

DİJİTAL KAPİTALİZM ÇAĞINDA YAPAY ZEKÂ, GÖZETİM VE İNSAN HAKLARI: MAHREMİYETİN VE ÖZGÜRLÜĞÜN GELECEĞİ

Demet Şefika MANGIR*
ORCID ID: 0000-0002-2542-8551

Declaration*

Özet

Dijital kapitalizm çağında insan hakları ve özgürlüklerin korunması hem uluslararası hukuk hem de küresel politika açısından giderek daha kritik bir mesele haline gelmektedir. Yapay zekâ temelli gözetim sistemlerinin yaygınlaşmasıyla birlikte, bireylerin mahremiyeti, ifade özgürlüğü ve veri güvenliği gibi temel haklar, dijital altyapıların ekonomik ve siyasal işleyişi içinde yeniden tanımlanmaktadır. Bu çalışma, dijital kapitalizmin ekonomik mantığı ile gözetim teknolojilerinin toplumsal etkilerini kesiştiren kuramsal bir çerçeve sunarak, insan haklarının dijital çağda nasıl dönüşüme uğradığını incelemektedir. Sonuç olarak, gözetim kapitalizminin yıkıcı etkilerini önlemede mahremiyet yasalarının yeterli olmadığı, aynı zamanda kurumsal yapılar ve uluslararası hukuk düzenlemelerinde köklü reformlarla mümkün olabileceğini göstermektedir. Bu kapsamda çalışma, dijital haklar, algoritmik hesap verebilirlik ve veri egemenliği konularındaki küresel tartışmalara katkı sunmayı amaçlamaktadır. Ayrıca politika yapımcılar ve hukuk reformcuları için dijital gözetim karşısında bireysel özgürlükleri koruyacak normatif mekanizmaların geliştirilmesine teorik ve pratik bir temel oluşturmayı da amaçlamaktadır. Sonuç olarak makale, dijital kapitalizm çağında mahremiyetin, özgürlüğün ve insan onurunun geleceğine ilişkin bütüncül bir değerlendirme ortaya koymaktadır.

Anahtar Kelimeler: Dijital kapitalizm, İnsan hakları, Dijital mahremiyet, Uluslararası hukuk, Özgürlük.

* Doç. Dr., SÜ İİBF Uluslararası İlişkiler Bölümü, demetacar@selcuk.edu.tr.

* Bu çalışmada yapay zekâ araçlarından yalnızca dilsel düzenleme ve yazım kurallarının iyileştirilmesi ve yabancı dildeki metinlerin çevrilmesi amacıyla yararlanılmış olup, çalışmanın bilimsel içeriği, kuramsal çerçevesi ve sonuçları tamamen yazara aittir.



Abstract

In the age of digital capitalism, the protection of human rights and freedoms is becoming an increasingly critical issue in terms of both international law and global politics. With the proliferation of AI-based surveillance systems, fundamental rights such as individual privacy, freedom of expression, and data security are being redefined within the economic and political functioning of digital infrastructures. This study examines how human rights are transformed in the digital age by presenting a theoretical framework that intersects the economic logic of digital capitalism with the social impacts of surveillance technologies. Ultimately, it demonstrates that privacy laws alone are insufficient to prevent the destructive effects of surveillance capitalism and that this can only be achieved through fundamental reforms in institutional structures and international legal regulations. In this context, the study aims to contribute to global debates on digital rights, algorithmic accountability, and data sovereignty. It also aims to provide a theoretical and practical basis for policymakers and legal reformers to develop normative mechanisms that protect individual freedoms in the face of digital surveillance. Ultimately, the article presents a comprehensive assessment of the future of privacy, freedom, and human dignity in the age of digital capitalism.

169

Keywords: Digital capitalism, Human rights, Digital privacy, International law, Freedom.

Giriş

Dijital kapitalizm, verinin birincil bir sermaye biçimi olarak işlev kazandığı, bilgi ve iletişim teknolojilerinin yanı sıra ağ temelli platformların ekonomik faaliyetlerin merkezi hâline geldiği çağdaş bir kapitalizm türünü ifade etmektedir. Bu çerçevede Zuboff (2019), gözetim kapitalizmi “insan davranışlarının izlenip kaydedilmesinden, bu davranışların tahmin edilmesine ve nihayetinde kâr elde edilmesine yönelik yeni bir iktisadi mantık” olarak tanımlamaktadır. Söz konusu sistem yalnızca özel sektörle sınırlı kalmamış, devletler ve uluslararası kurumlar da bu yapının içine dahil olmuştur. Özellikle gözetim kapitalizmi artık sadece bir iş modeli olmanın ötesinde, düzenlemeler, ticaret kuralları ve güçlü devletler tarafından desteklenen kurumsal bir çerçeveye sahip küresel bir güç düzenidir. Bu nedenle, dijital ortamlarda toplanan veriler ve bu veriler üzerine geliştirilen algoritmalar, küresel güç ilişkilerinin yeniden yapılandırılmasında belirleyici bir rol oynamaktadır (Kilic & Carr-Ryan, 2025). Dolayısıyla, az sayıda teknoloji devinin -Amazon, Google, Meta, Alibaba, Tencent,



Huawei gibi- elinde toplanmış olan küresel teknoloji hegemonisi bu bağlamda, hükümetlerin egemenliğine rakip ya da bazen ondan daha güçlü bir etki alanına sahip olmuştur.

Bu bağlamda, dijital kapitalizmin kurumsal ve ekonomik boyutlarının ötesinde, toplumsal denetim ve bireysel özgürlük alanlarını da yeniden şekillendiren gözetim pratikleri ortaya çıkmıştır. Yapay zekâ destekli gözetim teknolojileri -yüz tanıma sistemlerinden öngörücü polislik algoritmalarına ve sosyal medya filtreleme mekanizmalarına kadar- devletlerin ve özel sektör aktörlerinin bireyleri izleme, sınıflandırma ve yönlendirme biçimlerini köklü bir şekilde dönüştürmektedir. Günümüzde gözetim, bir polislik aracından daha fazlasıdır, dijital dünyamızın altyapısal bir koşulu haline gelmiştir. Lyon'un (2017) da belirttiği üzere, gözetim kavramı tarihsel olarak şüphelilerin, mahkûmların veya potansiyel suçluların yakından gözlemlenmesi anlamında kullanılırken, dijital çağda bu anlam köklü bir dönüşüm geçirmiştir. Günümüzde gözetim, bireylerin izlenmesi, dijital platformlar aracılığıyla kişisel verilerin toplanması, işlenmesi ve ekonomik değer üretiminde kullanılması sürecini kapsamaktadır. Bu durum gözetimi artık kültürel ve ekonomik bir olguya dönüştürmüştür. Benzer biçimde Zuboff (2019), bu yeni aşamayı *gözetim kapitalizmi* olarak tanımlayarak, gözetimin iktidar pratiği olmasının ötesinde, bütün bir siyasi-ekonomik düzenin temeli hâline geldiğini vurgulamaktadır. Böylece gözetim, klasik anlamdaki kontrol mekanizmalarından çıkıp dijital kapitalizmin temel üretim mantığına dönüşmüştür.

170

Bu bağlamda, dijital kapitalizm iş modeli düzeyinden, ulusal güvenlik, ticaret politikaları ve platform düzenlemelerinin iç içe geçtiği stratejik bir alan haline gelmiştir. Birkaç büyük teknoloji şirketi veri, bulut altyapısı ve algoritmaları üzerinden küresel ölçekte standart belirleme gücünü elde ederken, başka ülkeler veya aktörler bu standartlara uyum sağlama ya da bağımsız alternatif geliştirme noktasında dezavantajlı konuma düşmektedir. Bu durum, dijital ekonomide eşitsizliklerin derinleşmesine ve hegemonya mücadelelerinin sanal ortama taşınmasına olanak tanımaktadır. Dolayısıyla, dijital kapitalizm çerçevesinde az sayıda büyük aktör tarafından kontrol edilen veri ve altyapılar hem ekonomik hem siyasal düzeyde küresel adaletsizlikleri artırma potansiyeli taşımakta, uluslararası sistemde yeni hegemonik ilişkilerin temelini atmaktadır. Böylece küresel kapitalizmin dijitalleşme süreciyle birlikte üretim ilişkilerinin temelinde yaşanan dönüşüm, günümüz kapitalizmini artık klasik üretim ve emek sömürsü biçimlerinden ziyade veri, algoritma ve dijital altyapı sahipliği üzerinden değer üreten bir sistemin parçası haline getirmiştir. Bu yeni evre, *dijital platform kapitalizmi* ya da *rant kapitalizmi* olarak adlandırılmaktadır (Özlük, 2023). Dijital kapitalizmin temelinde, üretim veri akışının ve algoritmik yönlendirme kapasitesinin kontrolü yer almakta, dolayısıyla



ekonomik güç, üretimden ziyade bilgi tekellerinden doğmaktadır. Bu yeni ekonomik düzende, bireylerin davranışları, tercihleri ve iletişim biçimleri sürekli olarak izlenmekte, kaydedilmekte ve ekonomik değere dönüştürülmektedir.

Günümüzde kişisel veriler her yerde toplanmakta, analiz edilmekte ve giderek daha fazla biçimde davranış tahmini amacıyla kullanılmaktadır. Bu durum, bireylerin mahremiyetinin ötesinde, ifade, düşünce ve bilgi özgürlüğü gibi diğer temel hakların korunması açısından da ciddi sorular doğurmaktadır. Avrupa hukuku bu gelişmeye güçlü bir yanıt vermiştir: Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin korunmasını bir temel hak olarak tanımakta ve bu hakkın diğer özgürlüklerle dengelenmesi gerektiğini açıkça belirtmektedir. GDPR'nin 1. gerekçesinde (Recital 1) veri koruma hakkının temel bir hak olduğu vurgulanırken, 4. gerekçede (Recital 4) bu hakkın mutlak olmadığı, düşünce, ifade ve bilgi özgürlüğü gibi diğer haklarla uyum içinde uygulanması gerektiği ifade edilmektedir. Bu nedenle GDPR, veri gizliliğini koruyarak ifade ve bilgi özgürlüğü hakkı da dahil olmak üzere diğer AB temel haklarını destekleyen bütüncül bir yaklaşım benimsemektedir (European Union, 2016, Recital 1, Recital 4, Article 85). Benzer şekilde, Avrupa İnsan Hakları Sözleşmesi (AİHS/ECHR, 1950) bireylerin özel hayatına saygı hakkını (Madde 8) ve ifade özgürlüğünü (Madde 10) güvence altına almaktadır. Ancak gelişmiş yapay zekâ temelli gözetim sistemleri, bu güvenceleri yeni sınamalarla karşı karşıya bırakmaktadır. AİHM içtihadına göre (örneğin Big Brother Watch and Others v. the United Kingdom, ECHR 2021), kitle gözetimi uygulamaları kişisel verilerin orantısız biçimde toplanması yoluyla Madde 8 kapsamındaki özel hayat hakkını ihlal edebilmektedir. Benzer biçimde, algoritmik profillemeye ve otomatik sınıflandırma süreçleri bireyleri şeffaf olmayan kriterlerle kategorize ederek ifade ve bilgi edinme özgürlükleri üzerinde caydırıcı bir etki yaratabilmektedir. Avrupa Konseyi'nin Mass Surveillance Factsheet (ECHR, 2023) belgesinde de belirtildiği gibi, bu tür uygulamalar AİHS'nin 8. ve 10. maddeleri arasında hassas bir denge kurulmasını zorunlu kılmaktadır. Dolayısıyla, yapay zekâ destekli gözetimin gelişimi, mahremiyetin ve ifade özgürlüğünün korunması açısından Avrupa insan hakları sisteminin temel ilkelerini yeniden değerlendirmeyi gerektirmektedir.

Yapay zeka destekli gözetim teknolojileri, mahremiyet, ifade özgürlüğü ve eşit muamele ilkelerini ciddi biçimde tehdit edebilmektedir. Özellikle otomatik içerik filtreleme ve sosyal kredi sistemleri aracılığıyla, demokratik toplumlarda ifade özgürlüğü ve eşit muamele ilkeleri üzerinde karmaşık sonuçlar doğurmaktadır. Otomatik içerik filtreleri, dijital platformlarda yasa dışı veya zararlı içerikleri önleme amacı taşımakla birlikte, bağlamı tam olarak



değerlendiremedikleri için sıklıkla eleştirel veya muhalif söylemleri yanlışlıkla bastırabilmektedir. Bu durum, algoritmik sansür olarak adlandırılan ve ifade özgürlüğünü dolaylı biçimde kısıtlayan yeni bir olguyu ortaya çıkarmaktadır (Article 19, 2018, Yeung, 2018). Benzer biçimde, Çin’de uygulanan sosyal kredi sistemleri, vatandaşların çevrimiçi ve çevrimdışı davranışlarını değerlendirerek bir güven puanı üretmekte, bu puan bireylerin kamu hizmetlerine erişimini, istihdam fırsatlarını veya sosyal statüsünü etkileyebilmektedir. Ancak bu sistemler, hangi davranışların *iyi* veya *kötü* olarak tanımlandığına dair şeffaflık eksikliği nedeniyle politik uyum ve öz-sansür eğilimini teşvik edebilmekte ve azınlık gruplarını orantısız biçimde etkileyebilmektedir (Drinhausen & Brussee, 2021, Citron & Pasquale, 2014). Her iki örnek de, yapay zekâ sistemlerinin teknik önyargı ve veri temelli karar verme süreçleri aracılığıyla, demokratik katılımı ve temel hakları istemeden zayıflatma potansiyeline sahip olduğunu göstermektedir. Yeni dijital altyapıların uluslararası siyaseti dönüştürmesi bağlamında, veri ve ağ platformlarına yönelik hakimiyet yalnızca ekonomik düzeyle sınırlı kalmayıp, jeopolitik güç dengelerini de derinden etkilemektedir. Örneğin UNCTAD’ın Digital Economy Report 2021 adlı çalışmasında, veri-paylaşımı olmayan ya da çok sınırlı olan ülkelerin küresel dijital kazançlardan oldukça düşük pay aldığı belirtilmiş ve dijital ekonomide hâkimiyetin Kuzey Amerika ve Çin merkezli büyük platformlara kaydığına dikkat çekilmiştir.

172

Öte yandan yapay zeka destekli gözetim uygulamaları, kamu güvenliği ya da dolandırıcılıkla mücadele gibi meşru amaçlarla savunulabilir. Avrupa Birliği de bu tür ödünleşmelerle yakından ilgilenmektedir: önerilen AI Yasası (AI Act), yüksek riskli yapay zeka sistemlerini (örneğin işe alımda ya da kolluk uygulamalarında kullanılanları) özel denetim ve şeffaflık yükümlülüklerine tabi tutmayı hedeflerken, otomatik GDPR’nin Madde 22 kapsamında karar süreçlerini sınırlandırmakta ve insan müdahalesi, itiraz hakkı gibi koruyucu mekanizmalar içermektedir. Bu bağlamda, modern gözetimin yeniden şekillenmesiyle temel hakların korunması arasındaki gerilim, hukuk ve haklar açısından ele alınması gereken hayati bir meseledir. Dolayısıyla makale, ampirik bir araştırma sunmaktan ziyade kuramsal ve normatif analiz yoluyla dijital gözetimin insan hakları üzerindeki etkilerini tartışmaktadır. Bu nedenle çalışma üç kuramsal geleneğin kesişiminde konumlanmaktadır. Gözetim çalışmaları geleneği, yapay zekâ temelli izleme pratiklerinin nasıl işlediğini, yani gözetimin arkasındaki mekanizmaları, bilgi akışlarını ve güç dinamiklerini çözümlememize imkân tanımaktadır. Haklar teorisi geleneği, bu gözetim biçimlerinin ne zaman meşruluğunu yitirdiğine ilişkin normatif ölçütleri -gereklik, orantılılık ve insan onuru ilkeleri gibi- sağlamaktadır. Hukuk ve



teknoloji geleneği ise teknik kapasite ile hukuki denetim arasındaki yapısal boşlukları görünür kılarak, dijital çağda hesap verebilirliğin ve şeffaflığın nasıl sağlanabileceği sorusuna odaklanmaktadır. Bu üç gelenek birlikte, analizimizin kuramsal çerçevesini oluşturmakta ve bu çerçeve doğrultusunda, Avrupa hukuk sisteminin -özellikle AIHS, GDPR ve ilgili Avrupa Birliği Adalet Divanı (ABAD/CJEU) ile AIHM içtihatlarının- bu çok katmanlı zorluğa nasıl yanıt verdiği incelenecektir.

Dijital Kapitalizm, Gözetim ve Mahremiyetin Teorik Haritası

Makalenin kuramsal zemini, dijital kapitalizm, gözetim ve mahremiyet ilişkilerini açıklayan üç temel düşünsel geleneğin kesişiminde şekillenmektedir. Dijital kapitalizm, verinin birincil sermaye biçimi haline geldiği, bilgi teknolojileri ve algoritmik sistemlerin ekonomik üretim süreçlerinin merkezine yerleştiği yeni bir toplumsal-ekonomik düzendir. Bu yapı, piyasa dinamiklerini ve bilgi, iktidar ve gözetim ilişkilerini yeniden biçimlendirerek bireylerin mahremiyet alanlarını ekonomik değer üretiminin bir parçası hâline getirmektedir. Gözetim kuramı, yapay zekâ temelli izleme biçimlerinin ardındaki bilgi akışlarını, iktidar ilişkilerini ve davranışsal yönlendirme mekanizmalarını çözümleyerek dijital kapitalizmin gözetim mantığını açığa çıkarır. Haklar kuramı, bu gözetim yapılarının meşruiyet sınırlarını belirleyen normatif ilkeleri -özellikle gereklilik, orantılılık ve insan onuru ölçütlerini- tanımlayarak dijital mahremiyetin korunmasına teorik bir dayanak oluşturur. Hukuk ve teknoloji yaklaşımı ise dijital çağda kod, algoritma ve hukuk arasındaki karşılıklı etkileşimi inceleyerek teknik altyapıların normatif düzen üretme kapasitesini ve hukukun bu alanı düzenleme gücünün sınırlarını tartışır. Bu üç kuramsal çizgi birlikte ele alındığında, dijital kapitalizmin ekonomik mantığı, gözetimin iktidar biçimleri ve mahremiyetin normatif sınırları arasındaki ilişkileri bütüncül biçimde çözümleyen bir teorik çerçeve ortaya çıkmaktadır.

Yapay zekâ, dijital kapitalizm bağlamında yeni bir üretim faktörü olarak çapraz sektörel yayılım kabiliyeti olan genel amaçlı bir teknoloji olarak kavramsallaştırılmaktadır. Yapay zekanın üretim süreçlerine entegrasyonu arttıkça iş modellerinin, gelir dağılımının ve sermaye formasyonunun köklü biçimde değişeceği öngörülmektedir. Gerçekten de, sanayi ve hizmet alanlarında otomasyon, makine öğrenimi ve veri-yoğun algoritmalar metalaşmış emek biçimleriyle birlikte ekonomik büyümenin yeni lokomotifleri hâline gelmektedir. Bu bağlama uygun olarak, yapay zeka patent sayıları ile uzun dönem ekonomik büyüme arasında pozitif ve istatistiki olarak anlamlı bir ilişki tespit edilmiştir, özellikle gelişmiş ekonomilerde bu etki daha güçlü gözlemlenmektedir. Bu dönüşümün ardında yatan dinamikler arasında veri ve



hesaplama gücü yoğunlaşması, yani büyük teknoloji firmalarının devasa veri setlerine erişimi ve bulut altyapısı kontrolü ile üst düzey yapay zeka personeline sahip oluşu yer almaktadır. Dolayısıyla eleştirel siyasal ekonomi literatüründe, bu yapı yapay zeka kapitalizmi olarak tanımlanmakta ve veri sömürüsü, ticarileştirme ve kazanan her şeyi alır (winner-takes-all) mantığı çerçevesinde değerlendirilmektedir (Gonzales, 2023).

Günümüzde yapay zeka destekli gözetim sorununa yaklaşımda, Foucault'nun disipliner toplum kavramı, Zuboff'un teknolojik gözetim kapitalizmi analizi ve Lyon'un gözetimin toplumsal boyutlarına vurgu yapan perspektifleri önemli kavramsal çerçeveler sunmaktadır. Bu nedenle bu kuramsal perspektiflerden yola çıkılarak yapay zeka çağında gözetimin nasıl yeniden üretildiği ve klasik teorilerle hangi noktalarda örtüştüğünün analiz edilmesi gerekmektedir. Bu bağlamda klasik gözetim teorisi yapay zeka çağında da önemini korumaktadır. Michel Foucault, *Discipline and Punish: The Birth of the Prison* adlı eserinde Jeremy Bentham (1995)'ın panoptikon modelini bir metafor olarak ele almakta ve modern disiplin toplumunun iktidar yapısını bu çerçeveden okumaktadır. Foucault (1977), gözetim mimarisinin işleyişini "...merkezdeki gözetleme kulesi tüm hücreleri görebilir, fakat gözetlenenler kimin onları izlediğini bilemez" şeklinde betimlemektedir. Dolayısıyla bu yapı, bilinçli ve kalıcı bir görünürlük durumu yaratırken, bireyler her an izlenme ihtimalini dikkate alarak davranışlarını düzenleyebilmektedir. Aslında Foucault'nun Bentham'ın Panopticon'u üzerine yaptığı analiz, asimetrik görünürlüğün nasıl öz disiplini teşvik ettiğini vurguladığını göstermektedir. Burada, gözetimin fiziksel bir sürekliliğe sahip olmasa bile algılanan olasılıkla bireylerin içsel denetim geliştirmesi, ceza mimarisinin, norm üretimi, disiplin ve iktidar-bilgi ilişkisinin kodlandığı bir sistemdir. Günümüzün dijital panoptikonu ise yaygın ve her yerde mevcuttur. Bireyleri hiçbir insan operatör aktif olarak izlemiyor olsa bile kameralar, dronlar, sosyal medya izleme ve biyometrik sensörler tarafından izlenmektedir.

Shoshana Zuboff'un *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* adlı eseri de, dijital platformların kullanıcı davranışlarını veri olarak sermayeleştirme süreçlerini incelemektedir. Zuboff'un temel iddialarından biri, kullanıcı davranışlarının *gözetim varlıkları* hâline gelmesidir, bu varlıklar algoritmalar aracılığıyla analiz edilir ve geleceğe dair tahmin modellerine dönüştürülür. Bu bağlamda, klasik iktidar modellerinden farklı olarak, davranışsal müdahale odaklı bir *enstrümantarya iktidar* kavramını geliştirmiştir. Bu iktidar biçimi, baskı ya da açık zor kullanımı yerine detaylı bir şekilde yapılandırılmış tekniklerle bireylerin seçim mekanizmalarını yönlendirmeye odaklanmaktadır. Dolayısıyla, Zuboff'un yaklaşımı, Foucault'nun norm



üretimi ve iktidar-bilgi ilişkisinin dijital bağlamda yeniden kodlandığını göstermektedir. Bu durumu *epistemik darbe* olarak adlandırmakta, çünkü bilme yetisi -yani hangi davranışların bekleneceği, hangi müdahalelerin yapılacağı- artık teknolojik aktörlerin eline geçmiştir (Zuboff, 2019). Bu bağlamda bireyler verinin üreticisi ve aynı zamanda deneği konumuna gelmişlerdir.

Gözetim çalışmalarına katkıda bulunan önemli bir kuramcı olan Lyon, gözetimi toplumsal süreçlerle iç içe geçen bir fenomen olarak ele almaktadır. Lyon'a göre gözetim, bireysel verilerin toplanmasından öte, bu verilerin sınıflandırılması, sıralanması ve bu sıralamaya göre müdahale edilmesi süreçlerini içermektedir. Bu süreç Lyon tarafından *sosyal sıralama* olarak kavramsallaştırmıştır. Lyon, gözetim süreçlerinde devletin yanı sıra özel aktörlerin, kurumsal yapıların ve bireylerin de önemli roller oynadığını vurgulayarak, gözetim yapılarının çok katmanlı ağlar şeklinde işlediğini ve mekânsal sınırların giderek silikleştiğini elektronik panoptikon ya da akışkan gözetim kavramlarıyla tartışır. Lyon'un analizinde, gözetim toplumsal düzeni yeniden üretme ve ayrımcı sınıflandırmalara aracılık etme kapasitesine sahiptir. Algoritmik sistemlerdeki yanlışlık ve adalet sorunları, Lyon'un sosyal sıralama analizinin güncel teknolojilerle kesiştiği önemli alanlardır (Lyon, 2017). Dolayısıyla, gözetim sistemleri insanları kredi puanı, risk profili, davranış kalıpları gibi veriye dayalı kategorilere ayırarak farklı muameleye olanak tanımaktadır.

Günümüzde yapay zeka sistemleri ile gözetim pratikleri yeni biçimler kazanmıştır. Özellikle, bireylerin davranışlarını gerçek zamanlı olarak analiz edip sınıflandırarak panoptik algıyı algoritmik düzeyde yeniden üretebilmektedir. Bu bağlamda izlenen birey gözetim mekanizmasının nasıl işlediğini tam olarak bilmemekte, bu durum klasik panoptikon metaforundaki *görülür ama görünmez* dinamiğini daha karmaşıklştırmaktadır. Dahası Zuboff'un enstrümantarya iktidar anlayışı ile norm üretim süreci teknolojik düzeyde yeniden ele alınmakta ve normlar artık algoritmalar aracılığıyla uygulanabilmekte ve müdahaleler otomatik biçimde yapılabilmektedir. Yapay zeka destekli sistemler, gözetimi tek merkezden çok aktörlü ağlar biçiminde ele alan Lyon'un yaklaşımını da derinleştirmektedir. Görüldüğü üzere, Foucault'nun panoptikon kuramı, Zuboff'un gözetim kapitalizmi ve Lyon'un sosyal sıralama analizleri birlikte incelendiğinde, gözetimin tarihsel sürekliliği ve teknolojik dönüşümü arasındaki bağ daha görünür hale gelmektedir. Bu bağlamda, yapay zeka çağında gözetim, norm üretme, müdahale, sınıflama ve öngörü pratikleri üzerinden yeniden yapılandırılmıştır (Foucault, 1977, Lyon, 2018, Zuboff, 2019) Bu yeni ortamda klasik



kuramsal araçlar hala anlamlıdır, ancak teknolojik özgünlükleri hesaba katacak şekilde eleştirel olarak uyarlanmalıdır.

Bu noktada, gözetimin meşruiyeti meselesi doğrudan insan hakları teorisinin normatif temelleriyle kesişmektedir. Gözetim teknolojilerinin meşru sınırları, teknik güvenlik, toplumsal fayda kriterleri ve hakların temel statüsü ile belirlenmelidir. Çağdaş hukuk teorisi, belirli özgürlüklerin -ifade, vicdan ve mahremiyet gibi- dokunulmaz bir konumda olduğuna dikkat çekmektedir. Bu çerçevede, John Rawls'un (A Theory of Justice, 1971/1999) adalet kuramında belirttiği üzere, temel hak ve özgürlükler *toplumsal fayda* adına feda edilemez, çünkü bu haklar, yalnızca özgürlüğün kendisiyle çatıştığında ve eşit özgürlük ilkesinin korunması gerektiğinde sınırlanabilmektedir. Benzer biçimde, Ronald Dworkin (1977) de hakların genel refah ya da fayda hesaplamalarına karşı *koz* işlevi gördüğünü savunmaktadır. Bu bağlamda, mahremiyet veya ifade özgürlüğü gibi hakların yalnızca diğer temel haklar ya da olağanüstü derecede önemli toplumsal çıkarlar söz konusu olduğunda sınırlandırılabilceğini, ancak sıradan verimlilik ya da fayda artışları için sınırlandırılmayacağını ileri sürmektedir. Ayrıca, Jeremy Waldron (2010) hakların onur boyutunu ön plana çıkararak, hakların uygulanmasındaki zorlukları kabul etmekle birlikte korunmalarının dikkatli bir dengeleme gerektirdiğini -ancak hiçbir zaman terk edilmemesi gerektiğini- vurgulamaktadır. Özellikle mahkemeler ifade özgürlüğü veya onur gibi temel değerleri korurken genellikle farklı değerleri dengelemek ve zorlu değer yargılarında bulunmak zorunda kalmaktadır. Kısacası, haklar teorisi mahremiyet, ifade özgürlüğü ve eşitliği adil bir toplumun önkoşulları olarak görür, dolayısıyla getirilecek sınırlamalar insan onurunu hukuka aykırı biçimde tehlikeye atmayacak şekilde -yani yasaya uygunluk, gereklilik ve orantılılık ölçütlerine uyarak- düzenlenmelidir. Bu yaklaşım, çıkış noktasını doğrudan AİHS ve AB Temel Haklar Şartı'ndan almaktadır: her türlü dijital gözetim rejimi, keyfi ihlallere karşı korunan bu haklarla uyumlu olmalıdır.

Mahremiyetin yalnızca gizlilik değil, kişinin kendi kimliğini temsil etme, sınırlarını çizme ve özerkliğini sürdürme hakkı olduğunu vurgulayan Allen'in (2008) etik zemini Moore'un (2010) mahremiyeti bireyin ahlaki özerkliğini ve bilişsel alanını koruyan temel hak olarak görmesiyle derinleşmektedir. Nissenbaum (2004) ise dijital çağın veri akışlarında mahremiyetin, mutlak bir gizlilikten ziyade *bağlamsal bütünlük* ilkesiyle korunabileceğini savunmaktadır. Buna göre, bilginin akışı ancak uygun toplumsal norm ve bağlamlar içinde meşru sayılabilir. Bu normatif yaklaşımlar, AİHS ve AB Temel Haklar Şartı'nın insan onurunu ve özel yaşamın gizliliğini ayrılmaz haklar olarak kabul eden düzenlemelerinde



yansımasını bulmuştur. Dolayısıyla dijital gözetim, algoritmik sınıflandırma ve yapay zekâ temelli karar süreçleri, bireyin mahremiyetini, özerkliğini ve eşitlik ilkesini tehdit ettiğinde, insan onuruna dayalı hak kuramı, hukukun müdahale sınırlarını belirleyen temel ölçütleri ortaya koyar. Bu yaklaşım, her türlü dijital denetim veya veri işleme faaliyetinin yalnızca gereklilik, orantılılık ve insan denetimi ilkelerine uygun olduğu sürece meşru sayılabileceğini savunur. Böylelikle insan onuru, klasik liberal hak anlayışından dijital çağın etik yönetim paradigmasına uzanan bir süreklilik içinde hem hakların nihai dayanağı hem de onların sınırlandırılmasına yön veren normatif ilke olarak yeniden tanımlanmaktadır. Böylece, dijital çağda mahremiyet hakkı, insan onurunun, demokratik katılımın ve teknolojik yönetişimin meşruiyetinin de normatif dayanağı haline gelmiştir.

Bu çerçevede, hukuk ve teknoloji alanında yürütülen çalışmalar, gözetim aygıtlarının biçimlenmesinde yazılım altyapılarının *kod* ve düzenleyici normların birbiriyle etkileşime girdiğini ve sıklıkla çatıştığını ortaya koymaktadır. Örneğin, Lawrence Lessig (2000) *kod kanundur* ifadesiyle siber uzayın teknik mimarisinin toplumsal normları ve hukuki düzenlemeleri biçimlendiren bir düzenleyici etkinliğe sahip olduğunu vurgulamıştır. Bu bağlamda, bir sosyal medya platformunun gizlilik ayarları, hangi bilgilerin görünür ya da görünmez olacağını belirleyen mimari kodlar olarak işlev görmektedir. Dolayısıyla, bir yapay zekânın veya gözetim sisteminin tasarımı -tıpkı bir yasa gibi-gözetlemeyi ya kolaylaştırabilecek ya da sınırlandırabilecek bir mimari düzen anlamına gelmektedir. Bu noktayı daha ileri taşıyan Hildebrandt ve Tielemans (2013), tasarım yoluyla yasal koruma kavramını geliştirmiştir. Buradaki yaklaşıma göre, ağ bağlantılı çağımızda temel haklar - mahremiyet, adil yargılama hakkı, ayrımcılığa uğramama hakkı gibi- yazılı hukuk metinleri ve teknolojik altyapıların kendi içinde kodlanmış normlarla korunmalıdır. Dolayısıyla, pratikte hakların sistematik olarak güvence altına alınması -örneğin: varsayılan gizlilik ayarları, algoritmik etki değerlendirmeleri ve kullanıcıların veri akışı üzerindeki kontrolünü sağlayan mekanizmalar- için teknolojik çözümlerin uygulanması anlamına gelmektedir.

Teorik açıdan bakıldığında, dijital gözetim ve yapay zekâ temelli karar sistemleri, hukukun ve teknolojinin kesişiminde yer alan kritik bir normatif uyarıya işaret etmektedir. Bu bağlamda, temel hakların korunması için yasal düzenlemelerin yanı sıra bu düzenlemeleri somutlaştıran teknoloji mimarisine de hak koruma ilkelerinin entegre edilmesi gerekmektedir. Dolayısıyla, dijital gözetim rejimlerinin normların uygulanma biçimini belirleyen teknolojik tasarımlarla da şekillendiği görülmektedir. Bu nedenle, algoritmik süreçlerin şeffaflığı ve hesap verebilirliği sağlanmadıkça, hakların korunması yönündeki yasal çabalar teknik mimarinin



arkasında etkisiz kalma riski taşımaktadır. Bu noktada, Pasquale'nin algoritmik şeffaflık ve hesap verebilirliğe ilişkin eleştirileri, hak koruma ilkelerinin teknoloji tasarımının yapısal unsurlarında da içselleştirilmesi gerektiğini ortaya koymaktadır. Pasquale (2015), teknoloji destekli gözetimin *karanlık yüzünü* vurgulayarak, veri işleme süreçlerinin yoğunlaştığı dijital ekonomide güçlü aktörlerin ticari sırların ardına gizlendiğini ve algoritmaların sözde tarafsızlık iddialarının bu nedenle doğrulanamaz hâle geldiğini belirtir. Dahası, mevcut hukuk düzenleri çoğu zaman şirketlerin iş modellerini ve gözetim sistemlerinin gizli formüllerini de koruyarak hem bireyler hem de denetleyici kurumlar açısından ciddi bir şeffaflık sorunu yaratmaktadır. Bu durum, dijital düzenin giderek hukuki şeffaflığın yerini teknik gizliliğin aldığı bir yapıya dönüşmesine ve böylece denetim mekanizmalarıyla hukukun geleneksel işlevi arasında derin bir uyumsuzluk doğmasına yol açmaktadır.

Görüldüğü üzere, dijital çağda ortaya çıkan temel sorunlardan biri hesap verebilirlik boşluğudur. Tarihsel olarak insan karar vericilere yönelik geliştirilen hukuk sistemi, artık otomatikleştirilmiş, veri odaklı ve kodla işleyen güç biçimlerine uyum sağlamakta zorlanmaktadır. Bu yapısal boşluğu gidermeyi amaçlayan AB düzenleyicileri, önemli adımlar atmıştır: GDPR, bireyler üzerinde önemli etkiler doğuran tamamen otomatik karar alma süreçlerini yasaklamakta (Madde 22) ve veri sahiplerine açıklama talep etme, karar sürecine itiraz etme gibi haklar tanımaktadır. Benzer biçimde, Yapay Zekâ Yasası (AI Act) ve Dijital Hizmetler Yasaları, algoritmik sistemlerin tasarımı ile kullanımını düzenleyerek, insan denetimi, şeffaflık ve orantılılık ilkeleri çerçevesinde yeni bir hesap verebilirlik rejimi inşa etmeyi hedeflemektedir.

Sonuç olarak, bu kuramsal yapı dijital gözetimin teknik bir olgunun ötesinde derin bir normatif ve hukuki mesele olduğunu göstermektedir. Gözetim, haklar ve teknoloji arasındaki etkileşim, insan onurunu ve demokratik değerlere dayalı hukuk düzenini korumak için yeniden düşünülmesi gereken bir alan yaratmaktadır. Bu nedenle, dijital çağın gözetim pratikleri, hukukun meşruiyetini sınanan bir etik sorumluluk alanı haline gelmiştir.

Dijital Avrupa'da Gözetim ve Mahremiyet: Normatif Sınırlar ve Meşruiyet İlkeleri

Gözetim uygulamaları devlet çıkarları ile bireysel haklar arasında temel bir gerilim doğurmaktadır, liberal demokrasiler bağlamında mahremiyete yönelik her türlü müdahale, ancak güçlü ve meşru bir gerekçeyle savunulabilir. Normatif olarak sorgulanması gereken husus, gözetimin hangi koşullar altında meşru sayılabileceği ve ne zaman temel hakların yasadışı biçimde ihlal edildiği sorusudur. Bu soru özellikle, insan onuru ve mahremiyetin



temel değerler olarak ön plana çıktığı Avrupa İnsan Hakları Hukuku çerçevesinde büyük önem taşımaktadır. Nitekim, mahremiyet ile insan onuru arasındaki denge, gereklilik ve orantılılık ilkelerinin uygulanması ve gözetim faaliyetlerinin insan denetimine tabi olması gibi boyutlar, gözetimin meşruiyetini değerlendirmede kilit roller üstlenmektedir (Lissens, 2024, Fikfak & Izvorova, 2022).

Normatif hak teorileri, gözetimin ne zaman ve hangi koşullar altında bireysel hakları haklı olarak geçersiz kılabileceğini analiz etmek için önemli bir çerçeve sunmaktadır. Bu bağlamda Dworkin, bireysel hakları (örneğin gizlilik hakkını) kolektif hedeflerin üstünde konumlandırmakta ve ancak gerçek bir acil durum dışında ihlal edilemezliğini öne sürmektedir (Dworkin, 1977). Buna göre, gözetim uygulamaları ancak başka bir temel hakkı korumak amacıyla ya da gerçekten olağanüstü bir durumda meşru olabilmekte, rutin bir kamu refahı ya da güvenlik gerekçesi gizlilik hakkını geçersiz kılmak için yeterli olmamaktadır. Öte yandan Rawls'ın teorisi de benzer biçimde bireysel temel haklara özel bir öncelik tanımakta, temel eşit özgürlüklerin sosyal ve ekonomik hedeflerin önünde yer aldığını savunmaktadır (Rawls, 1971/1999). Bu bağlamda hakların üstünlüğünü esas alan anlayış, mahremiyet ve özgürlüklerin, kamu güvenliği gibi kolektif çıkarlar uğruna kolaylıkla sınırlandırılmayacağını öne sürmektedir.

179

Normatif hak kuramları perspektifinden bakıldığında, gözetimin hangi durumlarda bireysel hakların sınırlandırılmasını meşru kılabilceği tartışmalıdır. Bu konuda, özellikle 11 Eylül sonrasında benimsenen güvenlik-merkezli politikaların, hakları yalnızca güvenlik uğruna değiştirilebilir değişkenler olarak görme eğilimi eleştirilmektedir. Bu eleştirinin özünde, hakların maliyet-fayda analizine indirgenmesi ve özgürlük-güvenlik arasında nicel bir denge kurulabileceği varsayımının hem kavramsal hem de ahlaki açıdan yanıltıcı olduğu, dolayısıyla hakların kendi başına taşıdığı normatif önceliğin, araçsal gerekçelere indirgenmemesi gerektiği vurgulanmaktadır (Waldron, 2010). Dolayısıyla böyle bir yaklaşım, hakların doğasında var olan normatif üstünlüğü zayıflatmakta ve onları pragmatik bir çıkar analizinin unsuru hâline getirmektedir. Bu bağlamda özellikle temel medeni ve siyasal haklar, yalnızca değişen faydacı hesaplamalara dayanarak ödün verilemeyecek taahhütlerdir. Buna göre özgürlük ile güvenlik arasında kayan bir ölçek tahayyülü, hangi hakların kimin güvenliği için feda edildiği sorusunu ya da ölçütünü belirsizleştirmektedir (Waldron, 2010). Kısacası, özgürlüklerin sosyal ve ekonomik hedeflerin önünde konumlandırılması, bu özgürlüklerin kamu yararı gerekçesiyle sıradan biçimde feda edilemeyeceğini, gözetimin meşrulaştırılabilmesi için hak temelli ve ilkeli bir gerekçenin zorunlu olduğunu ortaya



koymaktadır. Böylelikle, güvenlik tehditleri hakların otomatik biçimde aşınmasına neden olmamalıdır.

Anita L. Allen (2008)'ın gizlilik etiğine ilişkin çalışması, gözetimin *prima facie* yani ilk bakışta ahlaki olarak yanlış olduğunu ortaya koyarak, hangi istisnai koşullar altında meşru görülebileceğine dair daha incelikli bir normatif çerçeve sunmaktadır. Allen'in ortaya koyduğu *casusluk karşıtı ilke*, bireylerin kasıtlı biçimde gözetlenmesinin -gizlilik normlarını ihlal ettiği ve çoğunlukla aldatma veya gizliliğin ihlali üzerine kurulu olduğu için- doğası gereği etik dışı olduğunu öne sürülmektedir. Bu öncül, gözetlemenin ahlaki bakımdan tarafsız bir yönetim aracı değil, bireyin haysiyetine ve özerkliğine içkin bir tehdit oluşturduğunu vurgulamaktadır. Bununla birlikte Allen, belirli istisnai durumlarda gözetlemenin etik açıdan kabul edilebilir, hatta zorunlu olabileceğini de kabul etmektedir. Bu durumlar, inkâr edilemeyecek ölçüde iyi amaçlar -örneğin ciddi bir zararın önlenmesi- güdüldüğünde ve daha az müdahaleci bir alternatifin mevcut olmadığı hallerde görülmektedir. Bu yönüyle Allen'in yaklaşımı, gözetimi hak temelli ve ilke odaklı bir etik çerçeveye yerleştirerek, onun meşruiyetini orantılılık, gereklilik ve insan onuruna saygı ilkeleriyle koşullandırmaktadır. Dolayısıyla, istisnai durumlarda dahi gözetleme pratiklerine katı ahlaki sınırlamaların getirilmesi gerektiğini ısrarla savunmaktadır. Bu bağlamda tanımladığı *erdemli casus* figürü, mahremiyete ancak ciddi bir isteksizlikle ve gözetlenen kişinin ahlaki iradesine saygı göstererek müdahale eden, bu müdahaleyi ise zararı en aza indiren, ölçülü ve özenli yöntemlerle gerçekleştiren bir aktörü temsil etmektedir (Allen, 2008). Bu anlayışa göre, etik olarak haklı gösterilebilecek her türlü gözetleme, en az müdahaleci araçları kullanmalı, yalnızca zorunlu olan hedefleri gözetmeli ve bireyin insan onuru ile özerkliğine koşulsuz bir saygı göstermelidir. Bu özellikle aşağılayıcı, keyfi ya da aşırı müdahaleci yöntemlerden sistematik biçimde kaçınmayı gerektirmektedir. Dolayısıyla Allen'in normatif yaklaşımı, gözetimin meşruiyet sınırını belirleyen temel ölçütün insan onuru ve özerkliğin korunması olduğunu vurgulamaktadır. Zira gözetim, bireyleri yalnızca birer nesne ya da veri noktasına indirgediği anda -amacı ne kadar iyi olursa olsun- etik sınırın ötesine geçmiş olacaktır.

Görüldüğü üzere bu teorisyenlerin ortak yaklaşımı, gözetim olgusuna ilişkin hak temelli bir normatif varsayım ortaya koymaktadır. Gözetim, doğası gereği etik açıdan şüpheli bir eylem olarak değerlendirilmektedir. Bu şüpheyi ortadan kaldırmak için kamu güvenliği ya da genel çıkar gibi soyut gerekçeler yeterli görülmemektedir. Bunun yerine, yalnızca diğer temel hakların korunmasına veya acil durumların yönetimine yönelik, açıkça tanımlanmış ve ikna edici etik gerekçeler sunulmalıdır. Bu nedenle, her türlü gizlilik ihlali dar kapsamlı bir



biçimde tanımlanmalı ve sıkı ahlaki sınırlamalara tabi tutulmalıdır. Bu normatif duruş, gözetimin meşruiyetinin belirlenmesinde gizlilik, özgürlük ve insan onuru gibi temel hakların belirleyici olduğu anlayışıyla örtüşmektedir. Dolayısıyla, bu kriterleri karşılamayan her türlü gözetim uygulaması, meşru bir güvenlik önlemi değil, açık biçimde hak ihlali olarak değerlendirilmelidir.

Dijital Kapitalizm Çağında Mahremiyet ve İnsan Onuru

İnsan onuru, özerk, eşit ve ahlaki değere sahip bir özne olarak, kurucu bir insan hakları ilkesi olarak çalışmamızda ele alınmaktadır. Bu bağlamda, Avrupa insan hakları söylemi, mahremiyetin insan onuruyla ayrılmaz bir biçimde bağlantılı olduğunu vurgulamaktadır. Özellikle 20. yüzyılın totaliter rejimlerinin deneyimleri, kişisel verilerin kötüye kullanılmasının insan onurunu doğrudan zedeleyebileceğini açık biçimde göstermiştir. Nazi Almanyası'nın azınlıkları izlemek, sınıflandırmak ve yok etmek amacıyla veri sistemlerini kullanması, gözetimin etik sınırlarının tarihsel olarak nasıl aşıldığını somut biçimde ortaya koymuştur (Bygrave, 2014, Whitman, 2004). Bu tarihsel travmaların ardından oluşturulan Avrupa hukuk araçları -başta Alman Temel Yasası (Grundgesetz, 1949) ve Avrupa İnsan Hakları Sözleşmesi (AİHS) olmak üzere- mahremiyetin korunmasını kasıtlı olarak insan onuru kavramına dayalı bir hak olarak yeniden tanımlamıştır (ECHR, 1950, Article 8, Grundgesetz, 1949, Article 1). Dolayısıyla bu yaklaşım, bireylerin yalnızca devletin kontrol nesnesi veya veri kaynağı olarak görülmezsizin, kişiliklerini ve kimliklerini bağımsız biçimde geliştirme hakkına sahip olmaları gerektiği anlamına gelmektedir. Böylelikle mahremiyet, salt bir bilgi gizliliği meselesi olmaktan çıkarak, insan onurunu koruyan özgür ve özerk varoluşun etik temeli hâline gelmiştir.

Avrupa'daki mahremiyet-onur ilişkisi, Anglo-Amerikan yaklaşımından belirgin biçimde ayrılmaktadır. Whitman'ın (2004) ileri sürdüğü gibi, kıta Avrupası'nda mahremiyet hukukunun kökeni esasen onur ve itibarın korunmasına dayanan bir tarihsel gelenekten türemiştir. Buna karşın Amerikan yaklaşımı, bireyin devlet müdahalesinden özgürlüğü ilkesine dayanmaktadır. Bu ayrım, mahremiyetin Avrupa düşüncesinde özel alanın gizliliği dışında kişiliğin, özsaygının ve sosyal tanınmanın korunması olarak kavramsallaştırıldığını göstermektedir. Bu bağlamda Avrupa normatif perspektifinde gizlilik ihlalleri, doğrudan kişiliğin bütünlüğüne ve insan onuruna aykırı eylemler olarak değerlendirilmektedir. Sürekli gözetim pratikleri -anlık zarar doğurmasa bile- bireyleri kalıcı bir maruz kalma, güçsüzlük ve aşağılanma konumuna yerleştirerek onurla bağdaşmayan bir varoluş biçimine zorlayacaktır



(Bygrave, 2014, De Hert & Gutwirth, 2006). Bu durum özellikle, bireylerin özel iletişimlerinin, davranışlarının veya hareketlerinin izlenmesi gibi uygulamalarda daha belirgindir. Zira bu tür eylemler bireyi varsayılan olarak şüpheli konumuna indirgemekte ve özgürce kendini ifade etme kapasitesini zayıflatmakta ve onurun gerektirdiği kişisel saygıyı aşındırmaktadır. Sonuç olarak, Avrupa insan hakları söylemi, mahremiyet hakkını negatif özgürlük biçimi olmanın ötesinde insan onurunun kurucu unsuru olarak yeniden tanımlamaktadır (ECHR, S. and Marper v. United Kingdom, 2008, para. 66).

Mahremiyet ile insan onuru arasındaki ilişki, sıklıkla gerilimli bir değerler alanı olarak tartışılrsa da Avrupa insan hakları hukukunda bu iki kavram birbirini karşılıklı olarak tamamlayan ve meşrulaştıran hak ilkeleri biçiminde kavramsallaştırılmaktadır. Mahremiyetin korunması, bireyin onurunu teyit etmenin ve kişisel bütünlüğünü sürdürmenin asli bir yoludur. Bu çerçevede etik zorluk, mahremiyet ile onuru birbirine karşı dengelemekten ziyade, her ikisini de güvenlik ve kamu yararı gibi diğer toplumsal hedeflerle uzlaştırmaktır. Bu bağlamda, gözetim pratiklerinde *onur* kavramının öne çıkarılması, sınırlama argümanını güçlendirir, çünkü bu vurgu, bireylerin her şeyi gören bir devletin şeffaf öznelerine indirgenmemesi gerektiğini hatırlatır (Bygrave, 2014). Dolayısıyla, gözetim uygulamaları meşru sayılabilecek olsa dahi, bireylerin onurunu ortadan kaldıracak biçimde yürütülmemelidir. Özellikle zalimane, aşağılayıcı veya son derece kişisel müdahale içeren yöntemlerden kaçınılması gerekmektedir. Nitekim AIHM, aşırı müdahaleci gözetleme biçimlerini, özel hayata saygı hakkı (ECHR, 1950, Article 8) kapsamında kişisel bütünlük ve onur temelli ihlallerle ilişkilendirmiştir. Daha aşırı vakalarda ise, son derece aşağılayıcı gözetim uygulamaları, bireyin insani özsaygısını zedeleyerek AIHS Madde 3 (insanlık dışı veya aşağılayıcı muamele yasağı) kapsamında değerlendirilmiştir. Böylece AIHM, mahremiyet ve onurun bir arada, insan kişiliğinin özüne ilişkin normatif bir bütünlük oluşturduğunu teyit etmiştir.

Görüldüğü üzere, onur merkezli bir etik anlayış, gözetim düzenlemelerinin kamu yararının yanı sıra bireyin özerklik ve eşit özne statüsüne saygı ilkesine de uygun biçimde sınırlandırılmasını gerektirir. Böyle bir yaklaşım, gözetimin meşruiyetinin amaçlarının ve kullandığı araçların bireysel onur üzerindeki etkilerinin değerlendirilmesine bağlı olduğunu varsaymaktadır. Dolayısıyla herhangi bir meşru gözetim politikası, bireysel onurun korunması için gerekli olan mahrem alanı koruduğunu, örneğin, mahrem kişisel verilerin toplanmasını sınırlayarak, bireyin şeref ve itibarına saygı göstererek ve kişilerin utanç verici ya da aşağılayıcı koşullarda izlenmesini önleyerek gösterebilmelidir. Bu çerçevede, mahremiyetin



insan onurunun korunmasıyla yakından ilişkili olduğu kabul edilmelidir. Güvenlik ile mahremiyet arasında sıfır toplamı bir karşıtlık kurmak, etik açıdan yanıltıcıdır, zira her iki değer de özgür ve haysiyetli bir yaşam biçiminin önkoşullarını oluşturur (Solove, 2007). Sonuç olarak, insan onurunu zedeleyen gözetim, ahlaki meşruiyetini kaybedecek: güvenliği sağlama iddiası taşısa bile, böyle bir sistem yaşamaya değer bir toplumsal düzenin korunmasına hizmet etmekten uzaklaşacaktır.

Hukuki ve Normatif Perspektiften Gözetim: Gereklilik, Orantılılık ve İnsan Denetimi

Avrupa insan hakları hukukunda, özellikle AIHS 8. maddesi uyarınca, bireylerin özel hayatına yönelik her türlü müdahale -gözetim uygulamaları dâhil- yalnızca yasallık, meşru amaç, gereklilik ve orantılılık kriterlerinin eşzamanlı biçimde karşılanması hâlinde meşru kabul edilmektedir (Harris vd., 2018). Bu iki temel ilke, demokratik bir toplumda hakların sınırlandırılmasının keyfilikten korunması ve devlet müdahalesinin ölçülülüğünün sağlanması için normatif bir çerçeve oluşturmaktadır (Letwin, 2023). Bu bağlamda gereklilik ilkesi, devletin gözetim önlemini yalnızca acil bir toplumsal ihtiyaç durumunda uygulayabileceğini, yani söz konusu amaca ulaşmak için daha az müdahaleci bir alternatif bulunmadığını göstermesi gerektiğini öngörmektedir (Guida & Tozzi, 2020). Buna karşılık orantılılık ilkesi, gözetimin bireyin mahremiyet hakkına müdahalesinin, elde edilmek istenen kamu yararıyla makul bir denge içinde olmasını zorunlu kılmalı ve müdahale, ulaşılmak istenen amaçla karşılaştırıldığında aşırı bir yük getirmemelidir.

AIHM içtihadında bu ilkeler, gözetim önlemlerinin meşruiyetini belirleyen başlıca değerlendirme araçları olarak yerleşmiştir. Örneğin Roman Zakharov v. Russia kararında Mahkeme, kitlesel telefon dinleme rejimlerinin demokratik bir toplumda gerekli olabilmesi için yeterli denetim mekanizmalarına ve sınırlı hedefleme ölçütlerine sahip olması gerektiğini belirtmiştir (ECHR, 2015, para. 232). Benzer biçimde, Szabó and Vissy v. Hungary kararında, ulusal güvenlik gerekçesiyle yürütülen geniş kapsamlı izlemelerin *orantılılık* koşulunu karşılamadığı sonucuna varılmıştır (ECHR, 2016, para. 89). Dolayısıyla, Avrupa insan hakları hukukunda gereklilik ve orantılılık, gözetim politikalarının yasallığını ve ahlaki meşruiyetini de sınırlandıran normatif ilkeler olarak işlev görmektedir.

Bu ilkelerin uygulama düzeyinde yorumlanması, gözetimin ultima ratio -yani son çare-niteliğinde olması gerektiği anlamına gelmektedir. Buna göre, gözetim yalnızca daha az müdahaleci önlemlerin yetersiz kaldığı, belirli ve ölçülebilir bir tehdidin mevcut olduğu durumlarda kullanılmalı ve bu tehdidin yoğunluğu ve niteliğiyle orantılı biçimde



sınırlandırılmalıdır. Benzer şekilde, AB Adalet Divanı (ABAD), AB Temel Haklar Şartı'nın 7. ve 8. maddelerini yorumlarken, gözetimin meşruiyetini gereklilik ve orantılılık kriterleriyle sıkı biçimde ilişkilendirmiştir. Digital Rights Ireland v Ireland ve Tele2 Sverige AB v Post-och telestyrelsen kararlarında Divan, ayırım gözetmeyen, genel veri saklama rejimlerinin bireylerin mahremiyetine ve veri koruma hakkına ölçüsüz biçimde müdahale ettiğine hükmetmiş ve bu tür uygulamaları *gerçek gereklilik* ve *orantılılık* ilkelerinden yoksun oldukları gerekçesiyle geçersiz kılmıştır (CJEU, 2014, paras. 54–69, CJEU, 2016, paras. 99–107). Bu içtihatlar, gözetimin meşru sayılabilmesi için yasal temele ve sıkı normatif gerekçelendirmeye ve birey-merkezli bir sınırlandırma rejimine dayanması gerektiğini teyit etmektedir. Görüldüğü üzere ABAD içtihadı, geniş kapsamlı ve ayırım gözetmeyen veri toplama uygulamalarının, bireylerin özel yaşamına yönelik ağır bir müdahale teşkil ettiğini açık biçimde ortaya koymaktadır. Dolayısıyla, bu tür kapsamlı veri saklama önlemlerinin yalnızca eşit derecede ciddi tehditlerle -örneğin organize suç veya terörizmle mücadele gibi- haklı gösterilebileceğini ancak, soyut, genel veya varsayımsal risklerin bu ölçüde bir müdahaleyi meşrulaştıramayacağını vurgulamıştır.

Gereklilik ve orantılılık ilkelerinin uygulanması, devletlerin gözetim faaliyetlerini her bir vaka için ayrı ayrı sürekli biçimde gerekçelendirmesini zorunlu kılmaktadır. Geniş kapsamlı genel yetkilendirmeler veya süresiz kitlesel izleme uygulamaları bu ilkelerle bağdaşmamaktadır. Bunun yerine gözetim, belirli bir amaca yönelik, ölçülü ve zamanla sınırlı şekilde kullanılmalıdır. AİHM'nin birçok kararında vurgulandığı gibi, demokratik bir toplumda alınan önlemler yararlı olmasının yanı sıra kesinlikle gerekli olması bağlamında anlamlı olmaktadır. Dolayısıyla gereklilik ve orantılılık ilkesi, aynı amaca daha az müdahaleci araçlarla ulaşıyorsa daha kapsamlı önlemlerin ölçüsüz sayılacağı anlamına gelir. Örneğin, tüm vatandaşların iletişim verilerini süresiz biçimde saklamak yerine yalnızca makul şüphe altındaki kişilerin iletişimlerinin izlenmesi hem daha dar kapsamlı hem de temel haklara daha saygılı bir yaklaşım benimsenmelidir. Bu yaklaşım, devletleri ayırım gözetmeyen kitlesel gözetimden uzaklaştırarak hedefli ve bağlama duyarlı gözetim yöntemlerini benimsemeye yönelten normatif bir teşvik yaratacaktır. Dahası gereklilik ve orantılılık ilkeleri düzenli denetimi de zorunlu kılmakta, ani bir tehdit veya olağanüstü durum sırasında gerekli görülen bir gözetim tedbiri, tehdit ortadan kalktığında artık gerekçesini yitirebilmektedir. Bu nedenle gözetim yetkilendirmeleri belirli sürelerle sınırlanmalı, devam edecekse yeni bir gerekçelendirme sürecinden geçmelidir. Avrupa hukuk literatüründe bu anlayış, hukukun



teknolojik dönüşüme uyum sağlayarak insan onuru, hesap verebilirlik ve demokratik denetim ilkelerini koruma çabasının bir parçası olarak değerlendirilmektedir.

Kısacası gereklilik ve orantılılık ilkeleri, temel hakların en önemli güvenceleri arasında yer alarak, demokratik bir toplumda gözetim faaliyetlerinin korumayı amaçladığı özgürlükleri ortadan kaldırmamasını sağlamaktadır. Araçlarla amaçlar arasında makul bir orantı kurulmasını ve haklara yalnızca zorunlu olduğu ölçüde müdahale edilmesini şart koşarak, bu ilkeler güvenlik politikalarının özgür, adil ve onurlu bir toplum düzeniyle bağdaşabilir kalmasını teminat altına almaktadır. Nitekim akademik literatürde de vurgulandığı üzere, güvenlik ile mahremiyeti karşıt kutuplar şeklinde konumlandırmak yanlış bir ikilemdir, çünkü güvenliğin meşru bir biçimde sağlanabilmesi, mahremiyetin özünü oluşturan iki temel değere -bireysel özerklik ve keyfi müdahalelere karşı korunma hakkına- saygı gösterilmesine bağlıdır. Dolayısıyla yalnızca gerekli ve orantılı nitelik taşıyan gözetim uygulamaları hukuken ve etik olarak meşru sayılmalı ve bu ölçütleri karşılamayan her türlü gözetim faaliyeti ise hak ihlali olarak değerlendirilmelidir.

Normatif kuram ve hukuk doktrininde sürekli vurgulanan bir tema, gözetim mekanizmalarında insan gözetiminin normatif zorunluluğudur. İnsan gözetimi, özellikle dijital çağın otomatik, özerk ve çoğu zaman şeffaf olmayan izleme teknolojilerinin yaygınlaştığı bir bağlamda, hukukun üstünlüğü, hesap verebilirlik ve temel hakların korunması açısından merkezi bir konuma sahiptir. Bu kavram, gözetim faaliyetlerinin yalnızca teknik süreçlere veya algoritmik yapılara bırakılmaması, aksine demokratik meşruiyet ve etik sorumluluk ilkeleri doğrultusunda, yetkilendirilmiş bireyler veya kurumsal aktörler tarafından sürekli denetlenmesi gerekliliğini ifade etmektedir (Green, 2022). Dolayısıyla, yüz tanıma gibi algoritmik gözetim teknolojilerinin uygulanmasından önce yetkili kurumlarca hazırlanacak etki değerlendirme raporlarının kamu denetimine açılması, insan karar vericilerin sürece dahil edilmesi gerekmektedir.

Bu çerçevede insan gözetimi, düzenleyici kurumlar, bağımsız denetim organları veya yargısal otoriteler gibi hesap verebilir mercilerin, gözetim uygulamalarının amaç, kapsam ve araçları üzerinde süreklilik arz eden bir kontrol mekanizması kurmasını gerektirmektedir. Böyle bir denetim, hem bireylerin özel hayatının gizliliğini ve ifade özgürlüğünü korurken hem de devletin gözetim yetkisinin keyfileşmesini önleyerek hukuk devletinin normatif sınırlarını güçlendirmektedir (Sterz et al., 2024). Dolayısıyla, insan gözetimi teknik bir güvenlik önlemi olmanın ötesinde demokratik yönetişimin ve insan onuruna dayalı hukuki düzenin



vazgeçilmez bir unsuru olmaktadır. Bu yaklaşım hem hukuki meşruiyet hem de demokratik denetim açısından kritik bir önem taşımakta ve insan gözetimi ve özgürlük boyutu bağlamında denetimsiz gözetim yetkilerinin bireysel özgürlük için ciddi bir tehdit oluşturduğunu kabul etmektedir. Bu nedenle özgürlüğün korunması, gözetim süreçlerinin her aşamasında bilinçli insan yargısına, şeffaf işleyişe ve bağımsız dış denetim mekanizmalarına tabi kılınmasını gerektirmektedir.

Normatif bir perspektiften bakıldığında, insan denetimi bireysel özgürlüklerin korunması ve devletin gözetim yetkisinin sınırlandırılması açısından temel bir güvence işlevi görür. Bu çerçevede, Dworkin'in hakların yalnızca diğer haklara veya olağanüstü durumlara tabi olabileceği yönündeki yaklaşımı, özgürlüklerin sınırlanmasının ancak istisnai ve rasyonel gerekçelere dayanabileceğini vurgular (Dworkin, 1977). Dolayısıyla, bir gözetim önleminin meşru kabul edilebilmesi için, bireysel haklara yapılan müdahalenin kamu yararıyla kurduğu denge, yalnızca teknik kurumlar tarafından değil, aynı zamanda bağımsız ve tarafsız insan aktörleri tarafından da normatif bir değerlendirmeye tabi tutulmalıdır.

Sonuç ve Değerlendirmeler

Bu çalışma, dijital kapitalizm çağında yapay zekâ destekli gözetim teknolojilerinin insan hakları üzerindeki etkilerini kuramsal ve hukuki bir çerçevede değerlendirmiştir. Özellikle mahremiyet, ifade özgürlüğü ve insan onuru gibi temel hakların, yapay zekâ teknolojilerinin yaygınlaştığı bir dijital altyapı içinde nasıl yeniden tanımlandığını ve kimi zaman tehdit altına girdiğini ortaya koymuştur. Dijital gözetim sistemlerinin teknik bir meselenin ötesinde etik, hukuki ve siyasal bir sorun olduğu sonucuna varılmıştır. Dolayısıyla, gereklilik, orantılılık ve insan denetimi ilkeleri, dijital gözetimin meşruiyetinin sağlanmasında temel normatif dayanaklar olarak tanımlanmıştır. Mahremiyet hakkı, bireysel bir özgürlük olmanın dışında demokratik toplumun temel taşı olan insan onurunun korunması bakımından da vazgeçilmez bir ilkedir. Bununla birlikte çalışmanın ortaya koyduğu en önemli bulgulardan biri, mevcut hukuk düzenlerinin hızlı dijital dönüşüm karşısında yetersiz kalmasıdır. Ayrıca hesap verebilirlik boşluklarının giderek artması ve algoritmik karar sistemlerinin şeffaflık ilkesinin zayıflamasıdır. Dijital gözetim, yalnızca yasal normlarla değil, aynı zamanda teknolojik tasarımlarla da şekillenmektedir. Dolayısıyla mahremiyetin ve özgürlüğün korunması, hukuk ve teknolojinin birlikte yeniden inşasını gerektirmektedir.

Bu bağlamda, algoritmaların ve veri işleme sistemlerinin, tasarım aşamasından itibaren temel haklara duyarlı bir şekilde yapılandırılması, varsayılan gizlilik ve kullanıcı özerkliği



ilkelerinin kod mimarisine entegre edilmesi gerekmektedir. Özellikle yüksek risk taşıyan yapay zekâ uygulamalarında, algoritmaların işleyişine dair şeffaflık sağlanmalı, değerlendirmeler kamuya açık hale getirilmelidir. Gözetim faaliyetleri teknik sistemlerin yanı sıra bağımsız kurumlar ve insan aktörler tarafından sürekli denetime tabi tutulmalıdır. Bireylerin veriler üzerindeki kontrolünü artıracak şekilde dijital egemenlik ilkesi geliştirilmelidir. Yapay zekâ ve gözetim teknolojilerinin sınır aşan niteliği göz önünde bulundurulduğunda, uluslararası hukukta koordineli düzenlemelerin yapılması, dijital hakların evrensel insan hakları çerçevesinde yeniden tanımlanması ve toplumun dijital haklar, algoritmik karar alma ve veri güvenliği konusunda bilinçlendirilmesi, özellikle genç kuşakların dijital yurttaşlık bilinciyle donatılması gerekmektedir.

Sonuç olarak, dijital kapitalizmin gözetim mantığına karşı insan haklarını korumak, teknik düzenlemelerle tek başına yeterli görülmemektedir. Daha derin etik, normatif ve yapısal müdahaleler gerekmektedir. Bu müdahaleler, mahremiyet ve ifade özgürlüğü gibi temel hakların demokratik toplum düzeninin devamlılığının teminatı olduğu düşüncesiyle yapılmalıdır. Bu bağlamda, insan onurunu merkeze alan ve teknolojik tasarımları hukuki normlarla bütünleştiren yeni bir dijital haklar rejimi inşa edilmelidir.

Kaynakça

- Allen, A. L. (2008). The virtuous spy: Privacy as an ethical limit. University of Pennsylvania Law School, 1–17. https://scholarship.law.upenn.edu/faculty_scholarship/168/.
- ARTICLE 19. (2018). *Side-stepping rights: Regulating speech by algorithm*. <https://www.article19.org>.
- Bentham, J. (1995). Panopticon (Preface). In Miran Bozovic (ed.), *The Panopticon Writings*, London: Verso, 29-95.
- Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.
- Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33.
- Court of Justice of the European Union (CJEU). (2014). *Digital Rights Ireland Ltd v Minister for Communications and Others*, Joined Cases C-293/12 and C-594/12, Judgment of 8 April 2014. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293>.
- Court of Justice of the European Union (CJEU). (2016). *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department*, Joined Cases C-203/15 and



C-698/15, Judgment of 21 December 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203>.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law*, Intersentia, 61–104.

Drinhausen, K., & Brussee, V. (2021). *China's social credit system in 2021: From fragmentation towards integration*. Mercator Institute for China Studies (MERICS). <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>.

Dworkin, R. (1977). Taking rights seriously. Harvard University Press. <https://www.law.nyu.edu/sites/default/files/Ronald%20Dworkin%20-%20Hard%20Cases.pdf>.

European Court of Human Rights. (1950). *European Convention on Human Rights*. Official Journal of the Council of Europe. https://www.echr.coe.int/documents/d/echr/convention_ENG.

European Court of Human Rights. (2008). *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008.

European Court of Human Rights. (2015). *Roman Zakharov v. Russia*, Application no. 47143/06, Judgment of 4 December 2015.

European Court of Human Rights. (2016). *Szabó and Vissy v. Hungary*, Application no. 37138/14, Judgment of 12 January 2016.

European Court of Human Rights. (2023). *Mass surveillance – Factsheet*. Press Unit. https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.

Fikfak, V., & Izvorova, L. (2022). Language and persuasion: Human dignity at the European Court of Human Rights. *Human Rights Law Review*, 22(3), 1–30.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books.

Gonzales, J. T. (2023). Implications of AI innovation on economic growth: A panel dataset analysis. *Journal of Economic Structures*, 12(1). <https://doi.org/10.1186/s40008-023-00307-w>

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, 1–22. <https://ssrn.com/abstract=3921216> or <https://doi.org/10.2139/ssrn.3921216>.

Grundgesetz, Article 1 of the Basic Law for the Federal Republic of Germany, (1949). Federal Law Gazette I p. 1.



- Guida, S., & Tozzi, D. (2020). The assessment of the proportionality of the measures that limit the privacy fundamental rights in the new guidelines of the European Data Protection Supervisor. *European Journal of Privacy Law & Technologies*, 2020(1), 195–207.
- Harris, D., O’Boyle, M., Bates, E., & Buckley, C. (2018). *Law of the European Convention on Human Rights* (4th ed.). Oxford University Press.
- Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, 29(5), 509–521. <https://doi.org/10.1016/j.clsr.2013.07.005>.
- Kilic, B., & Carr-Ryan, D. (2025). The geopolitics of surveillance capitalism [Working paper]. *Harvard Kennedy School*. https://www.hks.harvard.edu/sites/default/files/2025-10/25_Kilic_Tech_Paper_0.pdf?utm.
- Lessig, L. (2000). Code is law: On liberty in cyberspace. *Harvard Magazine*. <https://www.harvardmagazine.com/2000/01/code-is-law-html>.
- Letwin, J. (2023). Proportionality, stringency and utility in the jurisprudence of the European Court of Human Rights. *Human Rights Law Review*, 23(3), 478–503. <https://doi.org/10.1093/hrlr/ngad014>.
- Lissens, S. (2024). The foundations of EU personal data protection law: Privacy and human dignity. *EU-Renew*. <https://eu-renew.eu/the-foundations-of-eu-personal-data-protection-law-privacy-and-human-dignity/>.
- Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, 11, 824–842. <https://ijoc.org/index.php/ijoc/article/view/5527>.
- Moore, A. D. (2010). *Privacy rights: Moral and legal foundations*. Penn State University Press.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>.
- Özlük, D. (2023). Next stage of global capitalism: Digital platforms and rentier capitalism. *Ekonomi, Politika ve Finans Araştırmaları Dergisi (EPFAD)*, 8(4), 681–695. <https://doi.org/10.30784/epfad.1350739>.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Rawls, J. (1999). *A theory of justice* (Rev. ed.). Harvard University Press. (Original work published 1971)



<https://www.cita.or.id/wp-content/uploads/2016/06/John-Rawls-A-Theory-of-Justice-Belknap-Press-1999.pdf>.

Solove, D. J. (2007). *The digital person: Technology and privacy in the information age*. New York University Press.

Sterz, S., Baum, K., Biewer, S., Hermanns, H., Lauber-Rönsberg, A., Meinel, P., & Langer, M. (2024). On the quest for effectiveness in human oversight: Interdisciplinary perspectives. *arXiv preprint*, arXiv:2404.04059. <https://arxiv.org/abs/2404.04059>.

Waldron, J. (2010). Dignity, rights, and responsibilities (Public Law Research Paper No. 10-83). *New York University School of Law*.

Whitman, J. Q. (2004). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, 113(6), 1151–1221. <https://doi.org/10.2307/4135739>.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12160>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

