hakkı, gözetim faaliyetlerinin görünür ve denetlenebilir olmasını temin eder.

Veri koruma hukuku, özellikle bilgilendirme ve erişim hakkı gibi güvenceler aracılığıyla bireylerin veri işleme faaliyetlerinden haberdar olmasını amaçlasa da, kamu güvenliği, soruşturmanın gizliliği gibi nedenlerle bu hakların kullanımı sınırlanabilmektedir. Nitekim uygulamada, bireylerin kolluk makamları tarafından haklarında hangi verilerin işlendiğini öğrenmeleri oldukça güçtür. Bu durum, hukuka aykırı, yanlış veya eksik veriler temelinde oluşturulan profillerin uygulamaların önüne geçmeyi zorlaştırmaktadır.

Ancak veri işlemenin adil olması ilkesi, kişilerin veri işleme sürecine ilişkin risklerden, güvencelerden ve bu süreçte sahip oldukları haklardan tamamen mahrum olmamasını gerektirir[111]. Nitekim Kolluk Direktifi, soruşturmanın amacının tehlikeye düşmemesi gibi gerekçelerle bilgilendirme ve erişim haklarının sınırlanmasına izin verse de, hakları kısıtlanan bireylerin, kişisel verileri koruma kurumlarına başvurarak dolaylı yoldan bilgi edinmesini mümkün kılmaktadır[112]. Bilgi ve erişim hakları sınırlandığında, bu başvuru Kişisel Verileri Koruma Kurullarına yapılacak genel şikâyet hakkına ek ve ayrı bir yol olarak öngörülmüş olup[113], sürecin bağımsız bir kurum tarafından gözden geçirilmesini ve hukuki güvence sağlanmasını temin eder[114].

Sonuç olarak, Avrupa veri koruma hukuku, gözetim teknolojilerinin sunduğu imkânlar ile temel hak ve özgürlükler arasındaki dengeyi her alanda kurmayı amaçlamakta ve kitlesel gözetim riskine karşı hukuki sınırlamalar getirmektedir. Ancak bu sınırlamaların etkili

---

111 EDPB, *Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive*, 02.02.2021, https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf, Erişim Tarihi: 31 Mart 2026, s. 13.

112 İlgili hak, Direktif kapsamında 17. maddede düzenlenmiştir. Buna göre üye devletler 17. madde kapsamında Kişisel Verileri Koruma Kurullarına başvuru hakkını düzenlemek zorundadır.

113 Article 29 Working Party, *Opinion on Some Key Issues of Law Enforcement Directive*, 07.12.2017, https://ec.europa.eu/newsroom/article29/items/610178/ens, s. 23, Erişim Tarihi: 31 Mart 2026. Bununla birlikte, kısıtlama kararlarının yargı yetkisi çerçevesinde bağımsız hâkimlikler ve mahkemeler tarafından verildiği durumlarda, Kişisel Verileri Koruma Kurulları tarafından bir denetim söz konusu olmayacaktır, bkz. Direktif, md. 45.

114 Juraj Sajfert, Terasa Quintel, Teresa, "Data Protection Directive (EU) 2016/680 For Police And Criminal Justice Authorities", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, 2019, Erişim Tarihi: 31 Mart 2025, s. 13.

olabilmesi, bireylerin bu hakların farkında olmasına ve söz konusu hakların etkin bir şekilde ileri sürülebileceği idari ve yargısal mekanizmaların yaratılmasına bağlıdır.

Türkiye'de Gözetim Teknolojilerine Dair Hukuki Çerçeve

Türkiye'de gözetim teknolojilerinin kullanımı ve sınırlandırılmasına dair hukuki düzenlemeler incelendiğinde, Avrupa Birliği Yapay Zekâ Yasası'ndan farklı olarak yapay zekâ temelli teknolojileri ele alan bütüncül bir düzenleme bulunmadığı görülmektedir[115]. Bu nedenle, yapay zekâ temelli gözetim teknolojilerinin geliştirilmesi ve kullanımına ilişkin bir çerçeve sunulmamıştır. Bu durum, özellikle yüz tanıma sistemleri, sosyal ağ analizleri veya iletişimin teknik araçlarla izlenmesi gibi uygulamaların hangi koşullarda ve ne şekilde kullanılabileceği konusunda belirsizliklerin devam etmesine neden olmaktadır.

Bununla birlikte, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)[116], GDPR ile benzer şekilde veri işlemenin hukuka uygunluğu, belirli ve meşru amaçlara dayanması, asgari veri işlenmesi ve doğruluk gibi temel ilkeleri içermektedir. Bu ilkelerin uygulamada gözetim teknolojileri üreten özel şirketlere karşı daha etkin şekilde işletilmesi gerekmektedir. Nitekim veri koruma rejiminin etkinliği, yalnızca normatif düzeyde var olmasına değil, bu hakların fiilen kullanılabilmesine bağlıdır.

Öte yandan KVKK'nın 28. maddesinde düzenlenen istisnalar, oldukça karmaşık bir yapı arz etmekte ve uygulamada kolluk faaliyetlerinin büyük ölçüde kanun kapsamı dışında kaldığı yönünde hatalı bir algıya yol açmaktadır. Oysa mevcut düzenleme dikkatli şekilde değerlendirildiğinde, gerek idari[117] gerek adli kolluk faaliyetlerinin kanun kapsamı dışında bırakılmadığı görülmektedir[118]. Nitekim Anayasa'nın 20. maddesi ve Türkiye'nin taraf olduğu Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi gereğince kişisel verileri koruma yükümlülüğü Türkiye'de veri işleyen tüm

---

[115] Ancak bu yönde çalışmalar sürmektedir, bkz. Yapay Zekâ Kanun Teklifi (Esas No. 2/2234) https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53, Erişim tarihi: 28 Mayıs 2026.

[116] Kanun No: 6698, Resmi Gazete T.: 07.04.2016, Sayı: 29677.

[117] Önleyici amaçlı veri işleme, KVKK md. 28/2 kapsamında ele alınmış olup, *suçun önlenmesine yönelik faaliyetlerin tamamen kanun dışı olmadığı belirtilmiştir***.** Hem md. 28/1'de hem de md. 28/2'de önleyici faaliyetlerden söz edilmesi karışıklığa yol açmış olsa da, 28/1 (ç) bendinde *ayrıca* düzenlenen faaliyetlerin klasik kolluk icraî işlemleri olmadığı, millî güvenlik ve istihbarata dair veri işleme süreçleri olduğu anlaşılmaktadır. Bu nedenle, PVSK kapsamında durdurma veya parmak izi ve fotoğraf işleme gibi önleyici kolluk uygulamaları md. 28/2 kapsamında değerlendirilmelidir.

[118] KVKK md. 28/1(d) uyarınca, soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin kişisel verilerin yalnızca *yargı makamları ve infaz mercileri tarafından işlenmesi* Kanun kapsamı dışında bırakılmıştır; buna karşın *adli amaçla kolluk tarafından işlenen veriler bu istisna kapsamına girmediğinden*, KVKK hükümleri adli kolluk açısından uygulanmaya devam etmektedir. Nitekim, Anayasa'nın 9. maddesi uyarınca "Yargı yetkisi, Türk Milleti adına bağımsız ve tarafsız mahkemelerce kullanılır" ve kolluk kuvvetleri bir yargı mercii değildir.

kurum ve kuruluşlar açısından devam etmektedir. Bununla birlikte, suç öncesi ve sonrası alanda bu korumanın nasıl sağlanacağının, Avrupa Kolluk Direktifi örneğinde olduğu gibi, alanın nitelikleri göz önünde bulundurularak ayrı ve belirlilik ilkesine daha uyumlu bir düzenlemeyle ele alınması daha yerinde olacaktır[119].

KVKK hükümlerinin kolluk tarafından işlenen verilere hangi kapsamda uygulanacağına ilişkin tartışmalar bulunmakla birlikte, Anayasa Mahkemesi ("AYM")'nin kişisel verilerin korunmasına ilişkin güvenceleri ceza muhakemesi hukuku bağlamında da özellikle dikkate aldığı görülmektedir. Bu yaklaşım, polise sanal ortamda internet abonelerine ait kimlik bilgilerine re'sen ulaşma ve araştırma yetkisi tanıyan PVSK Ek md. 6'ya eklenen hükme[120] ve bilgisayarlarda arama, kopyalama ile el koyma yetkisini düzenleyen CMK md. 134'e ilişkin iptal kararlarında, ilgili hükümlerin kişisel verilerin korunması ve özel hayatın gizliliği çerçevesinde ele alınmasıyla açık biçimde ortaya konmuştur[121].

Sanal ortamda takibe dair en can alıcı noktalardan biri, bu takip sırasında kişilerin politik görüşü, dinî inançları, sendika üyeliği gibi pek çok özel nitelikli kişisel veriye dair bilgi edinilebileceğidir. Twitter, TikTok ve Instagram gibi sanal ortamlarda kullanılacak önleyici kolluk yetkisi bu nedenle ancak açık kanuni düzenlemeler çerçevesinde kullanılabilir. Bu yetki, PVSK kapsamında "Polis, sanal ortamda işlenen suçlarda yetkili Cumhuriyet başsavcılığının tespiti amacıyla internet abonelerine ait kimlik bilgilerine ulaşmaya ve sanal ortamda araştırma yapmaya yetkilidir." şeklinde tanımlanmak istenmiş; ayrıca polise bu bilgileri erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcılarından talep etme imkânı tanınmıştır. AYM kolluğun sanal ortamda devriye yetkisine ilişkin söz konusu hükmü incelediği kararda, ilgili hükmü Anayasa'nın 20. maddesi kapsamında incelemiş ve "yetkili Cumhuriyet başsavcılığının belirlenmesi amacıyla yapılan sınırlamanın zorunlu bir toplumsal ihtiyaca karşılık gelmediği" sonucuna varmıştır [122].

İlgili maddenin iptali, yalnızca kişisel verilerin korunmasının dikkate alınması bakımından önem teşkil etmemektedir. Bu karar, ilgili verilerin ceza soruşturmasında kullanımını sınırlandırması açısından da önem taşımaktadır. Nitekim iptal kararı, polisin sanal ortamda herhangi bir yargısal veya idari denetime tâbi olmaksızın devriye faaliyeti yürütme

[119] Benzer yönde bkz. Baran Kızılırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", Kadir Has Üniversitesi Hukuk Fakültesi Dergisi, Cilt. 7, Sayı: 2, 2019, ss. 225 - 261, s. 258, Tuğçe Duygu Köksal, "Bilgi Toplamaya Yönelik İstihbari Kolluk Faaliyetine İnsan Hakları Perspektifinden Bakış", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 20, Sayı: 2, 2021, ss. 1745-1798, ss. 1765, 1766.

[120] AYM, E. 2018/91, K. 2020/10, T. 19.02.2020.

[121] AYM, E. 2023/128, K. 2026/36, T. 12.02.2026.

[122] AYM, E. 2023/128, K. 2026/36, T. 12.02.2026, § 101, 102.

yetkisinin bulunmadığını ortaya koymaktadır. Aksi yöndeki bir yorum, kolluğun internette paylaşım yapan ve sanal iz bırakan herkesi olağan şüpheli olarak değerlendirebilmesi ve sürekli gözetim altında tutulmasına yol açabilecektir.

Söz konusu iptal hükmüne rağmen, gazetecilerin "sanal devriye" faaliyetleri sonucunda elde edilen deliller temel alınarak soruşturmaya tâbi tutulduğu[123], sosyal medya hesaplarına erişim engeli getirildiği [124], hatta İçişleri Bakanı tarafından "suç ve suçlularla mücadele amacıyla internet ortamında 7/24 esasına göre sanal devriye faaliyetleri yürütülmektedir" şeklinde açıklamalar yapıldığı görülmektedir[125].

Bu bağlamda, internet ortamında idari kararla yasaklanmış bir toplantı ve gösteri yürüyüşüne ilişkin paylaşım yapan kişiler, hâlâ sanal devriye faaliyetleri sonucunda elde edilen deliller doğrultusunda "halkı kin ve düşmanlığa tahrik" (TCK md. 216) ve "suç işlemeye tahrik" (TCK md. 214) gibi suçlamalarla soruşturmaya tâbi tutulmakta[126], soruşturmalarda kolluk tarafından elde edilen sosyal medya paylaşımlarına ilişkin "açık kaynak araştırması" raporları ve ilişkilendirme tutanakları ile iddianame düzenlenmektedir[127.] Açık kaynak araştırmalarında, sosyal medyada yer alan açık paylaşımlar ve dolayısıyla aktiviteler izlenerek elde edilen bilgiler fezlekeye dönüştürülerek savcılık makamına sunulmakta, oysa bu delil elde etme yönteminin yasal dayanağını bulunmamaktadır[128].

Kolluğun sanal ortamda devriye yetkisini öngören açık ve geçerli bir düzenleme bulunmamasının yanı sıra, mevcut diğer bazı yetkilerin de günümüzde gözetim teknolojilerinin sağladığı neredeyse sınırsız imkânlar karşısında, kişisel verilerin

---

123 Medya ve Hukuk Çalışmaları Derneği "AYM'nin İptal Ettiği 'Sanal Devriye'den Soruşturma Açılan Gazeteci Arat Barış'a Takipsizlik", 12 Ağustos 2024, https://www.mlsaturkey.com/tr/aymnin-iptal-ettigi-sanal-devriyeden-sorusturma-acilan-gazeteci-arat-barisa-takipsizlik, Erişim tarihi: 28 Mayıs 2026.

124 Politika Haber, "AYM Kararı Hiçe Sayılıyor: 'Sanal Devriye'den 25 Hesaba Erişim Engeli", 17 Eylül 2025, https://politikahaber.com/aym-karari-hice-sayiliyor-sanal-devriyeden-25-hesaba-erisim-engeli/, Erişim tarihi: 28 Mayıs 2026.

125 Bia Haber Merkezi, "Bakan Ali Yerlikaya, AYM'nin İptal Ettiği 'Sanal Devriye' Yetkisini Kullanmaya Devam Ediyor", 20 Mart 2025, https://bianet.org/haber/bakan-ali-yerlikaya-aymnin-iptal-ettigi-sanal-devriye-yetkisini-kullanmaya-devam-ediyor-305634, Erişim tarihi: 28 Mayıs 2026.

126 Bkz. incelenen bir iddianamede şu ifadeler yer almaktadır: "... şüphelilerin açık kaynak araştırma raporu uyarınca kullanımınlarında olduğu tespit edilen sosyal medya hesapları üzerinden anılan toplantı ve gösteri yürüyüşünü yasaklayan mahiyetteki Valilik kararına karşın ısrarlı şekilde vatandaşları yasa dışı şekilde eylemlere ve sokak olaylarına katılmaları adına kışkırtıcı ve teşvik edici nitelikte olduğu değerlendirilen paylaşımlar yapmaları neticesinde üzerilerine atılı TCK 214/1 maddesinde hüküm altına alınan Suç İşlemeye Alanen Tahrik Etme suçunu işlediklerine dair haklarında kamu davası açılması için gereken yeterli şüpheyi oluşturmaya muktedir nitelikte delil elde edildiği…".

127 Tuğçe Duygu Köksal, "Bilgi Toplamaya Yönelik İstihbari Kolluk Faaliyetine İnsan Hakları Perspektifinden Bakış", *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, Cilt:20, Sayı:2, 2021, ss. 1780.

128 A.g.e.

korunması ve toplanma özgürlüğü gibi pek çok hak ve özgürlük bakımından yeniden değerlendirilmesi gerekmektedir. Nitekim en yakın tarihli AYM kararında Mahkeme, bilgisayarlarda arama, kopyalama ve el koyma yetkisini düzenleyen CMK md. 134 hükmünü, dijital ortamda saklanan verilerin yeniden kullanılma ihtimalini de dikkate alarak kişisel verilerin korunması kapsamında yeniden değerlendirmiştir. AYM, kişisel verilerin söz konusu soruşturma ve kovuşturma bakımından gerekli olmadığı durumlarda ne şekilde ve ne süreyle saklanacağı, toplandıkları amaç dışında kullanımının nasıl engelleneceği ve hakkında veri toplanan kişilerin haklarının ne şekilde güvence altına alınacağı hususlarının açık şekilde düzenlenmemesi nedeniyle ilgili hükmü iptal etmiştir[129]. Ayrıca Mahkeme, bu kararında Türkiye'de kolluğun veri toplamasına ilişkin ayrı bir düzenleme bulunmamasına rağmen, AB Kolluk Direktifi'ne atıf yaparak kişisel verilerin kolluk faaliyetleri ile soruşturma, kovuşturma ve infaz aşamalarında da korunması gerektiğini vurgulamaktadır. Aksi hâlde, ceza muhakemesi alanındaki düzenlemelerin Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkını ihlal edebileceğini ortaya koymaktadır[130].

Gözetim teknolojileriyle elde edilen verilerin ceza muhakemesi sürecinde delil olarak kullanılması, bu alanda farklı hak ve özgürlükleri de dikkate alan özel düzenlemelere duyulan ihtiyacı daha da acil kılmaktadır. Bu hukuki boşluk, bilişim sistemleri ve çevrimiçi alanda kullanılan tedbirlerin yanı sıra Türkiye'de sıkça başvurulan ve oldukça kanıksanan MOBESE sistemlerinde de somutlaşmaktadır. Ülke genelinde yaygın şekilde kullanılan MOBESE kameralarının kurulması, veri kaydetmesi ve bu verilerin saklanmasına ilişkin açık ve kapsamlı bir yasal düzenleme bulunmamaktadır[131]. Sonuç olarak, MOBESE ile veri işleme faaliyetleri, sürekli ve sınırsız biçimde, açık bir yasal temele dayanmaksızın yürütülmektedir.

Bu konudaki hukuki boşluk, yüz tanıma teknolojilerinin kamera sistemlerine entegre edilmesiyle daha da derinleşmektedir. Bu tür teknolojiler yalnızca bireylerin izlenmesini sağlamakla kalmaz, aynı zamanda biyometrik verilerin işlenmesine ve bu verilere dayanarak kimlik tespitine olanak tanır. Düzenlenmedikleri takdirde, bu uygulamalar belirli bir şüpheye dayanmak zorunda olmaksızın geniş kitlelere uygulanabilir ve hâkim denetimi dışında kalabilir. Bu yönüyle, aramanın, el koymanın veya iletişimin denetlenmesi

[129] A.g.e., §§ 62-66.

[130] A.g.e., § 63.

[131] Mevcut Ceza Muhakemesi Kanunu, Polis Vazife ve Salahiyet Kanunu ve Jandarma mevzuatı teknik izlemeye ilişkin hükümlerinin neden MOBESE kameralarına uygulanamayacağına dair, Hazan Dicle Özer, "MOBESE İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 24, Sayı: 1, s. 459-500, 2022, s. 485 vd, Tuğçe Duygu Köksal, "Bilgi Toplamaya Yönelik İstihbari Kolluk Faaliyetine İnsan Hakları Perspektifinden Bakış", 1756.

gibi geleneksel tedbirlerle kıyaslanması ve bu hükümlere kıyasen uygulanması mümkün değildir.

Benzer şekilde, internetten veri çekme *(web scraping)* ve IMSI yakalayıcı gibi araçların kullanımı da açık ve özel bir yasal düzenlemeye tâbi değildir. Oysa bu teknolojiler, önceki bölümlerde de detaylı şekilde ele alındığı üzere, sınırlanmadıkları takdirde kişisel verilerin korunması ilkelerine aykırılık teşkil etmektedir[132]. Gözetim teknolojileri yoluyla hukuki zemini bulunmaksızın ve kişisel verileri koruma normlarını ihlal ederek elde edilen verilerin ve bu verilere dayalı olarak ulaşılan sonuçların ceza muhakemesi hukuku bakımından hukuka aykırı kabul edilmesi gerekir[133]. Bu tür delillerin Ceza Muhakemesi Kanunu'nun hukuka aykırı delillere ilişkin düzenlemeleri uyarınca kullanılmaması ve hükme esas alınmaması gerekir[134].

Tüm bu nedenlerle, Türkiye'de gözetim teknolojilerinin kullanımına ilişkin açık, ayrıntılı ve teknolojiye özgü yasal düzenlemelerin yapılması; veri işleme süreçlerinin özellikle veri toplama anından itibaren kişisel verilerin korunması ilkelerine uygun hale getirilmesi ve bu alanın etkin denetime tâbi tutulması zorunludur. Nitekim hukuk düzeni bir bütün olduğundan, ceza hâkimleri, yüz tanıma veya sınırsız gözetim sistemleri yoluyla elde edilen delillerin hukuka uygunluğunu incelerken, veri işleme sürecinde KVKK hükümlerine uygunluğu da dikkate almak zorundadır. Bu bağlamda, söz konusu teknolojilerin kullanımını düzenleyen hukuki zeminin bulunmaması, farklı amaçlarla toplanan verilerin işlenmesi, veri işleme süreçlerinin şeffaf bir şekilde paylaşılmaması ve çoğunlukla gerçek bir denetimden geçirilmeden salt otomatik yollarla karar alınması, kişisel veriler mevzuatına aykırılık teşkil edecektir.

---

[132] Nitekim KVKK'nın 4. maddesi de açıkça verilerin ancak belirli, açık ve meşru amaçlar için, bu amaçla bağlantılı ve sınırlı olacak şekilde işlenebileceği belirtmektedir. Kitlesel gözetimi ve sınırsız veri işlenmesini mümkün kılan teknolojilerin bu temel ilkeleri ihlal ettiği açıktır.

[133] Anayasası'nın 38. maddesinin "kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez" ifadesi ile hukuka aykırı delillerin kullanılamayacağı anayasal niteliğine kavuşmuştur.

[134] Bkz. Anayasa md. 38, CMK md. 206/2-a, md. 217/2, md. 230/1-b ve md.289/1-i. Burada gözetim teknolojilerinin kullanımının kanuni düzenlemeyle öngörülmemiş olması kadar; bu verilerin çoğunlukla suç öncesi, önleyici bir faaliyet kapsamında idari yetkiler çerçevesinde elde edilmiş olmasına rağmen sonradan adli amaçla, iddianamelere dayanak teşkil eden delil olarak kullanılması da hukuka aykırıdır. Dolayısıyla, KVKK düzenlemelerine ek olarak, PVSK Ek Madde 7 uyarınca, önleyici amaçla toplanan verilerin adli amaçla kullanılması mümkün değildir. Dolayısıyla, suç oluşmadan önce veri toplayan bu teknolojilerin elde ettiği sonuçların soruşturma amacıyla kullanılması, PVSK hükümlerine de aykırılık teşkil eder.

Sonuç ve Öneriler

Kanun Koyuculara Yönelik Öneriler

KVKK hükümlerinin kısmen veya tamamen uygulanmamasına yol açan istisnai haller oldukça karmaşık bir yapıda düzenlenmiş, söz konusu istisnai hallerde kişisel verilerin korumasına ilişkin ek güvenceler öngörülmemiştir. Ancak kişisel verilerin korunması mevzuatlarının en temel hedeflerinden biri, devletlerin veri işleme etkinliklerinin ivme kazanmasıyla bireyler aleyhine bozulan dengeyi yeniden kurmaktır[135]. Bu nedenle veri işlemeye ilişkin temel ilkelerin hukuk devletinin tüm işlem ve eylemlerine uygulanması gerekir.

Suçu önleme, tespit ve infaz gibi amaçlar, nitelikleri gereği, özel koşullar ve sınırlamalar gerektirse de, veri işleme sürecinin bu koşullara uygun ve bireyler için uygun güvenceler öngörülerek düzenlenmesi gerekir. Nitekim Avrupa'da bu nedenle 2016/680 sayılı Direktif ile suçla mücadele ve ceza yargılaması kapsamında kişisel verilerin işlenmesi ayrıca düzenlenmiştir. Türkiye'de de benzer bir düzenleme gereksinimi bulunduğu açıktır. Bu eksiklik yalnızca veri koruma açısından değil, özellikle toplanma ve gösteri yürüyüşleri sırasında gözetim teknolojilerinin orantısız etkileri karşısında toplanma hakkının korunması açısından da önem taşımaktadır. Düzenlemeler, veri işleme süreçlerinin ilgili tüm temel hak ve özgürlüklere müdahalelerini dikkate alarak, orantısız uygulamaları önleyici, şeffaflığı teşvik eden ve yeterli güvenceler sunan hükümler içermelidir.

Bu bağlamda yalnızca fiziksel gözetim teknolojileri değil, internet verilerinin sınırsız şekilde toplanmasına imkân tanıyan teknolojiler de toplantı ve gösteri yürüyüşlerinin düzenlenmesine müdahale teşkil etmektedir. Bu nedenle, pek çok hakkı etkileyen ve örneğin açık kaynak istihbaratı toplama veya derin paket gözetimi gibi ayrım gözetmeksizin veri toplayan teknolojilere ilişkin özel düzenlemelere ihtiyaç duyulmaktadır.

Elbette bu düzenlemelerin yalnızca kolluk faaliyetleri çerçevesinde öngörülmesi yeterli olmayacaktır; birçok durumda söz konusu veriler, üçüncü taraf şirketler veya internet hizmet sağlayıcıları tarafından toplanmaktadır. Bu nedenle, öngörülecek kanuni sınırların çevresinden dolanılmasını önlemek için, üçüncü kişilerin internet gözetimi yapma yöntemleri, kapsamı ve süresi detaylı biçimde ele alınmalı; kolluğun üçüncü kişiler

[135] Elif Küzeci, Kişisel Verilerin Korunması, On İki Levha Yayınevi: İstanbul, Mayıs 2020, s. 383.

tarafından toplanan bu verilere erişimi ise ayrı ve sınırları belirlenmiş tedbir kapsamında düzenlenmelidir[136].

Yüz tanıma ve diğer biyometrik veya yapay zekâ tabanlı gözetim teknolojilerinin kullanımı da aynı ilkeler çerçevesinde ele alınmalıdır. Bu teknolojiler, KVKK ve Anayasa'daki temel haklar çerçevesinde, kanuni sınırlamalar, meşru amaçlar ve orantılılık ilkesi gözetilerek düzenlenmeli; hedef gözetmeksizin kullanılmaları Avrupa Yapay Zekâ Yasası'na benzer şekilde açıkça yasaklanmalıdır. Yine bu hususta AİHM'in *Glukhin v. Rusya* kararı, bu tür teknolojilere yönelik bir emsal teşkil etmekte olup, kararda Mahkeme, yüz tanıma sisteminin kullanımına ilişkin özel bir düzenleme bulunmaması nedeniyle özel hayatın gizliliğinin ihlal edildiğine hükmetmiştir[137]. Ele alınan kararlarda toplanma hakkına müdahale değerlendirilmemiş olsa da, bu teknolojilerin gözetim kapasitesi göz önünde bulundurulduğunda, hukuki boşlukların toplanma hakkını ihlal etme potansiyeli açıktır.

Avukatlar ve Hak Savunucuları İçin Öneriler

Toplanma hakkının etkin şekilde kullanılabilmesi ile kişisel verilerin korunması arasında doğrudan ve ayrılmaz bir ilişki bulunmaktadır. Bu nedenle savunma stratejileri yalnızca CMK hükümleri ile sınırlı tutulmamalı; KVKK ve genel veri koruma ilkeleri de ceza muhakemesi süreçlerine aktif biçimde dâhil edilmelidir. Özellikle AYM kararları dikkate alınarak, hukuka aykırı şekilde elde edilen kişisel verilerin, hukuka aykırı delil niteliği taşıdığı açıkça ileri sürülmeli; veri işleme sürecinin hukuki dayanağı, amacı ve ölçülülüğü somut olarak sorgulanmalıdır.

Bu kapsamda, kişilerin tespitinde kullanılan teknolojilere dair bilgi; bu teknolojilerin hangi veri setleriyle eğitildiği, hata oranları ve önyargı riskleri -bu hususta doğrudan bilgi alınamasa dahi- tartışma konusu yapılmalıdır. Bu teknolojilerin KVKK'ya uygun veri işleyip işlemediği, meşru amaç, asgari veri işleme ve doğru veri işleme gibi temel ilkelere uyulup uyulmadığı ceza yargılamasına taşınmalıdır. Aksi hâlde, veri toplama aşamasındaki hukuka aykırılıkların, bunlara dayanılarak elde edilen sonuçları da "zehirli ağacın meyvesi" hâline getireceği vurgulanmalıdır.

Savunma sürecinde, özellikle soruşturma aşamasında KVKK mekanizmalarının etkin kullanımı için daha geniş bir alan bulunmaktadır. Bu çerçevede, doğrudan kolluk

[136] İnternet trafik bilgilerine erişimin bir kolluk tedbiri olarak açıkça düzenlenmesi gerektigine ilişkin bkz. Fatih Birtek, "Ceza Muhakemesinde İnternet Trafik Bilgilerine Erişim ve İnternet Trafik Bilgilerinin Delil Değeri", *Hacettepe Hukuk Fakültesi Dergisi*, Cilt: 16, Sayı: 1, 2026, s. 56.

[137] AİHM, *Glukhin v. Rusya*, Başvuru no. 11519/20, Karar Tarihi: 04.10.2023.

birimlerine başvurarak ilgili kişilere ilişkin veri işlenip işlenmediği sorulmalı; yanıt alınamaması veya yetersiz yanıt verilmesi hâlinde ise Kişisel Verileri Koruma Kurumu'na başvurularak ikincil bir süreç işletilebileceği göz önünde bulundurulmalıdır[138]. Aynı şekilde, veri sorumlularının aydınlatma yükümlülüğü (md. 10), hakkında herhangi bir suç şüphesi bulunmayan kişilerin verilerini silme ve yok etme yükümlülüğü (md. 7) ile yabancı şirketlerin ürettiği teknolojilerin kullanımından şüphelenildiğinde yurt dışına veri aktarımına ilişkin kurallar (md. 9), somut olaylarda etkin şekilde uygulanmalıdır.

Gözetim teknolojilerinin çoğu zaman özel şirketler tarafından sağlandığı dikkate alındığında, veri ekosisteminin yalnızca kamu otoriteleriyle sınırlı olmadığı unutulmamalıdır. Bu nedenle KVKK nezdindeki haklar, doğrudan teknoloji üreten özel şirketlere karşı da ileri sürülebilir. Bu şirketlerin Avrupa menşeli olması hâlinde, ayrıca GDPR kapsamındaki haklar kullanılabilecektir. Özellikle erişim hakkı (GDPR md. 15) çerçevesinde yapılacak başvurularla, verilerin hangi amaçla işlendiği, kimlerle paylaşıldığı, ne kadar süre saklandığı ve kaynağı gibi kritik bilgiler Avrupa menşeli şirketten elde edilebilir[139]. Bu başvuruların yanıtsız bırakılması durumunda, şirketin ana merkezinin bulunduğu ülkenin veri koruma otoritesi nezdinde şikâyet hakkının kullanılması hem somut dosya açısından hem de ilgili şirketle ilgili daha geniş ölçekte farkındalık yaratılması bakımından önemlidir.

Bunun yanında, savunma pratiğinde yapay zekâ okuryazarlığının geliştirilmesi acil bir ihtiyaçtır. Barolar bünyesinde doğrudan pratik dosyalarda uygulanabilecek eğitim programlarının düzenlenmesi, pratik rehberlerin hazırlanması ve KVKK–CMK etkileşimine odaklanan uzmanlaşmanın artırılması gerekmektedir. Benzer davalarda ortaya çıkan sorunların, kullanılan teknolojilerin ve yargı kararlarının sistematik şekilde toplanması ve paylaşılması da savunma kapasitesini güçlendirecektir. Bu tür bir bilgi paylaşımı, net bir bilgi toplanamamış olsa dahi belirli teknolojilerin kullanıldığına dair dolaylı delil üretilmesine katkı sağlayacaktır.

Son olarak, dünyada gittikçe yaygınlaşan "veri adaleti" yaklaşımının da gösterdiği üzere, veri ve gözetim teknolojileri temelli hak ihlallerinin ortaya çıkarılması çoğu zaman uzun, zahmetli ve çok katmanlı bir süreci gerektirir. Farklı başvuru yollarının paralel şekilde kullanılması, ısrarlı bilgi talepleri ve stratejik davalama yöntemleri sayesinde, başlangıçta tamamen kapalı görünen veri işleme süreçleri dahi zamanla aydınlatılabilmektedir. Bu nedenle, her bir başvuru ve dava yalnızca bireysel bir hak arama aracı değil, aynı

[138] KVKK md. 11, md. 14.

[139] Romain Lanneau, *Data Protection Handbook on Asylum and Migration in Europe*, https://www.statewatch.org/media/5154/data-protection-handbook.pdf, 2025, Erişim Tarihi: 31 Mart 2026, s. 65.

zamanda daha geniş bir şeffaflık ve hesap verebilirlik mücadelesinin parçası olarak değerlendirilmelidir[140].

Sivil Toplum Kuruluşları İçin Öneriler

Gözetim teknolojilerine karşı etkili bir mücadelede sivil toplum kuruluşları kilit bir rol oynamaktadır. Bu kuruluşların süreklilik arz eden ve ulusötesi bağlantılar içeren stratejiler geliştirmesi büyük önem taşımaktadır.

Bu bağlamda ilk olarak, ulusal düzeyde faaliyet gösteren sivil toplum kuruluşlarının (STK) Privacy International, Access Now, European Digital Rights ve Electronic Frontier Foundation gibi gözetim teknolojileri alanında uzmanlaşmış uluslararası kuruluşlarla iş birliği yapması, hem teknik ve detaylı bilgiye erişimi hem de sınır aşan gözetim pratiklerinin takip edilmesini mümkün kılmaktadır.

Bunun yanı sıra, STK'ların gözetim teknolojilerine ilişkin bağımsız veri üretimi ve saha araştırma kapasitesi geliştirmesi gerekmektedir. Özellikle gözetim teknolojilerinin toplanma hakkına gerek caydırıcı gerek doğrudan etkisi üzerine çok az çalışma bulunmaktadır. Bu alanda farklı gruplarla görüşülerek bu teknolojilerin gündelik örgütlenme, eylem düzenleme veya düzenlenen eylemlere katılım üzerindeki etkilerini incelemek ve belgelendirmek önemli bir katkı sağlayacaktır[141].

Bunun yanı sıra Privacy International tarafından geliştirilen Surveillance Industry Index[142] (Gözetim Endüstrisi Endeksi) gibi çalışmalar, gözetim teknolojilerinin kimler tarafından üretildiği ve hangi ülkelere ihraç edildiğini ortaya koyarak önemli bir model sunmaktadır. Nitekim bu rapor kapsamında Türkiye'ye ithal edilen teknolojilerin

---

[140] Veri adaleti yaklaşımı üzerinden dünyada pek çok ülkede yürütülen mücadele ve hukuki süreçler için, bkz. David Leslie, Morgan Briggs, Antonella Perini, Smera Jayadeva, Cami Rincón, Noopur Raval, Abeba Birhane, Rosamund Powell, Michael Katell, ve Mhairi Aitken, *Data Justice Stories: A Repository of Case Studies*, Alan Turing Institute, 2022, https://arxiv.org/pdf/2204.03100, Erişim Tarihi: 1 Nisan 2026.

[141] Gözetimin bireyleri yalnızlaştırdığı ve toplanma hakkının temelini oluşturan iletişim, dayanışma ve katılım pratikleri üzerindeki etkisini inceleyen çarpıcı saha çalışmaları için bkz. Amory Starr, Luis Fernandez, Randall Amster, Lesley Wood, Manuel Caro, "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis", *Qualitative Sociology*, Cilt:31, Sayı:3, 2008, https://www.researchgate.net/publication/225348127_The_Impacts_of_State_Surveillance_on_Political_Assembly_and_Association_A_Socio-Legal_Analysis, Valerie Aston, "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives", *European Journal of Law and Technology*, Cilt: 8, Sayı: 1, 2017.

[142] Privacy International, *The Surveillance Industry Index: An Introduction*, https://privacyinternational.org/blog/1214/surveillance-industry-index-introduction, 18 Kasım 2023. Tüm dünyada takip edilen gözetim teknolojilerini geliştiren şirketler ve bu teknolojilerin içeriğine ilişkin rapor için bkz. Privacy International, *The Global Surveillance Industry,* https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

tespitinde ilgili STK kaynakları yol gösterici olmuştur. Privacy International, *Surveillance Industry Index* kapsamında topladığı verileri, literatür ve haber taramanın yanı sıra, hatta çoğunlukla, teknoloji fuarlarını takip etme, şirket broşürlerini toplama ve açık kaynak analizleri gibi sürekli yürütülen faaliyetler aracılığıyla elde etmiştir. Dolayısıyla STK'ların bu alan için kurumsal kapasite ve bütçe ayırması gerekmektedir. Elbette bu durum her STK için mümkün olmasa da, ortak çalışmalar ve bilgi alışverişi ile veri toplama süreçleri daha sürdürülebilir hale getirilebilir, farklı uzmanlık alanları bir araya getirilerek daha kapsamlı analizler üretilebilir ve sınırlı kaynakların daha verimli kullanılması sağlanabilir. Bu tür iş birlikleri aynı zamanda bulguların doğrulanabilirliğini artırarak daha güvenilir ve etkili savunuculuk faaliyetlerine zemin hazırlamaktadır.

Nitekim, sivil toplum, gazetecilik ve hukukçular arasındaki iş birliği, gözetim teknolojilerine karşı pek stratejik davanın başarısında belirleyici bir rol oynamıştır. Örneğin, *Big Brother Watch ve Diğerleri v. Birleşik Krallık* kararında[143] internet iletişiminin kitlesel şekilde takibinin özel hayatın gizliliği ve ifade özgürlüğü haklarının ihlal olarak tespit edilmesi, bu davaya öncülük eden Big Brother Watch, Amnesty International, Liberty ve Privacy International gibi sivil toplum kuruluşlarının çabalarının ortak bir sonucudur. Benzer şekilde, *Centrum för Rättvisa v. İsveç* kararında da istihbari amaçlarla yürütülen gizli sinyal takibi programlarının hukuka uygunluğu tartışılırken, kâr amacı gütmeyen Centrum för Rättvisa'nın iddiaları kararda temel alınmıştır[144].

Gözetim faaliyetlerinin doğası gereği gizli yürütülmesi, çoğu durumda doğrudan delil elde edilmesini zorlaştırmaktadır. Bu nedenle mahkemeler, bazı durumlarda gözetim yetkilerinin genişliği, kullanılan teknolojilerin bilinen zararları veya somut olaydaki diğer dolaylı delillere dayanabilmektedir. Bu çerçevede, sivil toplum kuruluşlarının dolaylı delil toplanması sürecine katkısı önem taşımaktadır.

STK'lar, aynı zamanda bağımsız bir toplumsal kapasite inşası potansiyeline sahiptir. Bu kapsamda, gözetim teknolojilerine karşı bilinç kazandırma ve rehberlik sağlama gibi çeşitli araçlarla, toplumun yapay zekâ okuryazarlığını artırmaları ve kişisel veriler konusunda farkındalık yaratmaları mümkündür[145].

---

[143] *Big Brother Watch ve Diğerleri v. Birleşik Krallık*, Başvuru no. 58170/13, 62322/14 ve 24960/15, Karar Tarihi: 25 Mayıs 2021.

[144] *Centrum för Rättvisa v. İsveç*, Başvuru no. 35252/08, Karar Tarihi: 25 Mayıs 2021.

[145] Bu kapsamda Electronic Frontier Foundation tarafından düzenlenmiş "Gözetime Karşı Meşru Müdahale El Kitabı" iyi bir örnek oluşturmaktadır, bkz. https://www.eff.org/pages/surveillance-self-defense. Bu tür rehberlerin Türkçe'ye çevrilmesi önemli bir katkıdır; EFF tarafından hazırlanan rehberin Türkçesi için bkz. https://ssd.eff.org/tr. Ayrıca, Alternatif Bilişim Derneği tarafından hazırlanan *Kem Gözlere Şiş Rehberi* de önemli bir zemin sunmaktadır: https://kemgozleresis.org.tr/tr. Dijital gözetime ilişkin rehberlerle ilgili detaylı bilgi için bkz. Ahmet Sabancı, "Dijital

Sonuç olarak, bu rapor Türkiye örneğine yoğunlaşmakla birlikte, gözetim teknolojilerinin küresel yönüne ilişkin bilgi sunmayı amaçlamıştır. Raporda ele alınan veriler, farklı aktörlerin sürecin yalnızca ulusal değil, ulusötesi boyutlarını da dikkate alarak birlikte hareket etmesinin gerekliliğini ortaya koymaktadır. Toplanma hakkına ve demokratik toplumun temel unsurlarına müdahale eden bu teknolojileri sınırlandırmak için gereken uzun soluklu mücadelede kuşkusuz ki öncelikle bu teknolojilere dair şeffaflık ve toplum genelinde farkındalığın oluşması, öngörülebilir kanunlar ve süreklilik gösteren ortak bir çaba gereklidir.

Gözetime Karşı Savunma Rehberleri: Neden İhtiyacımız Var? Nasıl Daha İyi Kullanılabilirler?", *Gözetim Toplumu [Panoptikon]* (Derleyenler: Barış Çoban, Bora Ataman), ss. 6171.