YAPAY ZEKÂ ARAÇLARININ GÖZETİM (SURVEILLANCE) AMAÇLI KULLANIMI VE MAHREMİYET HAKKININ İHLALİ

* Öğr. Gör. Av. Sena VURAL AÇANAL

Anahtar Kelimeler: Gözetim, Kişisel Veri, Mahremiyet, Yapay Zekâ

İstanbul Barosu Bilişim Hukuku Komisyonu
Yapay Zekâ Çalışma Grubu

GİRİŞ

Yapay zekâ teknolojilerinin gündelik hayatın birçok alanında kullanılmasıyla, gözetimin mahremiyeti ihlal edip etmediğine yönelik değerlendirmeler yalnızca kamusal alanlarda yürütülen devlet veya kolluk faaliyetleriyle sınırlı olmaktan çıkmıştır. Klasik anlamda kamusal alanda gerçekleştirilen gözetim zorlayıcı ve tek taraflı bir müdahale olarak değerlendirilmektedir. Günümüzde bireyler, üretken yapay zekâ araçları ve sanal asistanlarla kurdukları sürekli etkileşim aracılığıyla, kişisel verilerinin önemli bir bölümünü bizzat kendileri üretmekte ve veri havuzuna sunmaktadır. Çoğu zaman bireylerin farkında olmadan üretip sundukları bu veriler, kapsamlı analizlere konu olmaktadır.

Dijitalleşmenin yarattığı iletişim ve medya teknolojilerindeki gelişmeler sonucunda devletin en büyük görev ve sorumluluğunun, toplumun ve toplumu oluşturan bireylerin kişisel verilerini korumak olduğu ifade edilmektedir[1]. Hukuk devleti ilkesiyle demokratik usullerle yönetilen devletlerde devlet tüzel kişiliği, vatandaşlarına ait olan yasalarca belirlenmiş bir takım bilgi ve verilere ulaşma hakkına sahiptir. Bu ulaşma yetkisi, devlet işleyişinin sağlanması, kamu düzeninin ve güvenliğinin korunması amaçları doğrultusunda kullanılmalıdır. Devlet, yetkilerini bu doğrultuda kullandığı müddetçe vatandaşları üzerinde gözetim yetkisini meşru bir şekilde kullanmış olacaktır. Bunun yanı sıra bireylerin de dijital platformları kullanırken veriler sunması, gözetimin sınırlarının belirlenmesi ihtiyacını da gündeme getirmektedir. Gözetimin sınırlarının nasıl olması gerektiği değerlendirilirken gerek iç hukukta gerekse uluslararası hukuk sistemlerinde mahremiyet kavramı ön plana çıkmaktadır. Mahremiyetin klasik "özel alanın ihlali" anlayışının ötesine geçerek, bireyin kişisel verileri üzerindeki özerkliği ve kendisi hakkında çıkarım yapılmasına karşı korunması gereken bir değer olarak değerlendirilmesi gerekmektedir[2].

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile Türk hukukunda Kişisel Verilerin Korunması Kanunu (KVKK) tarafından benimsenen şeffaflık, amaçla sınırlılık, veri minimizasyonu ve rızanın şeklindeki temel ilkelerin yapay zeka modelleri tarafından gerçekleştirilen gözetim faaliyetlerinde de göz önünde bulundurulması gerekmektedir. Bu doğrultuda, yapay zekâ çağında mahremiyetin korunmasın, yalnızca kamusal gözetimin sınırlandırılmasıyla değil; aynı zamanda birey ile dijital platformlar arasındaki veri temelli ilişkinin de kapsama alınmasıyla mümkün olabilecektir.

* Maltepe Üniversitesi Meslek Yüksekokulu, Mahkeme Büro Hizmetleri Programı, senavural@maltepe.edu.tr

[1]Baturalp Yavuz, "Gözetim ve Mahremiyet Toplumu," *Yaşar Hukuk Dergisi* 4, sy. 2 (2022): 61.https://dergipark.org.tr/tr/pub/yhd/article/1150267 (Erişim Tarihi: 06.02.2026)

[2] Yavuz, s. 61-62.

1. Algoritmik Gözetim Çağı

Dijital teknolojilerin gelişimi, gözetim olgusunun kapsamını genişletmiştir. Klasik anlamda gözetim, belirli bir kişi veya alanın sınırlı süreyle izlenmesini[3] ifade etmektedir. Michel Foucault'nun panoptik gözetim modelinde[4], gözetim belirli mekân ve kişilere uygulanan sürekli bir faaliyet olarak ele alınmaktadır[5]. Yapay zekâ destekli gözetleme faaliyetleriyle birlikte gözetim; sürekli, otomatik ve çoğu zaman fark edilmeden gerçekleşen bir yapıya kavuşmuştur. Kameralar artık yalnızca kayıt almakla yetinmemekte; yüzleri tanımakta, davranışları analiz etmekte ve geleceğe yönelik tahminler üretmektedir[6]. Bu dönüşüm, kamu güvenliği ve suçla mücadele bakımından önemli imkânlar sunmakla birlikte, mahremiyet hakkı ve kişisel verilerin korunması konularını güncel bir mesele haline getirmiştir[7].

Yapay zekâ destekli gözetim sistemleri çok farklı biçimlerde karşımıza çıkmaktadır. En yaygın örneklerden biri yüz tanıma teknolojileridir. Bu sistemler, kamusal alanlardaki kameralar aracılığıyla elde edilen görüntüleri biyometrik veri olarak işleyerek kişilerin kimliğini tespit edebilmektedir. Örneğin eğitim verisi olarak daha önceden suç işlemiş kişilerin yüzlerinin öğretildiği otomatik polis robotu yapay zekâ, suçluların gerçek zamanlı olarak belirlenmesi ve yakalanmasında kullanılmaktadır[8]. Bunun yanı sıra ses tanıma, yürüyüş analizi, mimik ve duygu analizi gibi biyometrik yöntemler de giderek yaygınlaşmaktadır.

Bir diğer önemli alan ise davranış analizi ve öngörücü sistemlerdir. Yapay zekâ, bireylerin geçmiş hareketlerini ve davranış örüntülerini analiz ederek "şüpheli" davranışları önceden tespit etmeyi veya suç işleme riskini tahmin etmeyi amaçlayabilmektedir. Bu tür sistemler

[3] David Lyon, "Surveillance Studies: An Overview," *Canadian Journal of Sociology* 33, no. 2 (2008): 471 https://doi.org/10.29173/cjs2004

[4] Panoptikon, İngiliz filozof Jeremy Bentham'ın 1785 yılında tasarladığı hapishane mimarisi modelinin adıdır. Model, mahkûmları gözetlemeye elverişli olacak şekilde tasarlanmıştır. Betül Sabahçı, "Sanal Ortamlarda Panoptikon Kavramı ve Gözetim Toplumu", *Amasya Üniversitesi Sosyal Bilimler Dergisi (ASOBİD)*, sy. 13, (2023):111-134.

[5] Michel Foucault, *Discipline and Punish: The Birth of the Prison, çev. Alan Sheridan* (New York: Pantheon Books, 1977), 195-228.

[6] Sermin Asıl, "Yapay Zekâ Destekli Gözetim ile İlgili Çalışmaların Bibliyometrik Analizi," *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi* 27, sy. 4 (2025): 1419. https://doi.org/10.32709/akusosbil.1675072

[7] OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (Paris: OECD Publishing, 2025), https://doi.org/10.1787/795de142-en (Erişim Tarihi: 05.02.2026).

[8] "Railway's AI-Powered Face Recognition System Intercepts 'Hardcore Habitual Offenders'," *The Economic Times*, 6 Şubat 2026, https://economictimes.indiatimes.com/industry/transportation/railways/railways-ai-powered-face-recognition-system-intercepts-hardcore-habitual-offenders/articleshow/127888713.cms (Erişim Tarihi: 06.02.2026)

özellikle kolluk faaliyetlerinde (predictive policing) ve sınır güvenliğinde kullanılmaktadır[9].

Yapay zekâ destekli gözetim yalnızca devlet eliyle yürütülen faaliyetlerle sınırlı değildir. Özel sektör de işyeri güvenliği, çalışan performansının izlenmesi, müşteri davranışlarının analizi gibi amaçlarla bu teknolojilerden yararlanmaktadır. Sağlık alanında kullanılan yapay zekâ alt yapılı uygulamalar, klinik veriler üzerinden bireyler hakkında risk skoru oluşturmaktadır. Davranış analizleri sonucunda davranışsal öngörülerde bulunulmakta ve bu analizler doğrultusunda bireylerin gelecekteki eğilimlerini yönlendirmek üzere tedbirler alınmaktadır. Kullanıcılar mahremiyet ihlallerine rağmen dijital platformları kullanmaktan vazgeçememekte, etkileşim alma ve içerik paylaşımı yoluyla sistemin sürekliliğini beslemektedirler. Üretilen davranış verilerinin, yalnızca kişisel analizlerde değil, toplumsal analizlerde de kullanıldığı ifade edilmektedir[10]. Bu durum, bireylerin çoğu zaman açıkça farkında olmadan gözetim altında kalmasına ve rıza kavramının fiilen tartışmalı hâle gelmesine yol açmaktadır.

2. Mahremiyet Hakkının Hukuki Çerçevesi

Mahremiyet hakkı, kişinin kendisiyle ilgili bir bilgiyi paylaşıp paylaşmama hakkına, paylaşacaksa bunun ne zaman veya ne kadar paylaşacağını belirleme yetkisine sahip olması şeklinde tanımlanmıştır[11]. Devlet otoritesi, bireylerin yaşamlarını çeşitli şekillerde gözetim altında tutmaktadır. Modern toplumun kurumsallaşmasıyla birlikte gözetim de kaçınılmaz hale gelmiştir[12]. Gözetim faaliyeti, günümüzde internet ve özellikle yapay zekâ kullanımının yaygınlaşmasıyla türlü mahremiyet ihlallerinin doğmasına sebebiyet vermiştir.

Devletin gözetleme yetkisi, bireylerin mahremiyet hakkı çerçevesinde sınırlandırılmıştır. Anayasanın 17. maddesinde kişilerin yaşam hakkı yanında maddi ve manevi varlığını koruma ve geliştirme hakkının olduğu düzenlenmiştir. Anayasanın 22. maddesinde herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu

[9] Richard A. Berk, "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement", *Annual Reviey of Criminology* 4, (2021): 210. **https://doi.org/10.1146/annurev-criminol-051520-012342** (Erişim Tarihi: 03.03.2026)

[10] Asıl, s. 1422.

[11] Alan F. Westin, "Privacy and Freedom," *(1967):* 7. https://archive.org/details/privacyfreedom00west/page/6/mode/2up (Erişim Tarihi: 29.04.2026)

[12] Anthony Giddens, *Ulus Devlet ve Şiddet*, çev. Cumhur Atay (İstanbul: Kalkedon Yayınları, 2008), 197.

vurgulanmaktadır. Mahremiyet hakkı ise Anayasa'nın "Özel Hayatın Gizliliği" başlıklı 20. maddesiyle güvence altına alınmış olup, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkını ifade eder. Anayasanın 20. maddesine 2010 yılında eklenen 3. fıkra ile *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* şeklindeki düzenleme ile kişisel verilerin korunması mahremiyet hakkı kapsamında anayasal bir hak olarak düzenlenmiştir.

Mahremiyet hakkı, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. maddesinde de düzenlenmiştir. AİHM, gözetim faaliyetlerini bireyin konutu veya kamusal alan farketmeksizin özel hayatın gizliliği kapsamında ele almaktadır. Mahkeme, kamusal alanı da bireyin mahremiyeti kapsamında değerlendirmektedir. Örneğin 28 Ocak 2003 tarihli *Peck/Birleşik Krallık* kararında[13], intihar girişiminde bulunan Peck'e ait kamusal alanda çekilen kamera görüntülerinin geniş kitlelere yayılmasının özel hayatın ihlali oluşturduğuna hükmetmiştir. Yine benzer şekilde 4 Aralık 2008 tarihli *S. and Marper/Birleşik Krallık* kararında[14], suç isnadı ortadan kalkmış olan bireylerin, yalnızca kolluk ile teması bulunduğu gerekçesiyle biyometrik verilerinin (parmak izi ve DNA) süresiz olarak saklanmasının bireyin özel hayatı üzerinde ölçüsüz bir gözetime sebebiyet verdiği ifade edilerek bu durumun mahremiyet ihlali oluşturduğuna hükmedilmiştir.

Yapay zekâ destekli sistemlerin kimi zaman kullanıcı bakımından şeffaf olmaması mahremiyet ihlali açısından bireyler nezdinde öngörülemeyen bir takım sonuçlar doğmasına sebebiyet verebilmektedir. Bu, gözetimin her durumda hukuka aykırı bir eylem olduğu anlamına gelmemektedir. AİHM'in kararlarında gözetimin hukuka uygun kabul edilebilmesi için özel hayatın gizliliğine müdahalenin kanuni dayanağının

[13] *Peck v. United Kingdom*, no. 44647/98, ECHR 2003, 28 April 2003. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60898%22]} (Erişim Tarihi: 05.02.2026)

[14] *S. and Marper v. the United Kingdom [GC]*, no. 30562/04 and 30566/04, ECHR 2008, 4 December 2008. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]} (Erişim Tarihi: 05.02.2026)

bulunması, meşru bir amaç gütmesi, demokratik toplum gereklerine hizmet etmesi ve ölçülü olması gerektiği vurgulanmaktadır. Örneğin 28 Mayıs 2024 tarihli *Pietrzak and Bychawska-Siniarska and Others/ Polonya* kararında, Polonya'nın daimi gözetim mekanizmalarının AİHS'nin 8. maddesi ile güvence altına alınmış olan mahremiyeti ihlal ettiği vurgulanmıştır. Polonya'da kabul edilen bir takım yasa maddeleri iletişim verilerinin saklanması, operasyonel kontrol ve gizli gözetim yetkileri gibi geniş kapsamlı gözetimi mümkün kılmaktadır. AİHM verdiği ihlal kararında veri saklama ve söz konusu öngörülebilirlikten uzak denetimin ölçülülük ilkesine aykırı olduğunu ve demokratik toplum gerekliği kriterlerini karşılamadığını tespit etmiştir[15].

3. Gözetim Faaliyeti Kapsamında Kişisel Veri ve Biyometrik Verilerin İşlenmesi

Kişisel veri kavramı, 6698 sayılı Kişisel Verilerin Korunması Kanununun (KVKK) "Tanımlar" başlıklı m. 3/1-d maddesinde; "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlanmıştır. KVKK m.4'e göre kişisel verilerin işlenmesinde keyfiyete yer olmamakta, kişisel veriler ancak kanunlarda öngörülen usul ve esaslara uygun şekilde işlenebilmektedirler. KVKK m.4/2'de kişisel verilerin işlenmesinde mutlak surette gözetilmesi gereken ilkeler sayılmıştır. Buna göre kişisel veriler;

- Hukuka ve dürüstlük kurallarına uygun şekilde,
- Doğru ve güncel şekilde,
- Belirli, açık ve meşru amaçlar doğrultusunda,
- İşlendikleri amaca uygun şekilde sınırlı ve ölçülü,
- İşlemenin özgülendiği amacın gerçekleşmesi için gereken süre kadar muhafaza edilecek şekilde

işlenebilecektir. İşlemenin meşru amaçlar doğrultusunda ve ölçülü şekilde yapılması gerekliliği AİHM kararlarında da vurgulanmıştır. Örneğin bir kararında[16] AİHM, GPS ile kamusal alanda yapılan izlemenin özel hayata müdahale teşkil ettiğini kabul etmiş; ancak müdahaleyi yalnızca terörle mücadele gibi istisnai bir bağlamda, hedeflediği amaca uygun, süreyle sınırlı ve yargısal denetime tabi

[15] *Pietrzak and Bychawska-Siniarska and Others v. Poland*, no.72038/17 and 25237/18), ECHR 2024, 28 May 2024. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-14333%22]} (Erişim Tarihi: 05.02.2026)

[16] *Uzun v. Germany*, no. 35623/05, ECHR 2010, 2 December 2010. https://www.lawpluralism.unimib.it/en/oggetti/629-uzun-c-germania-n-35623-05-corte-edu-quinta-sezione-2-dicembre-2010 (Erişim Tarihi: 04.02.2025)

olması nedeniyle ölçülü bulmuştur. Bu durum, kamusal alandaki gözetimin kural olarak zorlayıcı ve tek taraflı bir müdahale olarak değerlendirildiğini; meşruiyetin ancak çok dar koşullar altında kabul edilebildiğini göstermektedir. Mahkeme'nin ihlal bulmamış olması, GPS gözetiminin normalleştiği anlamına gelmemekte; aksine bu tür müdahalelerin ancak istisnai güvenlik tehditleri karşısında tolere edilebileceğini ortaya koymaktadır.

Bireylerin kimliğini kesin veya kesine yakın sonuçla belirleyebilen fiziksel, fizyolojik veya davranışsal özellikler, biyolojik nitelikler kişisel veri olarak kabul edilmektedir[17]. Parmak izi, yüz tanıma sistemleri tarafından kullanılan yüz görüntüsü, retina taraması, avuç içi taraması ve DNA verileri fizyolojik biyometrik verilerdir. GDPR'a göre biyometrik veriler, bir gerçek kişinin fiziksel, fizyolojik veya davranışsal özellikleriyle ilgili belirli teknik işlemlerden elde edilen ve bu gerçek kişinin benzersiz bir şekilde tanımlanmasına olanak sağlayan veya bunu doğrulayan kişisel veriler şeklinde tanımlanmıştır[18]. KVKK m. 6'ya göre biyometrik genetik veri, özel nitelikli kişisel veri olarak kabul edilmekte olup, m. 6/3'te yer alan istisnalar haricinde özel nitelikli kişisel verilerin işlenmesi yasaktır. Bu nedenle hem KVKK hem de AB hukuku, biyometrik verilerin işlenmesini istisnai olarak kabul etmekte; açık rızanın bulunması, ölçülülük prensibinin gözetilmesi ve sıkı güvenlik önlemlerine dair kriterlerin sağlanmış olmasını aramaktadır. Biyometrik verilerin özel nitelikli kabul edilmesi, değiştirilemez nitelikte olmaları, sızdırıldığında oluşacak risklerin geri alınamayacak oluşu ve ayrımcılık riskini arttırabilecek olmasından kaynaklanmaktadır[19].

Davranışsal biyometrik veriler ise konuşma biçimi, yürüyüş biçimi, yazı veya imza dinamikleri, klavye kullanma alışkanlıkları (daktiloskopik alışkanlıklar) olarak sayılmaktadır[20]. Yapay zekâ kullanılarak yapılan gözetim faaliyetlerinde işlenen verilerin büyük çoğunluğu kişisel veri niteliğindedir. Bunların hem kamusal alanda hem de bireysel kullanım teşkil eden yapay zekâ kullanımlarında işlenmesi

[17] Göksu Hazar Erdinç, "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi," *Kişisel Verileri Koruma Dergisi* 2, sy. 1 (2020): 3. https://dergipark.org.tr/tr/pub/kvkd/article/738174#article_cite (Erişim Tarihi: 06.02.2026)

[18] Avrupa Birliği, *General Data Protection Regulation (GDPR),* Madde 4(14). https://gdpr-info.eu/art-4-gdpr/ (Erişim Tarihi: 05.02.2026)

[19] Melike Çiçek, "Türkiye'ye Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme", *Kişisel Verileri Koruma Dergisi* 6, sy.1 (2024): 55. https://izlik.org/JA78XL44UN (Erişim Tarihi: 02.03.2026)

[20] Ensar Arif Sağbaş ve Serkan Ballı, "Davranışsal Biyometri ve Makine Öğrenmesi Kullanılarak Akıllı Telefon Yetkilendirmesi Üzerine Kısa Bir İnceleme", *İzmir Katip Çelebi Üniversitesi II. Uluslararası Yapay Zeka ve Veri Bilimi Kongresi (ICADA) Bildiriler Kitabı,* (2022): 89- 92. https://icada.ikcu.edu.tr/Share/A273F0E77201D76B40364A0A75999B69 (Erişim Tarihi: 06.02.2026)

noktasında özellikle açık rıza kavramı ön plana çıkmaktadır. Kamusal alanlarda veya işyerlerinde yapay zekâ sistemleri kullanılarak gerçekleştirilen gözetim faaliyetlerinde bireylerin gerçekten özgür iradeleriyle rıza gösterip göstermedikleri sorgulanmaya başlamıştır[21].

Kişisel Verileri Koruma Kurulu, biyometrik veri işlenmesine ilişkin çeşitli kararlarında ölçülülük ve amaca uygunluk ilkelerine ilişkin kriterlerin karşılanıp karşılanmadığını değerlendirmektedir. Örneğin Kurul, çalışanların devam kontrolü amacıyla parmak izi ile puantaj takibi yapılmasını veya yüz tanıma sistemlerinin kullanılmasını konu alan kararlarında, mesai takibi için şifre veya ıslak imza gibi alternatif yöntemler varken biyometrik veri işlenmesini ölçülülük ve amaca uygunluk ilkelerine aykırı bulmuştur[22]. Bu kararlar, yapay zekâ destekli gözetim faaliyetlerinin her durumda kendiliğinden meşru kabul edilemeyeceğini ortaya koymaktadır. Gözetim faaliyetlerinin hukuka uygunluk değerlendirilmesinde veri minimizasyonu, ölçülülük, amaca uygunluk gibi kriterlerin göz önünde bulundurulması gerekmektedir. Kurul ayrıca kamera kayıtlarının saklanma süresi, erişim yetkileri ve amaçla sınırlılık ilkesi bakımından da veri sorumlularını sıkı biçimde denetlemektedir. Buna göre kişisel verilerin ilgili mevzuatta veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi bir ilke olarak kabul edilmiş olup kurul, kararlarında ilkenin ihlal edilip edilmediğini değerlendirmektedir[23]. Yapay zekâ sistemleriyle entegre kamera gözetiminin, bu ilkeleri ihlal etme riskinin daha yüksek olduğu açıktır.

4. AB Hukuku ve Yapay Zekâ Tüzüğü

Avrupa Birliği, yapay zekâya özgü ilk kapsamlı düzenleme olan Yapay Zekâ Tüzüğü (AI Act) ile özellikle biyometrik gözetim uygulamalarına sınırlamalar getirmeyi hedeflemektedir. Yapay Zeka Tüzüğü'nün 5(1)(h) maddesinde kamusal mekanlarda kolluk kuvvetlerinin amaçları (kaçırma, insan ticareti, kayıp kişilerin aranması, bireylerin yaşamına veya güvenliğe yönelmiş önemli bir tehdidin veya öngörülebilir bir terör tehdidinin önlenmesi gibi) dışında kalan gerekçelerle

[21] Murat Uzunparmak, "Dijital Gözetimin Kavramsal ve Hukuki Çerçevesi: Yapay Zeka Destekli Gözetim Sistemlerinin Anayasal Sınırları", *Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 27, sy. 3 (2025): 1094. https://doi.org/10.26745/ahbvuibfd.1754538

[22] KVKK, 01.12.2020 tarihli ve 2020/915 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6872/2020-915 (Erişim Tarihi: 04.02.2026), KVKK, 04.08.2022 tarihli ve 2022/797 sayılı Karar, https://www.kvkk.gov.tr/Icerik/7434/2022-797 (Erişim Tarihi: 04.02.2026).

[23] KVKK, 02.12.2018 tarihli ve 2018/142 sayılı Karar, https://www.kvkk.gov.tr/Icerik/5424/2018-142 (Erişim Tarihi: 04.02.2026).

gerçek zamanlı uzaktan biyometrik kimlik sistemlerinin kullanımının yasak olduğu düzenlenmiştir. Yine 5(3)–(7). maddelerde bu sistemlerin kolluk amaçlı kullanımının bağımsız idari otorite veya mahkeme tarafından verilebilecek yetkilendirme ile mümkün olabileceği, bu yetkilendirmenin amaç ve araç arasındaki ölçülülük gözetilerek yapılması gerektiği, üye devletlerin yetkilendirme prosedürlerine ilişkin düzenlemelerinde şeffaflık ve hukuki öngörülebilirliği gözetmeleri gerektiği, üye devletlerin veri koruma otoriteleri tarafından biyometrik tanımlama kullanımlarına ilişkin olarak Avrupa Komisyonu'na yıllık raporlar iletmeleri suretiyle denetime tabii tutulmaları hususları düzenlenmiştir. Yapay Zeka Tüzüğü'nün bu yaklaşımı, güvenlik gerekçe gösterilerek mahremiyetin mutlak olarak geri plana atılamayacağını göstermesi bakımından önemlidir.

Yapay zekâ modelleri kullanılarak gerçekleştirilen gözetleme faaliyeti devlet, kolluk kuvveti, işveren tarafından kamusal alan gözetimi ve biyometrik tanıma amaçlarıyla üçüncü kişi gözetimi ekseninde gerçekleşmektedir. Bunun yanında bireylerin gönüllü bir şekilde yapay zekâ modellerini ve dijital platformları kullanması neticesinde üretilen veri üzerinde de bir gözetleme durumu söz konusu olmaktadır. Bu noktada artık klasik anlamda bir gözetlenen – gözetleyen ilişkisinden söz etmek yeterli olmayacaktır. Öyle ki bireyler artık dışsal bir şekilde gözetlenmeye maruz kalmamakta, kendisi doğrudan gözetim konusu veriyi üreten tarafta yer almaktadır. Gündelik hayatımızda kullandığımız chatbotlar, sağlık uygulamaları, yapay zekâ destekli kişisel asistanlar, üretken yapay zekâ araçları, kullanıcı ile gönüllü arasında aktif bir veri paylaşımı alanı oluşturmaktadır. Bu paylaşım sonucunda birey ile yapay zekâ modeli arasındaki sürekli etkileşim, yapay zekâ modelinin kullanıcı hakkında daha derin bir profil çıkarımı yapabilmesini olanaklı kılmaktadır. Bu halde artık klasik bir gözetlemeden ziyade katılımcı gözetim (participatory surveillance) şeklinde adlandırılan durum meydana gelmektedir. Katılımcı gözetim, hedef nüfusun doğrudan katılımıyla eyleme geçmek amacıyla veri alma ve iletme sürecinin karşılıklı olarak yürütüldüğü bir süreç olarak tanımlanmaktadır[24]. Bu derinlikte bir etkileşim sonucunda işlenen veriler yalnızca kişinin ismi, e-posta adresi veya IP adresi gibi klasik kişisel veriler ile sınırlı kalmamakta, bireyin yazdıkları, sordukları, yüklediği ses ve görüntüleri de

[24] Carrie McNeil vd., "The Landscape of Participatory Surveillance Systems Across the One Health Spectrum: Systematic Review," *JMIR Public Health and Surveillance* 8, no. 8 (2022): 2. https://doi.org/10.2196/38551

kapsamaktadır. Bu da yapay zekâ modelleri tarafından yapılan sınıflandırmalar ve analizler sonucunda bireyin düşünce şekli, ruh hali, hukuki veya tıbbi problemleri, ilgilendiği mesleki veya sosyal meseleler hakkında oldukça derin şekilde veri toplanmasını olanaklı kılmaktadır[25]. Bu verilerin büyük kısmı, kullanıcı tarafından doğrudan sunulmuyor olsa dahi, yapay zekâ modeli bunları çıkarım yoluyla (predictive ai) üretmektedir. Bu yolla elde edilen veriler özellikle büyük platformlar tarafından reklam, fiyatlandırma, içerik önceliklendirme, sigorta veya kredi risklerini belirleme gibi profil verileri oluşturmakta kullanılmaktadır.

Katılımcı gözetimin klasik gözetimden daha sakıncalı olarak değerlendirilmesinin en önemli sebebi dijital platformların veri işleme ve çıkarım süreçlerinin çoğu zaman şeffaf ve öngörülebilir olmamasıdır. Her ne kadar kullanıcıya ilk kullanım aşamasında "kullanım şartlarını kabul ediyorum" şeklinde beyanda bulunmaya olanak veren ve kolayca tıklanabilir bir arayüz sunuyor olsalar da bunlar genellikle çok uzun, teknik detaylı, kullanıcıya kabul etmekten başkaca bir alternatif sunmayan metinlerden ibaret olmaktadır. Buradaki rızanın, bireylere verileri üzerinde anlamlı bir kontrol sağlamadığı ifade edilmektedir[26]. Bu da, hem GDPR'daki özgür irade kriterini, hem de KVKK'daki aydınlatılmış onam anlayışını karşılamamaktadır. Bu tür bir gözetim, "amaçla sınırlılık" ilkesi bakımından da bir ihlal teşkil etmektedir.

95/46/EC sayılı Veri Koruma Direktifi'nin 29. maddesi uyarınca kurulan *Article 29 Working Party (WP29),* kullanıcıların uzun ve teknik kullanım şartları aracılığıyla verdikleri rızanın her zaman bilinçli ve özgür iradeye dayalı kabul edilemeyeceğini vurgulamış olup, bu yaklaşım daha sonra Avrupa Veri Koruma Kurulu rehberlerinde de sürdürülmüştür. Buna göre rızanın açık, özel ve aktif şekilde verilmesi gerekmektedir. Rıza sürecinde kullanıcıların üzerindeki bilişsel yükün azaltılması için basit ve anlaşılır bir dil kullanılmalıdır. Bunun yanı sıra kullanıcılara inceleme ve rıza geri çekme haklarının kolaylıkla sağlanması gerektiği vurgulanmaktadır. Özgür irade, menfaat dengesi, açık rıza vurgusu Madde 29'da spesifik bir madde içerisinde düzenlenmemiş olup, rehberde sürekli tekrar eden belirli bir yaklaşım olarak

[25] Thomas Ploug, "The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling", *Philos. Technol*. 36, no: 14 (2023): 1. https://doi.org/10.1007/s13347-023-00616-9

[26] Daniel J Solove, "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review* 126 (2013): 1880 https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications (Erişim Tarihi: 02.03.2026)

benimsenmiştir[27]. Mahremiyetin bireyin kişisel verileri üzerindeki kontrol yetkisi olarak tanımlanması (Westin, 1967), Avrupa Birliği hukukunda ilk olarak 95/46/EC sayılı Direktif ile normatif bir zemine kavuşmuş; ancak rızanın unsurları esas itibarıyla Article 29 Working Party'nin yorumlarıyla geliştirilmiştir. Nihayetinde GDPR'ın 4(11). maddesi ile birlikte rızanın özgürce verilmiş, belirli, bilgilendirilmiş ve açık bir irade beyanı şeklinde, aktif bir davranışla ortaya konulması zorunlu hale getirilmiştir

Yapay zekâ modelinin özgülendiği bir hizmetin sunulması amacıyla toplanan verilerin, yapay zekânın eğitimi ve ürün geliştirme amaçlarıyla üçüncü kişilerle paylaşım amacıyla kullanılması, gözetim amacına aykırılık meydana getirmektedir. Bu şekilde bir gözetim tam anlamıyla mahremiyet ihlali olarak nitelendirilemeyecek olsa dahi, kişisel alan sınırlarının ihlal edilmesi sonucunu doğurmaktadır. Birey her ne kadar kamerayla izlenmiyor, retinası taranmıyor veya parmak izi vermiyor olsa da tercihleri, alışkanlıkları ve zaafları sistematik bir şekilde ve arzusu dışında öngörülebilir ve yönlendirilebilir hale gelmektedir. Bir diğer anlatımla bireylerin yapay zekâ sistemlerini gönüllü olarak kullanması, gözetlemenin mahremiyeti ihlal etmeyeceği anlamına gelmemekte; aksine gözetimi daha görünmez, daha sürekli ve daha derin hâle getirmektedir. KVKK ve GDPR ilkeleri, yalnızca devlet veya işveren gözetimini platformların kullanmakta olduğu algoritmik veri işleme modellerini de kapsayan hukuki bir çerçeve teşkil ettiğinden, her durumda gözetilmelidir.

[27]European Commission, *Guidelines on Consent under Regulation* 2016/679 (wp259rev.01) https://ec.europa.eu/newsroom/article29/items/623051/en (Erişim Tarihi: 06.02.2026)

SONUÇ

Yapay zekâ destekli gözetim teknolojileri, modern toplumların kaçınılmaz bir gerçeği hâline gelmiştir. Ancak bu kaçınılmazlık, sınırsız ve denetimsiz bir gözetimi meşru kılmaz. Türkiye ve AB hukukunda mahremiyet hakkı ve kişisel verilerin korunmasına ilişkin mevcut ilkeler, yapay zekâ söz konusu olduğunda da geçerliliğini korumaktadır.

AİHM ve KVKK kararları birlikte değerlendirildiğinde, gözetimin ancak açık bir hukuki dayanağa sahip olması, ölçülü biçimde uygulanması ve etkili denetime tabi tutulması hâlinde kabul edilebilir olduğu görülmektedir. Yapay zekâ modellerinin şeffaflıktan uzak uygulamaları, karar alma süreçlerinin çoğu zaman açıklanamaması, hukuki denetimi zorlaştırmaktadır. Gözetim veya yapay zekânın kendisinin doğrudan zararlı olarak değerlendirilmesi ise isabetli olmayacaktır. Gözetimin gerçekleştiği bir toplumda teknolojinin varlığı değil; bu teknolojiyi kimin, hangi sınırlar içinde ve hangi denetim mekanizmalarıyla kullandığı önem arzetmektedir. Bu durum, hem idari hem de yargısal denetim mekanizmalarının güçlendirilmesini gerekli kılmaktadır.

TEŞEKKÜR

Bu çalışmanın akademik incelemesinde sunduğu değerli katkıları için Dr. Ayşenur Ocak'a teşekkür ederiz.

KAYNAKÇA

"Railway's AI-Powered Face Recognition System Intercepts 'Hardcore Habitual Offenders'." *The Economic Times*, 6 Şubat 2026.

Asıl, Sermin. "Yapay Zekâ Destekli Gözetim ile İlgili Çalışmaların Bibliyometrik Analizi." *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi* 27, sy. 4 (2025): 1418-1448. https://doi.org/10.32709/akusosbil.1675072

Berk, Richard A. "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement", *Annual Reviey of Criminology* 4, (2021): 209-237. https://doi.org/10.1146/annurev-criminol-051520-012342

Çiçek, Melike. "Türkiye'ye Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme." *Kişisel Verileri Koruma Dergisi* 6, sy.1 (2024): 54-76. https://izlik.org/JA78XL44UN

Erdinç, Göksu Hazar. "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi." *Kişisel Verileri Koruma Dergisi* 2, sy. 1 (2020): 1-19.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, Çeviren Alan Sheridan. New York: Pantheon Books, 1977.

Giddens, Anthony. *Ulus Devlet ve Şiddet*. Çeviren Cumhur Atay. İstanbul: Kalkedon Yayınları, 2008.

Lyon, David. "Surveillance Studies: An Overview." *Canadian Journal of Sociology* 33, no. 2 (2008): 471-474. https://doi.org/10.29173/cjs2004

McNeil, Carrie, S. Verlander, N. Divi ve M. Smolinski.)"The Landscape of Participatory Surveillance Systems Across the One Health Spectrum: Systematic Review." *JMIR Public Health and Surveillance* 8, no. 8 (2022): 2-12. https://doi.org/10.2196/38551

Ploug, Thomas. "The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling." *Philosophy & Technology* 36, no. 14 (2023): 1-22. https://doi.org/10.1007/s13347-023-00616-9.

Sabahçı, Betül. "Sanal Ortamlarda Panoptikon Kavramı ve Gözetim Toplumu." *Amasya Üniversitesi Sosyal Bilimler Dergisi (ASOBİD),* sy. 13 (2023):111-134.

Sağbaş, Ensar Arif ve Serkan Ballı. "Davranışsal Biyometri ve Makine Öğrenmesi Kullanılarak Akıllı Telefon Yetkilendirmesi Üzerine Kısa Bir İnceleme." *İzmir Katip Çelebi Üniversitesi II. Uluslararası Yapay Zeka ve Veri Bilimi Kongresi (ICADA) Bildiriler Kitabı.* (2022): 89- 92. https://icada.ikcu.edu.tr/Share/A273F0E77201D76B40364A0A75999B69

Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (2013): 1880-1903.

Uzunparmak, Murat. "Dijital Gözetimin Kavramsal ve Hukuki Çerçevesi: Yapay Zeka Destekli Gözetim Sistemlerinin Anayasal Sınırları." *Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 27, sy. 3 (2025): 1089-1116. https://doi.org/10.26745/ahbvuibfd.1754538

Westin, Alan F. *Privacy and Freedom.* Atheneum Newyork, 1967.

Yavuz, Baturalp. "Gözetim ve Mahremiyet Toplumu." *Yaşar Hukuk Dergisi* 4, sy. 2 (2022): 60-82.

Yararlanılan Yargı Kararları ve Mevzuat

Avrupa Birliği. *General Data Protection Regulation (GDPR).* Regulation (EU) 2016/679.

Avrupa İnsan Hakları Mahkemesi. *Peck v. United Kingdom.* Başvuru No. 44647/98. 28 Ocak 2003.

Avrupa İnsan Hakları Mahkemesi. *Pietrzak and Bychawska-Siniarska and Others v. Poland.* Başvuru No. 72038/17 ve 25237/18. 2024.

Avrupa İnsan Hakları Mahkemesi. *S. and Marper v. United Kingdom.* Başvuru No. 30562/04 ve 30566/04. 4 Aralık 2008.

Avrupa İnsan Hakları Mahkemesi. *Uzun v. Germany.* Başvuru No. 35623/05. 2 Aralık 2010.

European Data Protection Board (EDPB). *Guidelines 05/2020 on Consent under Regulation 2016/679.* Version 1.1. 4 Mayıs 2020.

Kişisel Verileri Koruma Kurumu (KVKK). 01.12.2020 tarihli ve 2020/915 sayılı Karar.

Kişisel Verileri Koruma Kurumu (KVKK). 02.12.2018 tarihli ve 2018/142 sayılı Karar.

Kişisel Verileri Koruma Kurumu (KVKK). 04.08.2022 tarihli ve 2022/797 sayılı Karar.

OECD. *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions.* Paris: OECD Publishing, 2025.

İSTANBUL BAROSU

•

Bilişim Hukuku Komisyonu

•

Yapay Zekâ Çalışma Grubu

•

2026

Editör

Av. Nursena Çetingül