IBAD
SOSYAL BİLİMLER DERGİSİ
Journal of Social Sciences

Derleme / Review Article

IBAD 2026 (20): 191-209
https://doi.org/10.21733/ibad.1982874 **OPEN**

Dijital Gözetimden Tersine Gözetime: Toplumsal Güven, Yurttaş Kanıtı ve Hesap Verebilir Kamusal Açıklık

From Digital Surveillance to Sousveillance: Social Trust, Citizen Evidence, and Accountable Public Scrutiny

Erdi Çelebi[1*]

ÖZ

Günümüz bilgi toplumu çağında dijital teknolojiler, kurumların veri toplama ve izleme kapasitesini genişletirken bireylere de kamusal olayları akıllı telefonlar ve sosyal medya aracılığıyla kaydetme olanağı sunmaktadır. Türkiye'de internet kullanımının yaygınlığı, kişisel verilerin korunmasına ilişkin hukuki düzenlemeler ve gündelik kayıt-paylaşım pratikleri, bu çift yönlü açıklık düzenini güncel bir sosyal bilim problemi haline getirmektedir. Gözetim yazını çoğunlukla denetim ve mahremiyete, tersine gözetim çalışmaları ise yurttaş gazeteciliği ve hesap verebilirliğe yoğunlaşırken iki hattın toplumsal güven içindeki ortak işleyişi sınırlı ölçüde ele alınmaktadır. Bu teorik çalışma, ölçüt temelli kaynak seçimine dayalı amaçlı teori sentezi ve kavramsal çözümleme yoluyla gözetim, tersine gözetim, güven, mahremiyet ve yurttaş kanıtı yazınını bir araya getirmektedir. Çalışma, kurumsal izleme pratiklerinin meşruiyetinin orantılılık ve denetlenebilirlik koşullarına, yurttaş kayıtlarının kanıt değerinin ise teknik doğrulama, bağlamsal bütünlük, kamusal erişim ve gerekçeli kurumsal yanıta bağlı olduğunu savunmaktadır. Makalenin katkısı, kurumsal, epistemik ve prosedürel güven katmanlarını kayıt-kanıt ayrımıyla birleştiren "orantılı ve hesap verebilir kamusal açıklık" modelini önermesidir.

Anahtar kelimeler: Dijital Gözetim, Tersine Gözetim, Toplumsal Güven, Mahremiyet, Hesap Verebilirlik, Vatandaş Kaynaklı Kayıt

ABSTRACT

In today's information society age, digital technologies expand institutional capacities for data collection and monitoring while enabling individuals to document public events through smartphones and social media. In Türkiye, widespread internet use, the legal framework for personal data protection, and routine practices of recording and sharing make this bidirectional structure of public scrutiny an increasingly relevant social-science issue. Surveillance research generally focuses on control and privacy, whereas sousveillance studies foreground citizen journalism and accountability; however, their intersection in relation to social trust remains underexplored. This theoretical study brings together scholarship on surveillance, sousveillance, trust, privacy, and citizen evidence through purposeful theory synthesis and conceptual analysis based on criterion-guided source selection. It argues that the legitimacy of institutional monitoring depends on proportionality and auditability, whereas the evidential value of citizen records rests on technical verification, contextual integrity, public accessibility, and a reasoned institutional response. The article contributes a model of "proportionate and accountable public scrutiny" that connects institutional, epistemic, and procedural trust with the distinction between records and evidence.

Keywords: Digital Surveillance, Sousveillance, Social Trust, Privacy, Accountability, Citizen Evidence

[*] **Sorumlu yazar / Corresponding author**
[1] Ankara Hacı Bayram Veli Üniversitesi, Rektörlük, Ankara, Türkiye, E-mail: erdi.celebi@hbv.edu.tr, ORCID: https://orcid.org/0009-0001-9454-8792
Başvuru/Submitted: 30.06.2026 **Kabul/Accepted:** 19.08.2026
***Turnitin* Similarity Index** 09%

Çelebi, E., (2026). Dijital gözetimden tersine gözetime: Toplumsal güven, yurttaş kanıtı ve hesap verebilir kamusal açıklık. *IBAD Sosyal Bilimler Dergisi-IBAD Journal of Social Sciences*, (20), 191-209. https://doi.org/10.21733/ibad.1982874

GİRİŞ

Dijital teknolojilerin yaygınlaşması, çağdaş toplumlarda izleme, kayıt alma, veri üretme ve kamusal açıklık pratiklerini gündelik hayatın sıradan bileşenleri arasına taşımaktadır (Lyon, 2018; Trottier, 2012). Güvenlik kameraları, akıllı telefonlar, sosyal medya platformları, konum servisleri, biyometrik sistemler ve algoritmik karar süreçleri teknik araçların ötesinde, toplumsal ilişkilerin hangi aktörlerce, hangi amaçlarla ve hangi koşullarda izlenebilir kılındığını belirleyen sosyo-teknik altyapılardır (Haggerty & Ericson, 2000; van Dijck vd., 2018). Dolayısıyla dijital toplumda gözetim, belli kurumların yukarıdan aşağıya yürüttüğü denetim faaliyetini aşan, veri akışları, platform mantığı, kullanıcı pratikleri ve kamusal tanıklık biçimleriyle birlikte işleyen bir ilişkiler ağıdır (Clarke, 1988; Zuboff, 2019).

Türkiye'de dijital teknolojilerin gündelik yaşama güçlü biçimde yerleşmesi, bu çalışmada ele alınan tartışmayı sosyal bilimler açısından anlamlı kılmaktadır. Türkiye İstatistik Kurumunun (TÜİK) 2025 yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması'na göre 16-74 yaş grubunda internet kullanım oranı 2024'te %88,8 iken 2025'te %90,9'a yükselmiştir (TÜİK, 2025). Bu yaygınlık; kişisel verilerin korunması, dijital kamu hizmetleri, çevrimiçi platform kullanımı, sosyal medya dolaşımı ve gündelik kayıt-paylaşım pratikleri gibi konuların Türkiye'nin güncel sosyal yapısıyla ilişkisini güçlendirmektedir. Ayrıca 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin belirli, açık ve meşru amaçlarla, amaçla bağlantılı, sınırlı ve ölçülü biçimde işlenmesi ilkelerini düzenlemesi, mahremiyet, veri güvenliği ve toplumsal güven tartışmasına Türkiye açısından genel bir hukuki zemin sunmaktadır (Kişisel Verilerin Korunması Kanunu, 2016).

Türkiye'deki akademik yazın, teknolojik izleme pratiklerini toplumsal denetim, beden ve mahremiyet ilişkileri üzerinden tartışırken yeni medya etiği çalışmaları ise kullanıcı üretimli içeriklerde mahremiyet, doğrulama ve sorumluluk sorunlarına dikkat çekmektedir (Dolgun, 2008; İsmayılov & Sunal, 2012; Binark & Bayraktutan, 2013). Kişisel verilerin korunmasına ilişkin hukuk yazını, 6698 sayılı Kanun'daki amaçla bağlantılı, sınırlı ve ölçülü işleme ilkesiyle ölçülülük arasındaki ilişkiyi özellikle hassas veri türleri bakımından ayrıntılandırmaktadır (Küzeci, 2020; Erdinç, 2020). Bu çalışmada "orantılılık", söz konusu hukuki ve akademik çizgiyle uyumlu biçimde, veri toplama ve kayıt paylaşma pratiklerinin amaçla sınırlı tutulması, daha az müdahaleci seçeneklerin gözetilmesi ve ilgili haklara yüklenen külfetin hedeflenen kamusal yararla dengelenmesi anlamında kullanılmaktadır. Türkiye'de yurttaş gazeteciliği ve sosyal medya üzerine yayınların artmasına rağmen (Akyüz & Öztat, 2025), bu alanın gözetim, kanıt ve toplumsal güven ekseninde bir arada ele alınması sınırlı kalmaktadır. Bu değişim iki hatta ilerlemektedir. Birinci hatta kamu kurumları, platform şirketleri, işverenler, medya kuruluşları ve hizmet sağlayıcılar; güvenlik, idari düzen, risk azaltma, hizmet verimliliği veya kullanıcı deneyimini iyileştirme gibi gerekçelerle veri toplama ve izleme kapasitelerini genişletmektedir (Lyon, 2007; Ziller & Helbling, 2021). İkinci hatta ise yurttaşlar, medya profesyonelleri, sivil toplum aktörleri ve sıradan kullanıcılar akıllı telefonlar ve sosyal medya aracılığıyla kamusal olayları, kurumsal süreçleri veya gündelik karşılaşmaları kaydedebilmekte ve bu kayıtları çevrimiçi dolaşıma sokabilmektedir (Brucato, 2015; Mann vd., 2003; Thompson, 2005). Böylece kurumların bireyleri veriler üzerinden izleyebildiği, bireylerin de kamusal olayları ve kurumsal süreçleri kayıt altına alabildiği çift yönlü bir kamusal açıklık düzeni ortaya çıkmaktadır (Mann ve Ferenbok, 2013; Thompson, 2005).

Bu çift yönlü açıklık düzeni, dijital toplumda güven sorununu yalnızca "kim izliyor?" sorusuna indirgemeyi güçleştirmektedir. Kurumsal gözetim süreklilik, altyapı, arşivleme ve sınıflandırma kapasitesiyle işlerken, yurttaş kaydı çoğu zaman olay anına, kayıt cihazına, platform dolaşımına ve kamusal ilgiye bağlıdır. Bu farklılık, gözetim ile tersine gözetimi basit bir karşıtlık içinde

değil, eşit olmayan iki açıklık pratiği olarak değerlendirmeyi gerektirmektedir. Kurumsal veri işleme ve izleme süreçleri güvenilirlik, şeffaflık ve ölçülülük beklentisiyle birlikte değerlendirilirken, bireylerin kayıt pratikleri de çoğu zaman olayların açıklığa kavuşturulması ve kamusal bilginin tamamlanması ihtiyacıyla ilişkilendirilmektedir. Böyle bir zeminde asıl mesele, daha fazla kayıt ya da daha fazla veri toplama değil, kayıt ve verinin hangi güvence, hangi kanıt standardı ve hangi değerlendirme süreci içinde ele alınacağıdır.

Literatürde kurumsal gözetim hakkında iki ana vurgu öne çıkmaktadır. Bir yaklaşım, gözetimin güvenlik tehdidinin belirginleştiği durumlarda kamu desteği bulabildiğini ve risk yönetimi bakımından işlevsel görülebildiğini ortaya koymaktadır (Ziller & Helbling, 2021). Diğer yaklaşım ise gözetimin mahremiyet, özdenetim, sınıflandırma, veri güvenliği ve uygulama ilkeleri bakımından dikkatle değerlendirilmesi gerektiğini vurgulamaktadır (Foucault, 1995; Nissenbaum, 2004; Richards, 2013; Solove, 2008). Tersine gözetim literatüründe de benzer bir ikilik vardır. Bir tarafta yurttaş kaydı, gözden kaçanı kamusal tartışmaya taşıma, olaylara ilişkin ek bilgi üretme ve hesap verebilirlik beklentisini destekleme kapasitesi sayesinde kamusal bir imkan olarak ele alınmaktadır (Bakir, 2010; Brucato, 2015; Mann vd., 2003). Buna karşılık tersine gözetim kavramının sınırları, güç farkı, karşılıklılık, kontrol ve ahlaki değer bakımından dikkatle belirlenmediğinde kavramsal belirsizliğin ortaya çıkabileceği iddia edilmektedir (Thomsen, 2019).

Bu çalışmanın çıkış noktası, gözetim ve tersine gözetim literatürlerinin çoğu zaman ayrı güzergahlarda ilerlemesidir. Gözetim çalışmaları ağırlıkla güvenlik, mahremiyet, veri toplama, disiplin ve iktidar ilişkilerine yoğunlaşırken, tersine gözetim tartışmaları yurttaş gazeteciliği, dijital aktivizm, kamusal tanıklık ve hesap sorma pratikleri üzerinden gelişmektedir. Oysa iki alanın kesişiminde daha temel bir güven sorunu yer almaktadır. Kurumsal gözetim, güvenlik ve hizmet verimliliği gerekçeleriyle kurumsal güvenilirlik beklentisi üretirken tersine gözetim ise mevcut bilginin tamamlanmasına, olayların farklı açılardan belgelenmesine veya kamusal tartışmaya ek tanıklık sunulmasına katkı sağlayabilmektedir. Böylece tartışmanın odağı kimin kimi izlediği sorusundan, kamusal açıklığın hangi güven ilişkisi, hangi kanıt standardı ve hangi değerlendirme mekanizması içinde anlam kazandığı sorusuna kaymaktadır.

Bu boşluğa cevap vermek üzere makale, kurumsal izleme ile yurttaş kaydını aynı açıklama düzeninde buluşturan üç katmanlı bir güven mimarisi önermektedir. Model, kurumsal izleme hattında amaç, kapasite ve normatif güvenilirliği, tersine gözetim hattında ise kaydın kökeni, bütünlüğü, olay bilgisi, teknik doğrulaması ve gerekçeli karşılık koşullarını birlikte ele almaktadır. Çalışmanın özgün katkısı, literatürde ayrı ayrı incelenen kurumsal, epistemik ve prosedürel güven biçimlerini çift yönlü kayıt kapasitesi ve kayıt-kanıt zinciriyle ilişkilendirmesinde yatmaktadır. Böylelikle kamusal açıklığın değeri, açıklığın miktarına göre değil, haklara duyarlılık, kanıt standartları ve hesap verebilirlik mekanizmalarının birlikte işleyişine göre değerlendirilmektedir.

Çalışma şu şekilde yapılandırılmıştır. İlk olarak yöntem bölümünde araştırma deseni, kuramsal kaynakların kapsamı, kaynak belirleme süreci, kavramsal çözümleme adımları, analitik geçerlik ve etik durum açıklanmaktadır. Ardından gözetim, tersine gözetim ve komşu kavramların sınırları çizilmektedir. İzleyen bölümde toplumsal güven, kurumsal, epistemik ve prosedürel katmanlarıyla ele alınmaktadır. Daha sonra kurumsal gözetimin güvenlik vaadi, mahremiyet ve meşruiyetle ilişkisi tartışılmakta ve tersine gözetim ise yurttaş kaydı ve yurttaş kanıtı ayrımı üzerinden değerlendirilmektedir. Son bölümde orantılı ve hesap verebilir kamusal açıklık modeli ve buna bağlı kavramsal önermeler sunulmaktadır.

YÖNTEM

Bu çalışma, dijital gözetim ve tersine gözetim arasındaki ilişkiyi toplumsal güven, mahremiyet, yurttaş kanıtı ve hesap verebilirlik ekseninde açıklamayı amaçlayan teorik bir makale olarak tasarlanmıştır. Bilimsel çalışmalarda yöntem, araştırma sorusuna uygun bilgi üretme yolunun sistematik biçimde belirlenmesini gerektirmektedir (Creswell & Creswell, 2018; Karasar, 2016; Neuman, 2014). Bu çalışmanın problemi belirli bir kullanıcı grubunun tutumunu ölçmeye, belirli bir platformdaki kayıtları sayısal olarak analiz etmeye ya da tekil bir olayın söylemini çözümlemeye yönelik değildir. Çalışma, gözetim ve tersine gözetim literatürlerinde ayrı hatlarda gelişen kavramları toplumsal güven odağında yeniden ilişkilendirmeyi hedeflemektedir. Çalışma herhangi bir güncel siyasal olay, hükümet uygulaması, parti politikası veya belirli bir kamu kurumu üzerine vaka analizi yürütmemektedir. Türkiye ile kurulan ilişki, dijitalleşmenin yaygınlığı ve kişisel verilerin korunmasına ilişkin genel hukuki çerçeveyle sınırlıdır.

Araştırma Deseni

Çalışmanın araştırma deseni teorik araştırma desenidir. Teorik/kavramsal çalışmalar, ampirik veri setlerinden bulgu üretmek yerine mevcut literatürdeki kavramları, teorileri, sınıflandırmaları ve tartışmaları sistematik biçimde analiz ederek yeni bir açıklama çerçevesi geliştirmeyi amaçlamaktadır (Gilson & Goldberg, 2015; Jaakkola, 2020; Whetten, 1989). Jaakkola'ya (2020) göre kavramsal makalelerde araştırma tasarımının açık biçimde gerekçelendirilmesi, kullanılan kavramların neden seçildiğinin, hangi literatür alanlarından beslendiğinin ve argüman zincirinin nasıl kurulduğunun açıklanması gerekmektedir. Bu çalışma söz konusu gerekliliği dikkate alarak teori sentezi ve kavramsal modelleme çizgisinde ilerlemektedir. Teori sentezi farklı literatür hatlarında dağınık biçimde tartışılan kavramları ortak bir problem etrafında bir araya getirirken kavramsal modelleme ise bu kavramlar arasındaki ilişkiyi açıklayıcı bir çerçeveye dönüştürmektedir.

Kuramsal Kaynak Kapsamı

Bu çalışmanın kuramsal inceleme kaynağı, insan katılımcılardan toplanmış birincil saha verilerinden oluşmamaktadır. İnceleme kapsamına gözetim, tersine gözetim, mahremiyet, toplumsal güven, yurttaş gazeteciliği, dijital aktivizm, platform toplumu ve hesap verebilirlik yazınındaki bilimsel yayınlar ile Türkiye'de kişisel verilerin korunmasına ilişkin temel hukuki düzenleme metinleri alınmıştır. Doküman incelemesi, araştırma problemine ilişkin yazılı materyallerin düzenli ve eleştirel biçimde incelenmesine imkan veren bir bilgi edinme yaklaşımıdır (Bowen, 2009; Yıldırım & Şimşek, 2021). Buradaki doküman incelemesi, ampirik bir belge çözümlemesi üretme amacıyla değil, modelin kurucu kavramlarını belirlemek, farklı yazın alanları arasındaki bağlantıları kurmak ve teorik önermelerin dayanaklarını gün yüzüne çıkarmak amacıyla kullanılmıştır.

Çalışmanın kaynak havuzu beş grupta düzenlenmiştir. Birinci grup gözetim literatürüdür; bu grup kurumsal ve altyapısal izleme pratiklerini açıklamak için kullanılmıştır (Clarke, 1988; Foucault, 1995; Haggerty & Ericson, 2000; Lyon, 2007; Zuboff, 2019). İkinci grup güven ve mahremiyet literatürüdür; bu kaynaklar güvenin belirsizlik, kırılganlık, kurumsal meşruiyet ve kişisel veri koruması ile ilişkisini açıklamak için kullanılmıştır (Baier, 1986; Giddens, 1990; Hardin, 2002; Luhmann, 1979; Mayer vd., 1995; Nissenbaum, 2004; Richards, 2013; Rousseau vd., 1998; Solove, 2008). Üçüncü grup tersine gözetim, yurttaş gazeteciliği ve dijital aktivizm literatürüdür; bu kaynaklar yurttaş kaydının demokratik imkanlarını ve sınırlarını tartışmak için kullanılmıştır (Bakir, 2010; Brucato, 2015; Mann & Ferenbok, 2013; Mann vd., 2003; Thomsen, 2019). Dördüncü grup platform toplumu ve algoritmik aracılık literatürüdür; bu

kaynaklar yurttaş kayıtlarının sosyal medya ortamlarında hangi şartlar altında dolaşıma girdiğini değerlendirmeye imkan vermiştir (Gillespie, 2018; Trottier, 2012; van Dijck vd., 2018). Beşinci grup ise Türkiye'de kişisel verilerin korunması ve dijitalleşmenin toplumsal yaygınlığına ilişkin kaynaklardan oluşmaktadır (Kişisel Verilerin Korunması Kanunu, 2016; TÜİK, 2025).

Kaynak Seçim Süreci

Kaynak belirleme süreci, ölçüt temelli amaçlı kaynak seçimi yoluyla yürütülmüştür. Nitel ve kuramsal çalışmalarda amaçlı seçim, araştırma sorusuna yüksek açıklama gücü sunan bilgi bakımından zengin materyallerin önceden belirlenmiş ölçütler doğrultusunda seçilmesini ifade etmektedir (Patton, 2015; Yıldırım & Şimşek, 2021). Buradaki seçim, belirli bir evreni temsil etmeyi amaçlayan istatistiksel örnekleme işlemi değildir. Modelin kurucu kavramlarını açıklama gücü yüksek çalışmaların kuramsal uygunlukları doğrultusunda belirlenmesidir. Kaynaklar üç ölçüte göre değerlendirilmiştir. İlk ölçüt, çalışmanın gözetim, tersine gözetim, mahremiyet, toplumsal güven veya hesap verebilirlik kavramlarından en az biriyle doğrudan ilişkili olmasıdır. İkinci ölçüt, kaynağın kayıt-kanıt, kamusal açıklık-hesap verebilirlik veya güvenlik vaadi-meşruiyet ayrımlarından birini açıklamaya katkı sunmasıdır. Üçüncü ölçüt ise derginin amaç ve kapsamıyla uyumlu biçimde Türkiye'deki dijitalleşme düzeyi ve kişisel verilerin korunmasına ilişkin genel hukuki çerçeveyle bağlantı kurulmasına imkan vermesidir. Sonuç olarak bu çalışma sistematik derleme iddiası taşımamaktadır. Sistematik derlemeler belirli veri tabanları, anahtar kelimeler, dahil etme-dışlama ölçütleri ve raporlama protokolleriyle literatürü bütüncül biçimde taramayı amaçlamaktadır (Creswell & Creswell, 2018; Neuman, 2014). Bu makalenin amacı ise belirli bir literatür evrenini tüketici biçimde haritalandırmak değil, farklı literatür hatlarında yer alan kavramları ortak bir sosyal bilim problemine cevap verecek biçimde ilişkilendirmektir. Dolayısıyla çalışma, sistematik derleme yerine amaçlı teori sentezi olarak konumlandırılmıştır.

Kavramsal Çözümleme Süreci: Amaçlı Teori Sentezi ve Modelleme

Kavramsal çözümleme, seçilen yazındaki temel kavramların tanımlanması, karşılaştırılması ve aralarındaki ilişkilerin açıklanması yoluyla yürütülmüştür. Süreç dört adımda ilerlemiştir. İlk adımda gözetim, tersine gözetim, karşı-gözetim, yanal gözetim ve katılımcı gözetim kavramlarının sınırları ayrıştırılmıştır. İkinci adımda toplumsal güven kurumsal, epistemik ve prosedürel güven olmak üzere üç katmanda ele alınmıştır. Üçüncü adımda kurumsal gözetimin meşruiyeti ile tersine gözetimin yurttaş kanıtı üretme kapasitesi aynı açıklama zinciri içinde değerlendirilmiştir. Son adımda bu ayrımlar "orantılı ve hesap verebilir kamusal açıklık" modeli altında birleştirilmiş ve gelecekteki araştırmalara yön verecek beş teorik önerme formüle edilmiştir. Bu analiz mantığı, kavramsal makalelerde teori kurmanın yalnızca kaynak aktarmakla sınırlı olmadığı varsayımına dayanmaktadır. Sutton ve Staw'a (1995) göre teori, referans listesi, değişken sıralaması veya veri sunumu değil, kavramlar arasındaki ilişkinin neden ve nasıl kurulduğunu açıklayan bir düşünsel yapıdır. Whetten (1989) ise teorik katkının neyin açıklandığı, kavramların nasıl ilişkilendiği, bunun neden böyle olduğu ve hangi koşullarda geçerli sayılabileceği soruları üzerinden değerlendirilmesi gerektiğini vurgulamaktadır. Bu çalışmadaki ampirik nedensellik testi iddiası taşımayan kavramsal model de, gözetim, tersine gözetim ve toplumsal güven arasındaki ilişkileri sonraki araştırmalar için sınanabilir bir açıklama çerçevesine dönüştürmeyi amaçlamaktadır.

Analitik Geçerlik veTutarlılık

Teorik/kavramsal çalışmalarda analitik geçerlik, kavramların açık biçimde tanımlanması, kaynak seçiminin araştırma problemiyle uyumlu tutulması, argüman zincirinin izlenebilir

biçimde kurulması ve önerilen modelin ilgili yazınla tutarlı biçimde ilişkilendirilmesiyle güçlenmektedir (Creswell & Creswell, 2018; Jaakkola, 2020; Neuman, 2014). Bu çalışmada kavramların sınırları tablolar aracılığıyla ayrıştırılmış; kayıt-kanıt, kamusal açıklık-hesap verebilirlik ve güvenlik vaadi-meşruiyet ayrımları gerekçelendirilmiş; modelin ampirik bir test sonucu değil, sınanabilir bir teorik açıklama çerçevesi olduğu açıkça belirtilmiştir. Analitik tutarlılık, kaynak seçimi ve çözümleme adımlarının şeffaf biçimde raporlanmasıyla sağlanmaya çalışılmıştır. Modelin beslendiği yazın grupları, kaynak seçim ölçütleri ve kavramlar arasındaki ilişki açıkça belirtilerek önermelerin ampirik hipotezlerden ziyade gelecekte sınanabilecek teorik yönelimler olduğu vurgulanmıştır.

Etik Beyan

Araştırma insan katılımcılarla yürütülmemiş, anket, görüşme, deney veya kişisel veri toplama süreci içermemiştir. Bu sebeple etik kurul onayı gerektiren bir saha araştırması niteliği taşımamaktadır. Çalışma, bilimsel araştırma ve yayın etiği ilkeleri uyarınca tüm kaynakların açık biçimde gösterilmesini ve kavramsal çıkarımların ilgili yazınla sınırlandırılmasını esas almaktadır.

KAVRAMSAL SINIRLAR: GÖZETİM, TERSİNE GÖZETİM VE KOMŞU PRATİKLER

Dijital gözetim tartışmasının sağlıklı ilerleyebilmesi için gözetim, tersine gözetim ve komşu kavramların sınırlarını belirlemek gerekmektedir. Gözetim, en genel anlamıyla bireylerin, grupların, mekanların, davranışların veya veri akışlarının izlenmesi, kaydedilmesi, sınıflandırılması ve belirli amaçlarla kullanılmasıdır (Lyon, 2007; Marx, 2002). Gözetimin disiplin, kamusal açıklık ve özdenetim ilişkisi içinde işlediği panoptikon tartışması klasik gözetim literatürünün temel dayanaklarından biridir (Foucault, 1995). Çağdaş gözetim çalışmaları bu ilişkiyi veri tabanları, algoritmalar, platform arayüzleri ve otomatik karar sistemleri üzerinden genişletmiştir (Clarke, 1988; Haggerty & Ericson, 2000; Lyon, 2007; Zuboff, 2019). Dolayısıyla dijital gözetim, tek bir merkezden yürüyen görsel denetimden çok, dağılmış veri toplama ve sınıflandırma ağlarıyla ilişkilidir (Haggerty & Ericson, 2000; van Dijck vd., 2018). Türkiye'deki gözetim çalışmaları da teknolojik izleme pratiklerini toplumsal denetim, beden ve mahremiyet ilişkileri üzerinden ele alarak sosyal medya ortamlarında gözetlenen ile gözetleyenin rollerinin iç içe geçebildiğine dikkat çekmiştir (Dolgun, 2008; İsmayılov & Sunal, 2012).

Tersine gözetim (sousveillance), izlenenlerin de izleme kapasitesi kazanmasını ifade etmektedir (Mann vd., 2003). Kavram, bireylerin kendi kayıt cihazlarıyla gözetim ortamlarında yukarıya doğru bakış geliştirmeleri kapsamında tanımlanmıştır (Mann vd., 2003). Tersine gözetim özellikle bireylerin veya kurumsal kaynağı sınırlı aktörlerin kamusal rol üstlenen kişileri, kurumları ya da kurumsal süreçleri kaydetmesi durumunda önem kazanmaktadır (Mann & Ferenbok, 2013; Thomsen, 2019). Bu yüzden tersine gözetim, kurumsal gözetimin basit karşıtı sayılmaktan ziyade, belirli olayların farklı açılardan belgelenmesine ve kamusal bilginin tamamlanmasına katkı sunabilen olay-temelli ve aracılı bir kayıt pratiği olarak okunmalıdır. Bu noktada tersine gözetimin farklı biçimlerini ayırmak gerekmektedir. Mann çizgisinde kişisel tersine gözetim, bireyin kendi deneyimini birinci kişi perspektifinden kaydetmesiyle ilişkilidir. Hiyerarşik tersine gözetim ise otorite temsilcilerinin, kurumların veya güç sahiplerinin eylemlerinin aşağıdan yukarıya doğru kaydedilmesini ifade etmektedir (Mann vd., 2003). Bu çalışmanın odağı özellikle hiyerarşik tersine gözetimdir. Çünkü toplumsal güven, yurttaş kanıtı ve hesap verebilirlik sorunu en açık biçimde güç sahibi aktörlerin kayıt altına alındığı

durumlarda ortaya çıkmaktadır. Sosyal medyanın akıllı telefonlarla birleşmesi, Bakir'in (2010) ifadesiyle tersine gözetim pratiklerinin yoğunlaşmasına zemin hazırlamıştır.

Bu noktada üç ayrım önemlidir. Karşı-gözetim, gözetim teknolojilerini veya gözetim pratiklerini fark etme, sınırlandırma, bozma ya da tersine çevirme yoluyla izleme süreçlerine karşı dengeleyici stratejiler geliştirme girişimlerini ifade etmektedir (Monahan, 2006). Yanal gözetim, bireylerin arkadaşları, aile üyeleri, potansiyel ilişkileri veya diğer sıradan kullanıcıları izlemesi ve onlar hakkında bilgi toplamasıyla ilişkilidir (Andrejevic, 2004; Trottier, 2012). Katılımcı gözetim ise özellikle çevrimiçi sosyal ağlarda kullanıcıların kendileri ve başkaları hakkında bilgi paylaşarak gözetim süreçlerine gündelik, gönüllü ve kimi zaman güçlendirici biçimde katılmasıdır (Albrechtslund, 2008). Bu ayrımlar, tersine gözetimin demokratik hesap verebilirlik potansiyelini yanal ifşa kültürü, teknik kaçınma pratikleri veya gönüllü platform katılımıyla karıştırmamak için gereklidir.

Tablo 1. *Gözetim ve ilişkili kavramların toplumsal güven açısından konumları*

Kavram	Temel yönelim	Toplumsal güven açısından anlamı	Temel risk
Kurumsal gözetim	Kurumların veri toplama, izleme ve sınıflandırma kapasitesi	Güvenlik vaadiyle meşruiyet arar; mahremiyet ve denetim güvencesi gerektirir.	Amaç dışı kullanım, mahremiyet sorunu, veri güvenliği ve ölçülülük tartışması.
Tersine gözetim	Yurttaşın veya güçsüz aktörün güç sahibini kaydetmesi	Kurumsal güven açığında kanıt üretme ve hesap sorma potansiyeli taşır.	Eksik kayıt, yanlış yorum, kişisel hakların zedelenmesi veya kurumsal yanıt eksikliği.
Karşı-gözetim	Gözetimi tespit etme, engelleme veya atlatma	Gözetim kapasitesine direnç üretir; güven yerine kaçınma stratejisi öne çıkar.	Güven ilişkisini onarmaktan çok savunmacı pratikleri güçlendirme.
Yanal gözetim	Bireylerin birbirlerini izlemesi veya ifşa etmesi	Toplumsal denetim ve mahremiyet ihlali riski doğurabilir.	Gündelik ilişkilerde kuşku, takip ve sosyal baskı üretme.
Katılımcı gözetim	Kullanıcıların gözetim süreçlerine gündelik pratiklerle katılması	Gönüllülük ve alışkanlık üzerinden veri üretimini normalleştirebilir.	Veri üretimini gönüllülük ve alışkanlık üzerinden normalleştirme.

Kaynak: *Yazar tarafından Mann vd. (2003), Thomsen (2019), Andrejevic (2004), Albrechtslund (2008) ve Trottier (2012) temel alınarak oluşturulmuştur.*

TOPLUMSAL GÜVEN, MAHREMİYET VE GÖZETİMİN MEŞRUİYETİ

Bu çalışmada dijital kamusal açıklık düzeninin meşruiyetini mümkün kılan çok katmanlı bir ilişki olarak ele alınan toplumsal güven, tek boyutlu iyi niyet ya da olumlu duygu düzeyine indirgenmemektedir. Güven, belirsizlik ve kırılganlık koşullarında anlam kazanır (Baier, 1986; Luhmann, 1979; Mayer vd., 1995; Rousseau vd., 1998). Giddens'ın soyut sistemlere güven tartışması dijital gözetim konusunda özellikle önem arz etmektedir. Çünkü yurttaşlar çoğu zaman verilerinin nasıl toplandığını, işlendiğini ve hangi karar süreçlerine bağlandığını doğrudan izleyemez (Giddens, 1990). Bu kapsamda gözetim, teknik kapasitenin yanında soyut sistemlere ve kurumsal düzenlemelere güven meselesidir (Giddens, 1990; Lyon, 2018).

Dijital kamusal açıklık düzeninde toplumsal güven üç katmanda düşünülebilir. Kurumsal güven, yurttaşların kamu kurumlarına, platform şirketlerine, düzenleyici yapılara, hizmet sağlayıcılara ve teknoloji kurumlarına duyduğu güvendir (Hardin, 2002; Luhmann, 1979). Epistemik güven, dijital kayıtların, verilerin, belgelerin veya tanıklıkların gerçek, olay bilgisi tamamlanmış ve güvenilir olduğuna ilişkin değerlendirmedir. Prosedürel güven ise gözetim

veya tersine gözetim sonucunda işleyen inceleme, itiraz, doğrulama, düzeltme ve hesap verme süreçlerine duyulan güvendir (Bovens, 2007). Bu üç katman iç içedir. Kurum güvenilir olsa bile kayıt doğrulanamıyorsa, kayıt doğru olsa bile prosedür işlemiyorsa toplumsal güven zayıflar. Örneğin bir güvenlik kurumuna genel düzeyde güven duyulabilir fakat o kurumun belirli bir olaya ilişkin sunduğu görüntü, belge veya veri doğrulanamıyorsa epistemik güven zedelenir. Tersinden, bir yurttaş kaydı teknik olarak doğru ve özgün olabilir ancak bu kaydı inceleyen, değerlendiren veya sonuç üreten adil bir süreç bulunmuyorsa prosedürel güven kurulamaz. Benzer biçimde platform şirketi yüksek teknik kapasiteye sahip olabilir, buna rağmen veri işleme süreçlerinin şeffaf olmaması kurumsal güveni zayıflatabilir. Bu yüzden dijital kamusal açıklık düzeninde toplumsal güven, tek bir kaynağa yönelen genel bir inanç olarak değil, kurumların güvenilirliği, kanıtların doğrulanabilirliği ve süreçlerin hesap verebilirliği arasında kurulan ilişkisel bir yapı olarak değerlendirilmelidir.

Epistemik güven, bir bilgi iddiasının yalnızca içeriğine bakılarak değil, iddiayı ileten kaynakların, tanıklıkların ve doğrulama süreçlerinin güvenilirliği değerlendirilerek kabul edilmesini ifade etmektedir. Hardwig (1991), modern bilgi üretiminin uzmanlara ve başkalarının tanıklığına duyulan güven olmadan sürdürülemeyeceğini savunmaktadır. Origgi (2012) epistemik güvenin bilgi aktarımında kaynağın niteliği ve sosyal ilişkinin değerlendirilmesini gerektirdiğini, Sperber vd. (2010) ise alıcıların kaynak, içerik ve iletişim koşullarını sınayan epistemik uyanıklık mekanizmalarından yararlandığını açıklamaktadır. Dijital kayıtlar bakımından bu katman, kaydın kaynağına, teknik bütünlüğüne, eşlik eden olay bilgisine ve doğrulama sürecine ilişkin değerlendirmelerin birlikte işletilmesini gerektirmektedir.

Kurumsal gözetim çoğu zaman güvenlik vaadiyle meşrulaştırılmaktadır. Kamu kaynaklı izleme tedbirlerine yönelik toplumsal desteğin hedeflenen kişi grubu, güvenlik tehdidinin kamusal alandaki ağırlığı ve veri güvenliği gibi koşullara bağlı olarak değişebildiği ortaya konmuştur (Ziller & Helbling, 2021). Ancak güvenlik iddiası tek başına meşruiyet üretmez. Güven genel ve sınırsız bir tutumdan çok, belirli bir aktöre, belirli bir konuda ve belirli koşullarda yönelir (Hardin, 2002). Yurttaş bir kurumun güvenlik amacıyla veri toplamasını kabul edebilir fakat aynı verinin amaç dışı kullanılmayacağına, güvenli saklanacağına, denetlenebileceğine ve itiraz edilebilir olduğuna ilişkin güvence bekler. Bu kapsamda kurumsal veri işleme ve izleme süreçleri, birey açısından belirli mahremiyet ve veri güvenliği hassasiyetleri doğurabilir. Kişisel verilerin, hareketlerin veya davranış izlerinin kaydedilmesi bireyin kendisi hakkında üretilen bilgi üzerindeki kontrolünü azaltabilir (Richards, 2013; Solove, 2008). Mahremiyet burada bütünüyle saklı kalma talebine indirgenemez. Bağlamsal bütünlük yaklaşımı, mahremiyetin bilginin hangi şartlarda, hangi aktörler arasında ve hangi normlara göre dolaştığıyla ilişkili olduğunu vurgulamaktadır (Nissenbaum, 2004, 2010). Bir veri belirli bir güvenlik amacıyla meşru biçimde toplanabilir ancak başka bir amaçla, başka aktörlere veya üretildiği şartlardan koparılarak aktarıldığında mahremiyet ve güven sorunu doğar (Nissenbaum, 2004; Solove, 2008). Türkiye'de kişisel verilerin korunmasına ilişkin çalışmalar, veri işleme faaliyetlerinin hukuka uygunluk, amaçla bağlantı, veri minimizasyonu ve ölçülülük ilkeleriyle birlikte değerlendirilmesi gerektiğini vurgulamaktadır (Küzeci, 2020). Biyometrik veriler üzerine yapılan incelemeler de ölçülülüğün mahremiyet ve güvenlik arasındaki dengeyi kuran temel bir ilke olarak değerlendirilmesi gerektiğine işaret etmektedir (Erdinç, 2020).

Kurumsal gözetimin meşruiyeti üç güven sorusuyla sınanabilir. Amaç güveni, gözetimin gerçekten belirtilen amaçla sınırlı kalıp kalmadığına ilişkindir. Kapasite güveni, kurumun veriyi güvenli ve yetkin biçimde işleyip işleyemeyeceğine ilişkindir. Normatif güvenilirlik ise gözetimin hukuk, etik, orantılılık ve hesap verebilirlik ilkeleriyle uyumlu olup olmadığına

ilişkindir. Böylece güvenlik ile mahremiyet arasında basit bir sıfır toplam ilişkisi kurmak yerine, gözetimin hangi güvenceler altında meşru görülebileceği tartışılabilir. Bu ayrım, çalışmanın temel savı açısından belirleyicidir. Güvenlik vaadi, gözetimin gerekçesini kurabilir. Meşruiyet ise bu gerekçenin nasıl sınırlandırıldığıyla ilgilidir. Bir gözetim pratiği güvenlik amacı taşısa bile hangi verinin toplandığı, verinin ne kadar süre saklandığı, kimlerin erişimine açıldığı, hangi denetim mekanizmalarına bağlı olduğu ve yurttaşın hangi itiraz yollarına sahip bulunduğu açıklığa kavuşmadıkça toplumsal güven üretemez. Başka bir ifadeyle güvenlik iddiası gözetimi başlatan gerekçe olabilir fakat gözetimin toplumsal olarak kabul edilebilir sayılması orantılılık, amaçla sınırlılık, şeffaflık ve hesap verebilirlik koşullarına bağlıdır.

TERSİNE GÖZETİM VE YURTTAŞ KANITI: İMKANLAR VE SINIRLAR

Tersine gözetim, çoğu zaman kamusal olayların farklı açılardan belgelenmesine ve olay hakkında ek bilgi üretilmesine yönelik bir kayıt pratiği olarak gündeme gelmektedir. Yurttaşlar, medya profesyonelleri, sivil toplum aktörleri veya sıradan kullanıcılar, bir olayın daha iyi anlaşılması, farklı tanıklıkların kamusal dolaşıma girmesi ya da mevcut bilginin tamamlanması amacıyla kayıt alma pratiğine başvurabilir (Bakir, 2010; Brucato, 2015). Bu anlamda tersine gözetim, kurumsal gözetimle simetrik bir ilişki kurmaz. Kurumsal gözetim altyapısal, sürekli ve veri depolamaya dayalı iken tersine gözetim çoğu zaman olay-temelli, sınırlı ve platform aracılığına bağımlıdır (Brucato, 2015; Mann & Ferenbok, 2013).

Tersine gözetimin ortaya çıkışını tek bir nedene bağlamak güçtür. Cop-watching grupları üzerine iki yıllık katılımcı gözlem ve görüşmelere dayanan Bock (2016), kayıt pratiklerinin yurttaşlık, tanıklık ve görsel kanıt üretimi arasında kurulduğunu belirtmektedir. Mohler vd. (2022) tarafından yürütülen deney ise çevrimiçi videoların kurumsal meşruiyet algılarını, görüntülerin olumlu ya da olumsuz niteliğine bağlı biçimde değiştirebildiğini ortaya koymaktadır. Wilson ve Serisier (2010) de video aktivizminin hesap verebilirlik potansiyelinin kaydın üretilmesi kadar dolaşım ve yorum koşullarına bağlı olduğunu savunmaktadır. Bu bulgular, tersine gözetimi yalnızca önceden var olan bir "kurumsal güven açığının" sonucu saymak yerine, ek bilgi ve belgeleme ihtiyacı, kamusal tanıklık, meşruiyet değerlendirmesi ve olayın medyadaki temsilini tamamlama arayışıyla ilişkili çok nedenli bir pratik olarak ele almayı gerektirmektedir.

Literatürde tersine gözetimin demokratik potansiyelinin, saklı kalanı kamusal tartışmaya taşıma kapasitesinden kaynaklandığı iddia edilmektedir (Mann vd., 2003; Thompson, 2005). Akıllı telefonlar ve sosyal medya platformları, kamusal olayların resmî kaynaklar ya da profesyonel medya yanında olay yerindeki yurttaşlar tarafından da kaydedilmesini mümkün kılmıştır (Brucato, 2015; Trottier, 2012). Böylece kurumsal süreçler, kamusal olaylar veya gündelik karşılaşmalar kullanıcı kayıtları aracılığıyla çevrimiçi tartışmaya konu olabilir (Brucato, 2015; Thompson, 2005). Bu pratik, yurttaş gazeteciliği, dijital aktivizm ve kamusal tanıklık bakımından önemli bir imkan sunmaktadır (Bakir, 2010; Mann vd., 2003). Türkiye'de yeni medya etiği ve yurttaş gazeteciliği yazını, kullanıcıların haber üretim ve dağıtım süreçlerine katılımının ifade imkanlarını genişletirken doğrulama, mahremiyet ve sorumluluk sorunlarını da beraberinde getirdiğini tartışmaktadır (Binark & Bayraktutan, 2013; Akyüz & Öztat, 2025).

Bu makalede kullanılan "yurttaş kanıtı" ifadesi, bütünüyle yeni ve daha önce kullanılmamış bir terim olarak sunulmamaktadır. Allan'ın (2013) "citizen witnessing" yaklaşımı sıradan kullanıcıların kriz anlarındaki tanıklık ve haber üretme rollerini, Farrell ve Allan (2015) yurttaş videolarının insan hakları savunuculuğundaki işlevini, Dubberley vd. (2020) ise açık kaynaklı dijital materyalin soruşturma, belgeleme ve hesap verebilirlik süreçlerinde nasıl değerlendirilebileceğini tartışmaktadır. Amnesty International'ın Citizen Evidence Lab girişimi

de kullanıcı üretimli görüntülerin doğrulanmasına yönelik araç ve rehberleri "citizen evidence" başlığı altında bir araya getirmektedir (Amnesty International, 2019). Bu çalışma terimi, söz konusu kullanımları temel alarak daha dar bir analitik anlamda kullanmaktadır: yurttaş tarafından üretilen kayıt, teknik özgünlük ve bütünlük, bağlamsal bütünlük, kamusal erişim ve gerekçeli kurumsal yanıt koşullarını karşıladığı ölçüde yurttaş kanıtı niteliğine yaklaşmaktadır.

Yurttaş kaydı kendiliğinden yurttaş kanıtı niteliği kazanmamaktadır. Kayıt, bir olayın dijital izidir; kanıt ise teknik olarak doğrulanmış, bağlamsal bütünlüğü kurulmuş ve hesap verme sürecinde kullanılabilir nitelik kazanmış kayıttır. Bir görüntü gerçek olsa dahi olayın öncesini, sonrasını, ses bütünlüğünü veya ilgili aktörlerin konumunu aktarmıyorsa yanlış yorumlara açık kalabilir. Buradan hareketle yurttaş kanıtı tekil bir görüntüden çok kaydın üretilmesi, özgünlük ve bütünlük bakımından sınanması, olayın zamanı, yeri, aktörleri ve öncesi-sonrası hakkında tamamlayıcı bilginin kurulması, kamusal erişime açılması ve gerekçeli kurumsal yanıt sürecine bağlanması gibi faktörleri içeren bir kanıt zinciri olarak düşünülmelidir. Bu zincirin halkalarından biri eksildiğinde kayıt yoğun ilgi uyandırsa bile hesap verebilirlik sürecine sınırlı katkı sunabilir (Bovens, 2007; Dubberley vd., 2020).

Tersine gözetimin ilk sınırı kaydın parçalı doğasıdır. Kamera kadrajı, ses kalitesi, kayıt anının başlangıcı ve bitişi, olayın yorumlanmasını doğrudan etkiler. İkinci sınır platform aracılığıdır. Bir kayıt sosyal medyaya yüklendiğinde belge niteliğinin yanına algoritmik sıralama, yorum, beğeni, paylaşım ve moderasyon düzeni içinde dolaşan içerik niteliği eklenir (Gillespie, 2018; van Dijck vd., 2018). Platformlar kaydın erişimini ve kamusal etkisini artırabilir fakat olay bilgisini kısaltabilir, duygusal tepkileri öne çıkarabilir veya içeriği başka tartışmaların malzemesi yapabilir (Gillespie, 2018; van Dijck vd., 2018). Reilly'nin Stokes Croft olayına ilişkin YouTube yorumları üzerine yaptığı çalışma, bu sorunu örneklendirmektedir. Çalışma, tersine gözetim görüntülerinin alternatif bakış açılarını kamusal dolaşıma sokabildiğini ancak yorumcuların her zaman görüntüleri hiyerarşik tersine gözetim olarak okumadığını ve çoğu zaman mevcut medya anlatılarının etkisi altında tartıştığını ortaya koymaktadır (Reilly, 2015). Bu bulgu, yurttaş kaydının platforma yüklenmesinin tek başına rasyonel kamusal tartışma veya hesap verebilirlik doğurmadığını hatırlatmaktadır. Kayıt, platform üzerinde dolaşıma girdiği anda yalnızca belge olarak değil, yorum, öfke, kutuplaşma, alay, şüphe ve medya çerçeveleriyle birlikte işleyen bir kamusal nesne olarak varlık kazanır. Böylece tersine gözetimin demokratik değeri, kayıt cihazının varlığından ziyade kaydın doğrulanabilirliği, haklara duyarlılığı, platformda nasıl dolaşıma girdiği ve hesap verme sürecine bağlanıp bağlanmadığı üzerinden belirlenmektedir. Üçüncü sınır mahremiyet ve üçüncü kişilerin haklarıdır. Tersine gözetim kamusal rol üstlenen aktörleri ve kurumsal süreçleri belgelemeyi amaçlasa da kayıtlar olay yerindeki mağdurları, çocukları, tanıkları veya ilgisiz kişileri de açığa çıkarabilir (Nissenbaum, 2004; Solove, 2008). Bir diğer sınır kurumsal karşılık eksikliğidir. Kayıt geniş kitlelere ulaşsa bile açıklama, inceleme, değerlendirme veya düzeltme süreci oluşmadığında kamusal açıklığın hesap verebilirliğe katkısı sınırlı kalabilir (Bovens, 2007; Brucato, 2015).

Üretken yapay zeka çağında yurttaş kaydının epistemik statüsü iki yönlü baskı altına girmektedir. Sentetik içerikler hiç gerçekleşmemiş olayların gerçekçi görüntülerini üretebilirken, sentetik medya farkındalığı gerçek kayıtların da "yapay" veya "manipüle edilmiş" olduğu iddiasıyla reddedilebilmesine elverişli bir şüphe alanı yaratmaktadır (Chesney & Citron, 2019; Fallis, 2021; Rini, 2020). Deneysel araştırmalar, derin sahte (deepfake) içeriklerin her zaman doğrudan aldatma üretmese bile belirsizliği artırarak sosyal medyadaki haberlere duyulan güveni azaltabildiğini ortaya koymaktadır (Vaccari & Chadwick, 2020). Epistemik güvenin zedelenmesi yalnızca kaydın sahte olmasından kaynaklanmamaktadır. Gerçek ve sentetik kayıtları ayırt etmeye yarayan işaretlerin güvenilirliğinin aşınması da benzer bir sonuç

doğurmaktadır. Bu şartlarda yurttaş kaydının kanıt değeri yalnızca kurumsal yanıtla değil, teknik doğrulama mimarisiyle de ilişkilidir. Böyle bir mimari; dosyanın köken ve düzenleme geçmişini belgeleyen provenans bilgilerini, bütünlük kontrollerini, zaman ve konum tutarlılığını, açık kaynak karşılaştırmalarını, görsel-işitsel incelemeyi ve insan denetimli kurumsal değerlendirmeyi birlikte işletmektedir (Dubberley vd., 2020). C2PA içerik kimlik bilgileri gibi standartlar, dijital materyalin üretim ve düzenleme geçmişine ilişkin imzalı bilgiler sağlayarak kaynağın izlenebilirliğini güçlendirmeyi amaçlamaktadır (Coalition for Content Provenance and Authenticity, 2025). Kaydın doğruluğunu tek başına garanti etmesi mümkün olmayan bu araçlar, kaynağın, bütünlüğün ve işlem geçmişinin denetlenmesine yardımcı olarak yalnızca epistemik güvenin kurulmasını destek işlevi üstlenebilmektedir.

Yukarıda bahsedilen sınırlılıklar tersine gözetimin değerini ortadan kaldırmamaktadır. Aksine, tersine gözetimin demokratik niteliğini korumak için hangi durumda kanıt, hangi durumda ifşa, hangi durumda bağlamdan koparma ve hangi durumda hesap sorma pratiği niteliği taşıdığını ayırt etmek gerekir. Kamusal açıklık dikkat üretir; hesap verebilirlik ise cevap, gerekçe, denetim ve sonuç gerektirir (Bovens, 2007; Brighenti, 2007). Tablo 2, yurttaş kaydının hangi koşullarda yurttaş kanıtı niteliği kazanabileceğini ve bu koşulların eksikliğinde hangi sorunların doğabileceğini özetlemektedir.

Tablo 2. *Yurttaş kaydının yurttaş kanıtı değeri kazanma koşulları*

Koşul	Anlamı	Eksikliğinde doğabilecek sorun
Özgünlük	Kaydın sahte, montaj veya manipüle edilmemiş olması	Sahicilik şüphesi ve kanıt değerinin zayıflaması
Bütünlük	Kaydın olayın anlamlı bir kesitini taşıması	Seçici kadraj ve eksik temsil
Teknik doğrulama	Kaynağın, işlem geçmişinin, zaman-konum tutarlılığının ve dosya bütünlüğünün çeşitli araçlarla sınanması	Sentetik veya manipüle edilmiş içeriğin ayırt edilememesi ve epistemik güven kaybı
Bağlamsal bütünlük	Kaydın olayın öncesi, sonrası, aktörleri ve koşullarıyla birlikte değerlendirilmesi	Eksik olay bilgisi ve yanlış yorum
Dolaşım	Kaydın kamusal tartışmaya girebilmesi	Dolaşımdan dışlanma veya algoritmik bastırma
Kurumsal karşılık	Açıklama, inceleme, düzeltme veya yaptırım süreci	Kamusal açıklığın hesap verebilirlik üretmemesi

Kaynak: *Yazar tarafından Bovens (2007), Brucato (2015), Gillespie (2018), Nissenbaum (2004), Chesney ve Citron (2019), Dubberley vd. (2020) ve C2PA (2025) temel alınarak oluşturulmuştur.*

İLGİLİ KAVRAMSAL ÇERÇEVELERLE KARŞILAŞTIRMA VE ÇALIŞMANIN ÖZGÜN KATKISI

Gözetim, mahremiyet, kamusal açıklık ve hesap verebilirlik yazınındaki dört güçlü yaklaşım ile kesişmekte olan bu çalışmada önerilen model, söz konusu yaklaşımların odaklarını tek bir güven mimarisi altında birleştirmektedir. Nissenbaum'ın (2004, 2010) bağlamsal bütünlük yaklaşımı, mahremiyeti bilginin belirli aktörler, amaçlar ve aktarım normları doğrultusunda uygun biçimde dolaşması üzerinden açıklamaktadır. Söz konusu argüman, her ne kadar kurumsal veri akışlarının normatif sınırlarını değerlendirmek bakımından temel bir dayanak sunsa da yurttaş kaydının kanıta yaklaşma sürecini, çift yönlü kayıt kapasitesini ve hesap verebilirlik ilişkisini aynı model içinde ayrıntılandırmamaktadır. Burada önerilen çerçeve,

bağlamsal bütünlüğü koruyarak orantılılık, teknik doğrulama ve kurumsal yanıt koşullarını aynı açıklama zincirine eklemektedir.

Thompson'ın (2005) yeni kamusal açıklık yaklaşımı ile Brighenti'nin (2007) açıklığı toplumsal bir kategori olarak ele alan çalışması, medya aracılığıyla genişleyen izlenebilirlik ve kamusal dikkat süreçlerini açıklamaktadır. Ananny ve Crawford (2018) şeffaflığın tek başına algoritmik hesap verebilirlik üretmediğini, Bovens (2007) ise hesap verebilirliğin açıklama, sorgulama, değerlendirme ve sonuç ilişkisine dayandığını savunmaktadır. Mevcut çalışma, bu iki hattı kayıt-kanıt ayrımıyla birbirine bağlamaktadır. Kamusal açıklık kaydın erişimini artırabilir, fakat kaydın kanıt değeri teknik özgünlük, bağlamsal bütünlük ve gerekçeli yanıt koşullarıyla kurulmaktadır.

Mann vd. (2003) tarafından geliştirilen tersine gözetim yaklaşımı, aşağıdan yukarıya kayıt alma kapasitesinin kurumsal gözetim karşısındaki dengeleyici potansiyelini açıklamaktadır. Söz konusu yaklaşımı kurumsal güven açığına indirgemeyen bu çalışma, ek bilgi ve belgeleme ihtiyacı, kamusal tanıklık, meşruiyet değerlendirmesi ve platform aracılığı gibi farklı güdüleri aynı çerçeveye almaktadır. Ayrıca üretken yapay zeka çağında kaydın epistemik statüsünü teknik doğrulama mimarisiyle ilişkilendirerek klasik tersine gözetim modeline yeni bir koşul eklemektedir.

Çalışmanın özgün katkısı dört düzeyde toplanmaktadır. İlk olarak kurumsal izleme ve yurttaş kaydı, kurumsal, epistemik ve prosedürel güven katmanlarını içeren ortak bir yapı içinde buluşturulmaktadır. İkinci olarak kayıt ile kanıt arasına teknik doğrulama, bağlamsal bütünlük, kamusal erişim ve gerekçeli yanıt aşamalarından oluşan bir kanıt zinciri yerleştirilmektedir. Üçüncü olarak "orantılı ve hesap verebilir kamusal açıklık" modeli, KVKK'daki ölçülülük ilkesiyle ilişkilendirilerek Türkiye'deki hukuki ve toplumsal şartlara uyarlanabilir bir yorum çerçevesi sunmaktadır. Son olarak teorik önermelere eklenen operasyonelleştirme notları, modelin sonraki anket, deney, içerik analizi ve dijital iz araştırmalarında sınanabilmesini kolaylaştırmaktadır.

TARTIŞMA: ORANTILI VE HESAP VEREBİLİR KAMUSAL AÇIKLIK

Dijital toplumun çift yönlü kayıt kapasitesi, kurumsal izleme ile yurttaş kaydını aynı kamusal açıklık düzeninde buluşturmaktadır (Mann & Ferenbok, 2013; Trottier, 2012; van Dijck vd., 2018). Ancak bu ortak zemin, iki pratiğin aynı sonucu ürettiği anlamına gelmemektedir. Kurumsal izleme meşruiyet ve ölçülülük, yurttaş kaydı ise teknik doğrulanabilirlik ve kanıt değeri sorularıyla karşılaşmaktadır. Güvencelerin yetersiz kaldığı durumlarda ilk pratik mahremiyet ve veri güvenliği, ikinci pratik ise eksik olay bilgisi, ifşa ve yanlış yorum bakımından hassasiyet doğurabilmektedir (Nissenbaum, 2004; Richards, 2013; Thomsen, 2019).

Bu çalışmada önerilen "orantılı ve hesap verebilir kamusal açıklık" yaklaşımı, açıklığın miktarından ziyade düzenlenme ilkelerine odaklanmaktadır. Orantılılık, izleme veya kayıt paylaşma pratiğinin amacı aşmamasını; şeffaflık, amacın ve sorumlulukların anlaşılabilir olmasını; bağlamsal bütünlük, kayıtların üretildikleri şartlar ve olayın öncesi-sonrasıyla birlikte değerlendirilmesini; doğrulanabilirlik, kaynağın ve işlem geçmişinin sınanabilmesini; hesap verebilirlik ise itiraz, açıklama, değerlendirme ve kurumsal yanıt mekanizmalarının bulunmasını ifade etmektedir. Şeffaflığın tek başına yeterli olmadığı, açığa çıkan bilginin sorgulanabilir ve sonuç üretebilir bir sürece bağlanması gerektiği ilgili yazında da vurgulanmaktadır (Ananny & Crawford, 2018; Bovens, 2007).

Modelin açıklama mantığı üç aşamada ilerlemektedir. İlk aşamada kurumların veri işleme, bireylerin ise kayıt üretme kapasitesi belirlenmektedir. İkinci aşamada kurumsal izleme için

meşruiyet, yurttaş kaydı için kanıt değeri sorusu ortaya çıkmaktadır. Üçüncü aşamada her iki hat orantılılık, şeffaflık, bağlamsal bütünlük, teknik doğrulanabilirlik ve hesap verebilirlik ölçütleriyle değerlendirilerek ulaşılan sonuç toplumsal güvenin kurumsal, epistemik ve prosedürel katmanlarına bağlanmaktadır.

Şekil 1'de güvenlik, hizmet verimliliği ve risk yönetimi gerekçeleriyle başlayan kurumsal izleme hattı, amaç, kapasite ve normatif güvenilirlik ölçütleri üzerinden değerlendirilmektedir. Tersine gözetim hattı ise ek bilgi ve belgeleme ihtiyacıyla başlayarak yurttaş kaydını teknik doğrulama, bağlamsal bütünlük ve gerekçeli yanıt aşamaları üzerinden kanıt değerine yaklaştırmaktadır. İki hat, orantılı ve hesap verebilir kamusal açıklık koşullarında birleşmektedir. Ampirik nedensellik testi düzeyinde okunmaması gereken bu model sonraki araştırmalarda sınanabilecek kavramsal bir açıklama çerçevesi olarak değerlendirilmelidir. Model, her durumda gözetimin güvensizlik veya her durumda tersine gözetimin hesap verebilirlik üreteceği iddiasını taşımamaktadır. Amaç, dijital kamusal açıklık düzenindeki iki hattın hangi güven, kanıt ve meşruiyet koşullarında toplumsal güvene katkı sağlayabileceğini açıklamaktır.

Şekil 1. *Dijital gözetim ve tersine gözetim ilişkisinde toplumsal güven ve kamusal açıklık çerçevesi*

Aşağıdaki önermeler ampirik olarak test edilmiş hipotezler değil, bu çalışmada geliştirilen kavramsal çerçevenin gelecekteki araştırmalar tarafından sınanabilmesi için formüle edilmiş teorik yönelimlerdir.

- Önerme 1: Kurumsal gözetimin meşruiyeti, güvenlik tehdidinin algılanan ciddiyetiyle birlikte gözetimin gereklilik, orantılılık, şeffaflık ve denetlenebilirlik koşullarına bağlıdır.[1]
- Önerme 2: Kamusal olaylara ilişkin ek bilgi ve belgeleme ihtiyacı arttıkça, kullanıcıların tersine gözetim pratiklerine başvurma ve yurttaş kayıtlarına kanıt değeri atfetme eğilimi güçlenebilir.[2]

[1] Önerme 1; algılanan gereklilik, orantılılık, şeffaflık ve denetlenebilirlik ölçekleri ile kurumsal meşruiyet veya güven puanları arasındaki ilişkiler üzerinden anket ya da deney tasarımlarında sınanabilir.

[2] Önerme 2; ek bilgi ve belgeleme ihtiyacı, kayıt alma niyeti veya sıklığı ve yurttaş kaydına atfedilen kanıt değeri değişkenleri üzerinden anket, senaryo deneyi ya da dijital iz analiziyle sınanabilir.

- Önerme 3: Bir yurttaş kaydının hesap verebilirlik sürecine katkı sunması kaydın teknik özgünlük ve bütünlük bakımından doğrulanmasına, olay bilgisinin tamamlanmasına, kamusal erişime açılmasına ve ilgili aktörlerden gerekçeli bir yanıt üretilmesine bağlıdır.[3]
- Önerme 4: Platform aracılığı yurttaş kaydının erişimini artırdığı ölçüde kamusal katkıyı genişletir, algoritmik dağıtımın olay bilgisini daraltması, yanlış yorumları çoğaltması veya moderasyon yoluyla erişimi sınırlaması ise bu katkıyı azaltır.[4]
- Önerme 5: Hukuki, etik ve teknik güvencelerin zayıf kaldığı durumlarda gözetim ve tersine gözetim pratiklerinin eşzamanlı genişlemesi, toplumsal güveni desteklemek yerine kayıt ve izleme süreçlerine ilişkin belirsizlikleri artırabilir.[5]

Çerçeve; kamu kurumları için amaçla sınırlılık, veri güvenliği ve itiraz yollarını; platformlar için içerik kökeni, bütünlük ve olay bilgisi işaretlerini; medya okuryazarlığı açısından ise kayıtların paylaşılmadan önce doğrulanmasını öne çıkaran uygulamalı bir değerlendirme zemini sunmaktadır.

SONUÇ

Bu çalışma, dijital gözetim ve tersine gözetim arasındaki ilişkiyi toplumsal güven, mahremiyet, yurttaş kanıtı ve hesap verebilirlik ekseninde kavramsal olarak tartışmıştır. Çalışmanın temel iddiası, kurumsal izleme pratiklerinin güvenlik, hizmet verimliliği ve risk yönetimi gerekçeleriyle güvenilirlik beklentisi ürettiği, tersine gözetimin ise kamusal olayların belgelenmesi ve ek bilgi sağlanması yoluyla kullanıcı kayıtlarına kanıt değeri kazandırabileceğidir. Böyle bakıldığında birbirinin basit karşıtı sayılmaması gereken gözetim ve tersine gözetim dijital kamusal açıklık düzeninde toplumsal güvenin farklı biçimlerde sınandığı iki pratik olarak değerlendirilmelidir. Bu yaklaşım, gözetim tartışmasını yalnızca mahremiyet kaybı, tersine gözetim tartışmasını ise yalnızca demokratik imkan üzerinden okumayı yetersiz bırakmaktadır. Her iki pratik de uygun güvence mekanizmalarıyla desteklenmediğinde toplumsal güvene katkı sunmakta sınırlı kalabilir ve mahremiyet, veri güvenliği ya da yanlış yorum gibi yeni hassasiyetler doğurabilir. Böylece bu çalışmanın önerdiği çerçeve, açıklığın miktarından çok açıklığın hangi ilkelere göre düzenlendiğini merkeze almaktadır.

Çalışmanın teorik katkısı; kurumsal, epistemik ve prosedürel güveni aynı modelde birleştirmesi, kayıt ile kanıt arasına teknik ve kurumsal bir doğrulama zinciri yerleştirmesi ve söz konusu zinciri Türkiye'deki ölçülülük ilkesiyle ilişkilendirmesidir. "Orantılı ve hesap verebilir kamusal açıklık" çerçevesi, mevcut mahremiyet, açıklık ve tersine gözetim yaklaşımlarının açıklama gücünü korurken, üretken yapay zeka çağında köken ve bütünlük doğrulamasını modelin kurucu koşullarından biri olarak eklemektedir.

Çalışmanın temel sınırlılığı, önerilen ilişkilerin belirli bir kullanıcı grubu, kurum, platform veya ülke örneğinde henüz sınanmamış olmasıdır. Gelecek çalışmalar Türkiye'de kurumsal veri işleme ve izleme uygulamalarının hangi güvenceler altında kabul edilebilir bulunduğunu, kullanıcı kayıtlarına hangi şartlarda güven atfedildiğini ve teknik doğrulama işaretlerinin epistemik güven üzerindeki etkisini anket, deney, görüşme, içerik analizi veya dijital iz

[3] Önerme 3; teknik özgünlük-bütünlük doğrulaması, tamamlayıcı olay bilgisi, kamusal erişim ve gerekçeli kurumsal yanıt göstergelerinin açıklama, inceleme, düzeltme veya karar çıktılarıyla ilişkisi üzerinden operasyonelleştirilebilir.

[4] Önerme 4; erişim ve görüntülenme, yorum-paylaşım örüntüleri, moderasyon müdahaleleri, olay bilgisi kaybı, yanlış yorum ve algoritmik dağıtım göstergeleri birlikte incelenerek sınanabilir.

[5] Önerme 5; açık politika, itiraz yolu, veri güvenliği, köken bilgisi ve doğrulama mekanizması göstergeleri ile kayıt-izleme süreçlerine yönelik belirsizlik veya güven düzeyi arasındaki ilişki üzerinden test edilebilir.

analiziyle inceleyebilir. Modelin farklı sosyo-teknik ortamlarda sınanması, önermelerin kapsam koşullarını ve açıklama sınırlarını daha belirgin biçimde ortaya çıkaracaktır.

KAYNAKÇA

Akyüz, S. S., & Öztat, F. (2025). Yurttaş gazeteciliği ve sosyal medya kavramları üzerine bibliyometrik bir analiz. *Kritik İletişim Çalışmaları Dergisi*, *7*(1), 182-211. https://doi.org/10.53281/kritik.1682623

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). https://doi.org/10.5210/fm.v13i3.2142

Allan, S. (2013). *Citizen witnessing: Revisioning journalism in times of crisis*. Polity Press.

Amnesty International. (2019, December 11). *Amnesty International updates Citizen Evidence Lab for cutting-edge open-source human rights investigations*. https://www.amnesty.org/en/latest/press-release/2019/12/amnesty-international-updates-citizen-evidence-lab-for-cutting-edge-open-source-human-rights-investigations/

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973-989. https://doi.org/10.1177/1461444816676645

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497.

Baier, A. (1986). Trust and antitrust. *Ethics*, *96*(2), 231-260. https://doi.org/10.1086/292745

Bakir, V. (2010). *Sousveillance, media and strategic political communication: Iraq, USA, UK*. Continuum.

Binark, M., & Bayraktutan, G. (2013). *Ayın karanlık yüzü: Yeni medya ve etik*. Kalkedon Yayınları.

Bock, M. A. (2016). Film the police! Cop-watching and its embodied narratives. *Journal of Communication*, *66*(1), 13-34. https://doi.org/10.1111/jcom.12204

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, *13*(4), 447-468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brighenti, A. M. (2007). Visibility: A category for the social sciences. *Current Sociology*, *55*(3), 323-342. https://doi.org/10.1177/0011392107076079

Brucato, B. (2015). The new transparency: Police violence in the context of ubiquitous surveillance. *Media and Communication*, *3*(3), 39-55. https://doi.org/10.17645/mac.v3i3.292

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*(6), 1753-1820.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512. https://doi.org/10.1145/42411.42413

Coalition for Content Provenance and Authenticity. (2025). *C2PA technical specification (Version 2.2).* https://spec.c2pa.org/specifications/specifications/2.2/specs/C2PA_Specification.html

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.).* SAGE.

Dolgun, U. (2008). *Şeffaf hapishane yahut gözetim toplumu: Küreselleşen dünyada gözetim, toplumsal denetim ve iktidar ilişkileri*. Ötüken Neşriyat.

Dubberley, S., Koenig, A., & Murray, D. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press. https://doi.org/10.1093/law/9780198836063.001.0001

Erdinç, G. H. (2020). Ölçülülük ilkesi ve açık rıza kapsamında biyometrik verilerin işlenmesi. *Kişisel Verileri Koruma Dergisi*, *2*(1), 1-19.

Fallis, D. (2021). The epistemic threat of deepfakes. *Philosophy & Technology, 34*(4), 623-643. https://doi.org/10.1007/s13347-020-00419-2

Farrell, N., & Allan, S. (2015). Redrawing boundaries: WITNESS and the politics of citizen videos. *Global Media and Communication, 11*(3), 237-253. https://doi.org/10.1177/1742766515606291

Foucault, M. (1995*). Discipline and punish: The birth of the prison (A. Sheridan, Trans.).* Vintage Books. (Original work published 1975)

Giddens, A. (1990). *The consequences of modernity*. Stanford University Press.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.

Gilson, L. L., & Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? *Group & Organization Management, 40*(2), 127-130. https://doi.org/10.1177/1059601115576425

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605-622. https://doi.org/10.1080/00071310020015280

Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.

Hardwig, J. (1991). The role of trust in knowledge. *The Journal of Philosophy, 88*(12), 693-708. https://doi.org/10.2307/2027007

İsmayılov, E. K., & Sunal, G. (2012). Gözetlenen ve gözetleyen bir toplumda, beden ve mahremiyet ilişkisi: Facebook örneği. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi, 18*, 21-41.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*, 18-26. https://doi.org/10.1007/s13162-020-00161-0

Karasar, N. (2016). *Bilimsel araştırma yöntemi: Kavramlar, ilkeler, teknikler*. Nobel Akademik Yayıncılık.

Kişisel Verilerin Korunması Kanunu. (2016). 6698 sayılı Kişisel Verilerin Korunması Kanunu. *Resmî Gazete, 29677*, 7 Nisan 2016.

Küzeci, E. (2020). *Kişisel verilerin korunması* (4. baskı). On İki Levha Yayıncılık.

Luhmann, N. (1979). *Trust and power.* Wiley.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society, 11*(1/2), 18-34. https://doi.org/10.24908/ss.v11i1/2.4456

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331-355. https://doi.org/10.24908/ss.v1i3.3344

Marx, G. T. (2002). What is new about the new surveillance? Classifying for change and continuity. *Surveillance & Society, 1*(1), 9-29. https://doi.org/10.24908/ss.v1i1.3391

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734. https://doi.org/10.2307/258792

Mohler, M., vd. (2022). Policing in an era of sousveillance: A randomised controlled trial examining the influence of video footage on perceptions of legitimacy. *Policing and Society, 32*(1), 52-70. https://doi.org/10.1080/10439463.2021.1878169

Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics, 16*(4), 515-534. https://doi.org/10.1080/10350330601019769

Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches (7th ed.).* Pearson.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119-157.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Origgi, G. (2012). Epistemic injustice and epistemic trust. *Social Epistemology, 26*(2), 221-235. https://doi.org/10.1080/02691728.2011.652213

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice (4th ed.)*. SAGE.

Reilly, P. (2015). Every little helps? YouTube, sousveillance and the "anti-Tesco" riot in Stokes Croft. *New Media & Society, 17*(5), 755–771. https://doi.org/10.1177/1461444813512195

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934-1965.

Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosophers' Imprint, 20*(24), 1-16.

Rousseau, D. M., vd. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393-404. https://doi.org/10.5465/amr.1998.926617

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Sperber, D., vd. (2010). Epistemic vigilance. *Mind & Language, 25*(4), 359-393. https://doi.org/10.1111/j.1468-0017.2010.01394.x

Sutton, R. I., & Staw, B. M. (1995). What theory is not. *Administrative Science Quarterly, 40*(3), 371-384. https://doi.org/10.2307/2393788

Thompson, J. B. (2005). The new visibility. *Theory, Culture & Society, 22*(6), 31-51. https://doi.org/10.1177/0263276405059413

Thomsen, F. K. (2019). The concepts of surveillance and sousveillance: A critical analysis. *Social Science Information, 58*(4), 701-713. https://doi.org/10.1177/0539018419884410

Trottier, D. (2012). *Social media as surveillance: Rethinking visibility in a converging world*. Ashgate.

TÜİK. (2025). *Hanehalkı bilişim teknolojileri kullanım araştırması, 2025*. Türkiye İstatistik Kurumu.

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1). https://doi.org/10.1177/2056305120903408

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world.* Oxford University Press.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review, 14*(4), 490-495. https://doi.org/10.5465/amr.1989.4308371

Wilson, D., & Serisier, T. (2010). Video activism and the ambiguities of counter-surveillance. *Surveillance & Society, 8*(2), 166-180. https://doi.org/10.24908/ss.v8i2.3484

Yıldırım, A., & Şimşek, H. (2021). *Sosyal bilimlerde nitel araştırma yöntemleri* (12. baskı). Seçkin Yayıncılık.

Ziller, C., & Helbling, M. (2021). Public support for state surveillance. *European Journal of Political Research, 60*(4), 994-1006. https://doi.org/10.1111/1475-6765.12424

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

Hakem Değerlendirmesi
Dış bağımsız
Yazar Katkısı
Çalışmanın Tasarımı, EÇ (%100); Veri Toplama, EÇ (%100); Araştırma ve Analiz, EÇ. (%100); Orijinal Taslak, EÇ (%100); İnceleme ve Düzenleme, EÇ (%100).
Veri Seti Erişimi
Mevcut çalışma sırasında kullanılan ve/veya analiz edilen veri setleri, makul bir talep üzerine sorumlu yazardan temin edilebilir.
Finansal Destek
Sorumlu yazar, bu çalışmanın herhangi bir finansal destek almadığını beyan etmiştir.
Çıkar Çatışması
Sorumlu yazar herhangi bir çıkar çatışması olmadığını beyan etmiştir.
Etik Beyan
Bu makale, insan katılımcılarla yapılan herhangi bir süreç içermemektedir. Bu yüzden etik kurul izni alınmasına gerek yoktur.
Bilgilendirilmiş Onam
Bu makale, insan katılımcılarla yapılan herhangi bir süreç içermemektedir. Bu yüzden etik kurul izni alınmasına gerek yoktur.
Bilgilendirme
Bu makalede araştırma ve yayın etiğine uyulmuştur.
Yazışmalar ve materyal talepleri ile ilgili konular için sorumlu yazarla iletişim kurulmalıdır.
Bu makalede üretken yapay zeka destekli teknolojiler kaynak taraması ve kaynakların raporlanması ile özetlenmesi, dil kontrolü, tekrar eden içeriklerin belirlenmesi ve anlatımın güçlendirilmesi amacıyla yardımcı araç olarak kullanılmıştır.
Makalede kullanılan üretken yapay zeka aracı: OpenAI ChatGPT 5.5.
Tüm yazarlar, makalenin yayınlanmış versiyonunu okumuş ve kabul etmiştir.

Peer-review
Externally peer-reviewed.
Author Contributions
Conceptualization, EÇ (100%); Data Curation, EÇ (100%); Research & Analysis, EÇ (100%); Original Draf, EÇ(100%); Review & Editing, EÇ (100%).
Data Availability Statement
The data sets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.
Funding
The author declared that this study has received no financial support.
Conflict of Interest
The corresponding author has no conflict of interest to declare.
Ethical Approval
This article does not contain any studies with human participants performed by any of the authors.
Informed consent
This article does not contain any studies with human participants performed by any of the authors.
Acknowledgement
Research and publication ethics were followed in this article.
Correspondence and requests for materials should be addressed to Corresponding Author.
This article used generative AI-powered technologies solely for literature review and reporting/summarization, language check, identification of repetitive content, and strengthening of narrative. The generative AI tool used in the article: OpenAI ChatGPT 5.5
All authors have read and accepted the published version of the manuscript.