

Dijital Totalitarizm: Yeni Nesil Denetim Rejimi Üzerine Çin Örneği Üzerinden Bir İnceleme

Digital Totalitarianism: An Analysis of the New Generation of Control Regime through the Case of China

ÖZET

Yirminci yüzyılda ortaya çıkan totalitarizm kavramı, yirmi birinci yüzyılın başından itibaren internet, büyük veri, yapay zekâ, yüz tanıma sistemleri ve sosyal medya platformları gibi dijital teknolojilerin gelişimiyle birlikte yeni araçlar kazanmıştır. Bu nedenle, söz konusu teknolojik ilerlemenin yalnızca ekonomik ve toplumsal dönüşümlere değil, aynı zamanda siyasal iktidarların dönüşümüne de yol açtığı tartışılmaktadır. Totaliter özellikler sergileyen siyasal iktidarlar, bireylerin ve toplumların yalnızca fiziksel değil, aynı zamanda dijital davranışlarını da gözetim, denetim ve kontrol altında tutmakta; gerekli görülen durumlarda ise sansür mekanizmalarını devreye sokmaktadır. Bu çerçevede, dijital totalitarizm kavramı ortaya çıkmıştır. Dijital totalitarizm, internetin özgürlükleri artırdığı ve toplumları daha açık hale getirdiği yönündeki varsayımların sorgulanmasına neden olmuştur. Çin, dijital totalitarizmin en belirgin örneklerinden biri olarak değerlendirilmektedir. Hu Jintao döneminde inşa edilen ve Çin'i özellikle Batı etkilerinden izole etmeyi amaçlayan Büyük Güvenlik Duvarı ile Çin'in merkezileşen ve otoriter yapısının arttığı belirtilen Xi Jinping döneminde oluşturulan Sosyal Kredi Sistemi bu çerçevede ön plana çıkmaktadır. İfade özgürlüğünü sınırlayan bu uygulamalar, kimi yaklaşımlara göre Çin hükümetinin çıkarlarını koruma ya da toplumsal düzenin sağlanması açısından meşru bir araç olarak değerlendirilmektedir.

Anahtar Kelimeler: Büyük Güvenlik Duvarı, Çin, Dijital Totalitarizm, Sansür, Sosyal Kredi Sistemi

ABSTRACT

Totalitarianism, which emerged as a concept in the twentieth century, has acquired new instruments through the development of digital technologies such as the internet, big data, artificial intelligence, facial recognition systems, and social media platforms since the beginning of the twenty-first century. Therefore, it is argued that such technological advances have led not only to economic and social transformations but also to transformations in political power. Political regimes exhibiting totalitarian features monitor, regulate, and control not only the physical but also the digital behaviors of individuals and societies; whenever deemed necessary, they also activate censorship mechanisms. Within this framework, the concept of digital totalitarianism has emerged. Digital totalitarianism has led to questioning the assumptions that the internet enhances freedoms and makes societies more open. China is regarded as one of the most salient examples of digital totalitarianism. The Great Firewall, constructed during the Hu Jintao era with the aim of isolating China from Western influence, and the Social Credit System, established during the Xi Jinping era when China's centralist and authoritarian structure is said to have intensified, stand out in this regard. These practices, which limit freedom of expression, are considered by some as legitimate tools either for protecting the interests of the Chinese government or for maintaining social order.

Keywords: Great Firewall, China, Digital Totalitarianism, Censorship, Social Credit System.

GİRİŞ

Yirminci yüzyılda yaşanan siyasal ve ideolojik kırılmalar, modern siyaset düşüncesinde totalitarizm kavramının ortaya çıkmasına neden olmuştur. Bu kavram, yalnızca otoriterliğin özelliklerini değil, aynı zamanda bireyin toplumsal, ekonomik ve özel yaşamını da içine alan kapsamlı bir denetim biçimini ifade etmektedir. Totaliter rejimler, yalnızca siyasal iktidarı ele geçirmekle kalmamakta; aynı zamanda eğitim, medya, hukuk, ekonomi ve kültür gibi alanlar üzerinde de mutlak hâkimiyet kurmaya çalışmaktadır.

Totalitarizmin teorik temelleri, 1930'lardan itibaren özellikle Nazi Almanyası ve Stalin dönemi Sovyetler Birliği'nin incelenmesiyle şekillenmiştir. Hannah Arendt, Carl Friedrich, Zbigniew Brzezinski gibi siyaset teorisyenleri, bu rejimlerin yapısal ortaklıklarını ve ideolojik dinamiklerini analiz ederek totalitarizmi klasik diktatörlüklerden ayıran nitelikleri ortaya koymuşlardır. Bu bağlamda tek parti yönetimi, resmi ideoloji, kitlesel propaganda, yaygın gözetim mekanizmaları ve muhalefetin sistematik olarak bastırılması totaliter sistemlerin ayırt edici özellikleri arasında sayılmaktadır.

Meryem Nergis Ataçay¹

How to Cite This Article

Ataçay, M. N. (2025). "Dijital Totalitarizm: Yeni Nesil Denetim Rejimi Üzerine Çin Örneği Üzerinden Bir İnceleme" International Social Sciences Studies Journal, (e-ISSN:2587-1587) Vol:11, Issue:9; pp:1646-1658. DOI: <https://doi.org/10.5281/zenodo.17215478>

Arrival: 24 August 2025

Published: 27 September 2025

Social Sciences Studies Journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

¹ Dr. Öğr. Üyesi, Kastamonu Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi, Kastamonu, Türkiye. ORCID: 0000-0002-9723-0536

Yirmi birinci yüzyıla gelindiğinde, totalitarizm dijital teknolojiler aracılığıyla yeniden üretilebilecek bir tehdit olarak da ortaya çıkmaktadır. Özellikle internet, büyük veri, yapay zeka, yüz tanıma sistemleri ve sosyal medya platformları gibi dijital teknolojilerin hızlı gelişimi yalnızca ekonomik ve toplumsal alanları etkileyen bir faktör değildir. Aynı zamanda, siyasal iktidarlara da dönüştürmektedir. Bu dönüşümün sonucunda, klasik otoriterlik ve totalitarizm tanımlarından farklı olarak dijital totalitarizmin ortaya çıktığı tartışılmaktadır. Dijital totalitarizm, bireylerin yalnızca fiziksel değil, dijital davranışlarının da sürekli gözetim altında tutulduğu, veri temelli denetimin ideolojik manipülasyonla birleştiği bir yönetim modeli olarak tanımlanmaktadır.

Bu çerçevede, Çin'in Büyük Güvenlik Duvarı ve Sosyal Kredi Sistemi gibi uyguladığı dijital gözetim, denetim ve sansür mekanizmalarıyla dijital totalitarizmin önemli bir örneğini oluşturduğu tartışılmaktadır. Çin hükümeti, bu tür uygulamaları ve düzenlemeleri Batı'dan gelecek ideolojik etkileri engellemeye yönelik önlemler olarak göstererek meşrulaştırmaktadır. Ayrıca bu şekilde, diğer toplumlarda olduğu gibi internetin ve sosyal medyanın olumsuz toplumsal etkilerinin ortadan kaldırılması da amaçlanmaktadır. Literatür taraması yöntemiyle oluşturulan bu makalenin ikinci bölümünde, totalitarizmin genel teorik çerçevesi, dijital totalitarizm ve özellikle dijital gelişmeler ile demokrasi arasındaki ikilem üzerine olan tartışmalar sunulmaktadır. Bu makalede, temel olarak Çin'de Hu Jintao döneminden itibaren gelişmeye başlayan ve Xi Jinping döneminde artan dijital totalitarizm eğiliminin var olduğu değerlendirilmektedir.

KAVRAMSAL ÇERÇEVE: TOTALİTARİZMDEN DİJİTAL TOTALİTARİZME

Toplumu bütünüyle kontrol altına almak isteyen, muhalefeti ortadan kaldıran, bireysel özgürlükleri yok eden ve devletin ideolojisini mutlak hakikat olarak dayatan rejim biçimi olarak tanımlanan totalitarizmin felsefi ve kuramsal temellerine bakıldığında Hannah Arendt önemli bir yere sahiptir. Arendt, *The Origins of Totalitarianism* (1951) başlıklı kitabında, totaliter rejimleri yalnızca birer otoriter yönetim değil, insanın özgürlüğünü ve düşünme kapasitesini yok etmeyi hedefleyen bir ideoloji ve yönetim biçimi olarak tanımlamaktadır. Arendt'in totalitarizm anlayışı birey, kitleler, ideoloji, terör ve propaganda arasındaki ilişkiye dair çıkarımlarına dayanmaktadır. Totalitarizmin bireyselliği tamamen ortadan kaldırmayı ve toplumu birbirine özdeş üyelerden oluşan bir kitleye dönüştürmeyi hedeflediğini savunan Arendt'e göre, bu özellikle bireyi toplumsal ilişkilerden kopartıp eleştirel kapasitesini azaltarak ve gerçeğin yerine ideolojik kurgular ve yalanlar koyarak yapılmaktadır (Kohn, 2002: 634).

Carl J. Friedrich ve Zbigniew Brzezinski ise *Totalitarian Dictatorship and Autocracy* (1956) başlıklı kitaplarında totaliter rejimlerin temel öğelerini diktatör ve parti, totaliter resmi ideoloji, devlet kontrolünde medya ve eğitim, devlet tekelinde ekonomi ve totaliter bürokrasi, terör aygıtı ve silahlı kuvvetler üzerinde tam kontrol şeklinde açıklamışlardır. 1984 (1949) başlıklı romanıyla George Orwell de özellikle "Büyük Birader" figürüyle sürekli gözetim ve gerçekliğin çarpıtılması sorunlarına dikkat çekerek totalitarizmin birey üzerindeki etkisini kurgu üzerinden anlatmaktadır. Raymond Aron, *Democracy and Totalitarianism, A Theory of Political Regimes* (1965) başlıklı kitabında belirttiği üzere, totalitarizm bir partiye siyasi etkinlik konusunda tekel olma hakkı veren bir olgudur, belirli bir ideoloji çerçevesinde bunu zorlama ya da ikna yoluyla da yapması mümkündür (s.193). Aron (1965) aynı zamanda tek parti sisteminin ya da devlet planlamasının totalitarizme ne derece yol açacağı sorusunu tartışmaktadır ve rejimin totaliter yapısının tek parti sisteminden çok sergilenen radikal tutumlar ve kullanılan yöntemlerin aşırılığı tarafından belirlendiğini vurgulamaktadır (s.195). Michel Foucault doğrudan totalitarizme odaklanmasa da analizleri özellikle dijital çağdaki gözetim rejimlerini anlamada etkilidir. *Discipline and Punish* (1977) ve *The History of Sexuality* (1978) başlıklı kitaplarında yer verdiği "panoptikon", "biyopolitika" ve "mikro-iktidar" kavramlarıyla bireyin gözetim altına alınmasını analiz etmektedir. Bireyleri gönüllü olarak itaat eden öznelerle dönüştüren "panoptikon" dijital çağda gerçek anlamını bulmaktadır. Bireyler, sürekli izlendiğini bilerek kendi kendini denetleyen öznelerle dönüşmektedir (Lyon, 2007: 59-60).

Totaliter siyasi iktidarlara ilişkin özellikler, dijital teknolojinin gelişmesiyle birlikte yeniden ve daha hızlı bir şekilde üretilmektedir. Bu çerçevede ortaya çıkan dijital totalitarizm, klasik totalitarizmin fiziksel araçlarına dijital teknolojileri eklemektedir. Bunun sonucunda da bireylerin düşünsel ve davranışsal özgürlüklerini kısıtlamada görülmesi ve fark edilmesi daha zor; ancak daha etkili yöntemler ortaya çıkmaktadır. Bu durum, internetin özellikle demokrasinin gelişmesi konusundaki faydalarına ilişkin varsayımları tersine çevirmektedir. Evgeny Morozov *The Net Delusion: The Dark Side of Internet Freedom* (2011) başlıklı kitabında ortaya koyduğu "ağ (internet) yanılsaması" kavramıyla teknolojinin demokratikleşmeden çok merkezîyetçi kontrolü güçlendirme potansiyeline dikkat çekmektedir. Shoshana Zuboff tarafından geliştirilmiş ve *The Age of Surveillance Capitalism* (2019) başlıklı kitabında açıklanan "gözetim kapitalizmi" kavramı ise bu dönüşümü politik ekonomi çerçevesinde açıklamaktadır. Bu kavram, dijital çağda veri toplama, analiz etme ve yönlendirme süreçlerinin kapitalist kâr mantığıyla birleştiği yeni bir ekonomik sistemi ifade etmektedir. Yirmi birinci yüzyılın başlarında, dijitalleşme ve finansallaşma küresel "seçkinleri" görünmez kılarak kitleleri gözetim altına almıştır (Hendrikse, 2021: 73-74). Üstelik dijital teknolojiye ilişkin gelişmelerin etkileri, neoliberal kapitalizm modelinin sorunları ile olduğu kadar iklim krizinin

etkileri, küresel pandemi ve nükleer savaş tehdidi gibi diğer toplumsal, ekonomik ve kültürel gelişmelerle iç içe geçmiştir (Thomas, 2024: 116).

Dijital teknolojilerin gelişmesiyle birlikte siyasi iktidarların kullandığı çeşitli dijital denetim mekanizmaları ortaya çıkmıştır. Yapay zekâ destekli gözetim sistemleri ve yüz tanıma sistemleri, özellikle otoriter rejimlerde, bireylerin kimliklerini anlık olarak tespit etme, kalabalıklar içinde davranış analizleri yapma ve potansiyel muhalefeti bastırma amacıyla kullanılmaktadır. Sosyal medya algoritmaları, kullanıcıların bilgiye erişimini kontrol etmenin yanı sıra, kitle psikolojisini ve siyasi kararları yönlendirme amacına da hizmet etmektedir. Örneğin, 2018 yılında gerçekleşen Cambridge Analytica skandalı bireylerin çevrim içi verilerinin siyasi kampanyalar için nasıl manipüle edildiğini göstermiştir (Cadwalladr & Graham-Harrison, 2018). Bunların yanında, geleneksel sansürden çok da farklı olmayan ve en temel insan haklarından biri olan ifade özgürlüğüne zarar veren çevrim içi sansür ortaya çıkmıştır (Erixon ve Lee-Makiyama, 2011: 4). Bu süreçte, devlet ile özel sektör arasında karşılıklı bağımlılığın ortaya çıktığı, şeffaflığın azaldığı ve gücün merkezileştiği gözlemlenmektedir (Peron vd., 2025: 12).

Çin Halk Cumhuriyeti'nin 2014'te başlattığı Sosyal Kredi Sistemi, dijital totalitarizmin en çok tartışılan örneklerinden biridir. Bilgi teknolojileri üretimi konusunda oldukça gelişen Çin bu teknolojiyi vatandaşlarını kontrol etmek amacıyla kullanmak konusunda da öndedir. Çin'de mahremiyeti ortadan kaldıran ve bir tür "toplumsal puanlama" sistemi kuran Sosyal Kredi Sistemi yanında, vatandaşların "dış ağ" kullanımından izole edilmesini sağlayan "Altın Kalkan" sistemi de bulunmaktadır. Rusya'da ise ulusal olmayan internet ağını dışlamak amacıyla ulusal güvenliği sağlamak için yapıldığı iddiasıyla meşrulaştırılan "Egemen İnternet" sistemi oluşturulmuştur. Öte yandan bu konuya ilişkin dönüm noktasının 11 Eylül saldırılarından sonra ABD'de gerçekleştiğini vurgulamak önem kazanmaktadır. Bu süreçte, ABD'nin teröre karşı önlem almak adına kendi vatandaşlarının özgürlüğü ve mahremiyetini bu tür yöntemlerle kısıtlamayı ön plana çıkardığı gözlemlenmiştir (Tymchyshyn, 2020: 90). Dijital teknolojilerin gelişimi, faydalarının yanı sıra bireylerin özgür iradesiyle karar alma kapasitelerini zayıflatarak, totaliter eğilimleri besleyen bir manipülasyon ortamı yaratmaya çoktan başlamıştır. Bu durum, dijital teknolojilerin gelişimi ile demokrasi arasında bir karşıtlık olduğu şeklinde tartışmalara neden olmaktadır.

İletişim araçlarının tarihsel gelişimi önemli toplumsal ve siyasi değişimleri de beraberinde getirmiştir. Bu gelişme, kitlelerin sahip olduğu bilginin artmasını sağlarken aynı zamanda merkezi devletlerin güçlenmesinde de önemli rol oynamıştır. Bilgi akışını çok yönlü bir şekilde geliştiren ve sıradan insanları hem alıcı hem de üretici konumuna getiren dijital teknolojiler, ilk başta demokratikleşmenin önemli bir aracı olarak görülsede, baskıcı rejimler bu etkiyi engellemek için çeşitli yöntemler geliştirmek zorunda kalmıştır (Feldstein, 2021: 4). Hatta artık dijital teknoloji araçlarının çoğunlukla otoriter rejimler tarafından daha etkili kullanıldığı tartışılmaktadır. Başlarda internet kullanımındaki farklılıklar bireysel ve toplumsal nedenlerden kaynaklanırken zamanla internet yukarıdan aşağıya düzenlenmeye başlanmıştır ve hükümetlerin kontrolü altına girmiştir. Bu durumu, hükümetlerin küreselleşme ve internete karşılık önceden de pek çok durumda kullandıklarına benzer fiziksel baskı araçları olarak görmek mümkündür (Goldsmith ve Wu, 2006: 49, 180). Otoriter rejimler başlarda teknolojiyi kullanmakta geride kalmıştır; ancak bu tür siyasi iktidarlar da artık aktif bir şekilde kendi ulusal çıkarlarını ve iç meselelerine ilişkin politikalarını meşrulaştırmak için teknolojiyi kullanmaktadır (Deibert, 2016: 212).

Morozov (2011)'in geliştirdiği "ağ (internet) yanılması" kavramı, eleştirel bir şekilde dijital teknolojilerin ve özellikle de internetin demokrasi ve özgürlük getireceği yönündeki beklentilere karşı çıkmaktadır. Morozov (2011)'e göre, kendisi istikrarsız bir yapıya sahip olan internetin siyaset, ekonomi ve kültür ile geliştirdiği karşılıklı ilişki de istikrarsızdır. Batı, küreselleşme koşullarında otoriterliğin siyasi ve toplumsal özelliklerine odaklanmak yerine, internetin otoriter rejimleri güçlendirmek için kullanılamayacağını varsaymaktadır. Bu çerçevede, internetin gücün merkezileşmesini engelleyebileceği ve demokrasiyi güçlendireceği iddia edilmektedir (Morozov, 2011: 284, 289). Teknolojinin bu anlamda bir özgürleştirme getireceğine ilişkin varsayım temelde devletlerin özellikle de otoriter devletlerin kendi öncelikleri çerçevesinde iletişim teknolojileri kurumları oluşturdukları gerçeğini yadsımdan kaynaklanmaktadır. Bu kurumlar vatandaşların internet kullanımlarını izleme, düzenleme ve kontrol etme görevlerini üstlenmektedir (Feldstein, 2021: 5). Batı'nın bu yaklaşımının, yani Batılı olmayan toplumların aynı yöntemleri izleyerek demokrasiye ulaşabilecekleri savının sadece demokratikleşme süreci ile ilgili olmadığı, ekonomik gelişme konusuna ilişkin de geçerli olduğu ve özellikle post-kalkınma yaklaşımı çerçevesinde tartışıldığı bilinmektedir.

Twitter and Tear Gas, The Power and Fragility of Networked Protest (2017) başlıklı kitabında Zeynep Tüfekçi, dijital teknolojilerin gelişimiyle ortaya çıkan toplumsal ve siyasi alanı Habermas'ın kamusal alan kavramına referansla "ağ bağlantılı kamusal alan" olarak tanımlamıştır. Aynı zamanda, dijital çağda siyasal eylemi anlamak için tam olarak aynı şekilde olmasa da Arendt'in siyasal eylemi açıklamak için kullandığı metodolojinin de faydalı olacağı belirtilmektedir (Longo, 2024: 14-15). Öte yandan Tüfekçi (2017), otoritelerin de dijital dönüşüme paralel

olarak kamusal alanı ve toplumsal hareketleri kontrol altında tutmak için Orwell'in 1984 romanında tasvir ettiği korku dolu yöntemlerden farklı taktiklere başvurmak zorunda kaldığını vurgulamaktadır. Açıkça sansür uygulamak yerine kafa karışıklığına ve dikkat dağınıklığına neden olmak amacıyla bilgi bolluğu yaratmak ve karşı hareketler düzenlemek hükümetlerin bu anlamda kullandığı yöntemler arasında yer almaktadır (Tüfekçi, 2017: xxviii, 6-7).

Zuboff (2019)'un gözetim kapitalizmi olarak tanımladığı süreç bireylerin arama geçmişi, konum bilgisi, tıklamalar, beğeniler, mesajlar vb. dijital izlerinin büyük teknoloji şirketleri tarafından toplanıp analiz edilmesi ve bu veriler aracılığıyla kâr elde edilmesini sağlamaktadır. Bu süreçte, insan tecrübesi davranışsal veriye dönüşecek hammadde olarak görülmektedir ve insan davranışlarını tahmin etmek, şekillendirmek ve kontrol etmek için kullanılmaktadır. Öncüleri arasında Google, Facebook ve Amazon'un sayılabileceği gözetim kapitalizmi, hangi verilerin toplandığını çoğu zaman bilmeyen kullanıcılar açısından mahremiyet kaybı ortaya çıkmasına neden olmaktadır. Ayrıca bu süreç sadece ekonomik değil siyasi kararların da manipülasyonuna neden olarak demokratik süreçlerin işleyişine zarar verebilmektedir. Bütün bunların sonucunda, teknolojinin gelişmeye başladığından itibaren yalnızca araç değil aynı zamanda güç ve kontrol biçimi hâline geldiğini vurgulamak önem kazanmaktadır (Zuboff, 2019:13-15). Gözetim, Google ve Facebook gibi internet şirketlerinin kurumsal ve ekonomik güçlerinin temelini oluşturmaktadır. Gözetim azaltılırsa ve veri toplama sınırlandırılırsa bu türden şirketlerin batacağı açıktır. Bu nedenle, bu tür şirketler mahremiyet sorununa ilişkin siyasi bir çözümün ortaya çıkmasından korkmaktadır (Levine, 2018: 150).

İnternet kullanıcılarının gözetim altında olmaları ve mahremiyetlerinin zarar görmesi konusunda ne düşündükleri de önemlidir. Bu çerçevede tartışılan "gözetim gerçekliği" kavramına göre, verilerin toplanması ve gözetim normalleşmiştir (Hintz, Dencik ve Wahl-Jorgensen: 2019: 5, 18). Dijital teknolojilerin geliştirilme nedenleri düşünüldüğünde, gözetimin kaçınılmaz olduğu kabul edilmektedir; ancak bu çerçevede gelişen kontrol her zaman eşit olmamaktadır. Bu durumda, gözetim ve kontrolün söz konusu siyasi kültürün özelliklerine göre nasıl kullanıldığı önem kazanmaktadır (Lyon, 2007: 3-6, 14-16; Levine, 2018: 154). Bu süreçte, Batı demokrasilerinde de dijital gözetim ve denetim eğilimleri meşrulaşmakta ve bir tür liberal dijital gözetim sistemi ortaya çıkmaktadır. Bireysel özgürlüklerin savunulduğu iddia edilen demokratik ve liberal siyasi rejimlerde de dijital teknolojiler kullanılarak vatandaşların izlendiği, verilerinin topladığı, sınıflandığı ve işlendiği görülmektedir (Padden, 2023). Akıllı telefonların konum, mikrofon ve kamera verilerine erişim izni bu duruma en iyi örneği oluşturmaktadır. Covid-19 pandemi sürecinde uygulanan dijital izleme uygulamaları da bu eğilimleri güçlendirmiştir (Greitens, 2020: 169). Demokratik sistemlerde gözetimin şeffaflık, güvenlik, hizmet kalitesi ya da kullanıcı deneyimi gerekçeleriyle meşrulaştırıldığı görülmektedir (Aradau ve McCluskey, 2022: 2; Hintz, Dencik ve Wahl-Jorgensen, 2019: 95-98).

Ancak bu tür dijital süreçler, liberal demokrasilerde de ve daha çok teknoloji şirketleri lehine, benzer sonuçlar ortaya çıkarabilmektedir. Hizmete ulaşabilmek için kendi rızaları bulunan dijital teknoloji kullanıcıları uzun dönemde bireysel mahremiyet açısından zarar görmektedir (Nouwens vd., 2020: 193-194). Üstelik çoğu zaman bu verileri toplama ve işleme işiyle ilişkili olan ve birbirleriyle işbirliği yapan devlet kurumları ya da teknoloji şirketleri herhangi bir denetime tabi tutulmamaktadır. Böylesi asimetrik güç ilişkilerinin bulunduğu ortamda, doğal kaynaklar ve işgücü yerine insan hayatını veriye çevirerek işleyen "veri kolonyalizmi" ortaya çıkmaktadır (Thatcher et.al., 2016: 3; Couldry ve Mejias: 2019: xix, 67). Dijital teknolojinin gelişmesiyle birlikte güç kullanımının görülmesi ve anlaşılması daha zor hale gelmiştir. Bu durumun sonucunda, güç kullanımına ilişkin yasal düzenlemeler yapılması zorlaşmakta ve gücün kötü amaçlarla kullanılması kolaylaşmaktadır (Miller, 2018: 154-155). Bu nedenle, demokratik ülkelerde bile internet özgürlüğünün zarar görmesinin sorumluları olarak görülen büyük teknoloji şirketleri ve devletlere karşı düzenlemelerin yetersiz kaldığı ve gerekli kontrol mekanizmalarının ve yasal düzenlemelerin oluşturulmasının önemi vurgulanmaktadır (Deibert, 2016: 213; Feldstein, 2019: 50).

Bu çerçevede, Reset: Reclaiming the Internet for Civil Society (2020) başlıklı kitabında Ron Deibert, internetin sivil toplum yararına nasıl yeniden inşa edilebileceğini tartışmaktadır. İnternetin bilgiye açık erişim, demokratikleşme ve küresel bağlantı gibi vaatlerinin yerini gözetim, manipülasyon ve ayırıştırma almıştır. Özellikle sosyal medya olmak üzere dijital platformlar, yalan haberler, mahremiyet ihlalleri, kutuplaşma, devlet gözetimi ve sansürü ortaya çıkararak sivil toplumu zayıflatıcı etkilere yol açmaktadır. Sosyal medya platformlarında sağlıklı bir kamusal alan bulunmamaktadır. Bu bakış açısıyla Deibert (2020), internetin sivil toplum yararına yeniden inşa edilebilmesi için radikal yapısal reformlar ve eğitim ile desteklenen güçlü bir yurttaş bilinci çağrısı yaparak internetin bugünkü sorunlarını sadece teknik değil, siyasi ve etik bir mesele olarak ele almaktadır (Deibert, 2020: 12, 234-235). Gelecekte tam olarak nasıl bir biçim alacağını kestirmek mümkün olmasa da internet teknolojisinin uzun bir süre siyaseti ve kültürü etkileyeceği açıktır. Bu nedenle, interneti anlamaya ve demokratikleştirmeye çalışmak dijital teknolojinin gücünün demokratik ve insani değerleri arttırması için kullanılması anlamına

gelecektir. Bu yaklaşım, aynı zamanda bu teknolojinin faydalarının azınlık yerine çoğunluğa yayılmasını da sağlayacaktır (Levine, 2018: 154).

Dijital totalitarizmden kaçınmak da bu yöntemlerle mümkün olabilir; ancak görülüyor ki teknolojik araçlar aracılığıyla bireyin ve toplumların davranışlarını gözetim altında tutma, ceza mekanizmaları ve yönlendirme gibi yöntemlerle güçlenmektedir ve yayılmaktadır. Çin gibi ülkelerin kendi siyasi ve toplumsal düzenlerini dijital totalitarizme tabi kılarak küreselleşmenin etkileriyle başka ülkelere de yayması bu anlamda bir dengenin kurulmasını zorlaştırmaktadır. 2017 yılında Çin Devlet Konseyi tarafından yapay zekâ konusunda 2030 yılı itibarıyla yaklaşık 150 milyar ABD Doları yatırım yapılarak küresel liderliği elde etmek amacıyla kapsamlı bir plan hazırlanmıştır (Qiang, 2019: 63). Bu gelişme, yapay zekâ teknolojisinin ve beraberinde getirdiği dijital gözetimin, Çin'in jeopolitik stratejisinin önemli bir ögesi olarak, özellikle de Bir Kuşak Bir Yol girişimi sayesinde diğer baskıcı rejimlere ulaştırılmasına neden olmaktadır (Feldstein, 2019: 41-42, 49).

ÇİN VE DİJİTAL TOTALİTARİZM

Mao Zedong'un liderliğindeki Çin'in, Marksist-Leninist ideolojisi, ekonomik merkezileşmeye dayanması ve Kültür Devrimi (1966-1976)'nin getirdiği baskı ortamı nedeniyle totalitarizmin birçok temel ögesini barındırdığı tartışılmaktadır. Bu tartışma, başka bir çalışmada ele alınması gerekecek kadar geniş ve önemlidir; ancak 1978 yılından itibaren Deng Xiaoping liderliğinde başlatılan ekonomik reformlarla birlikte, merkezîyetçi ekonomik planlamadan piyasa temelli üretim modeline geçiş sağlandığı bilinmektedir. Buna karşın ideolojik anlamda daha esnek ve pragmatist bir yaklaşımla siyasal yapıda tek parti sistemi korunmuştur.

Dijital totalitarizm kavramının Çin ile ilişkilendirilmesi ise temel olarak 2013 yılından itibaren Çin Halk Cumhuriyeti Devlet Başkanlığı görevini üstlenen Xi Jinping döneminde gerçekleşmiştir. Aslında medyanın özellikle de sosyal medyanın denetimlerinin artması 2003-2013 yılları arasında devlet başkanlığını üstlenmiş olan Hu Jintao döneminde başlamıştır. Hu döneminde, reformların başladığı dönemden itibaren uygulanan ekonomik politikaların ortaya çıkardığı, başta hızla artan farklı türlerde eşitsizlikler olmak üzere toplumsal sorunlar fazlasıyla görünür hale gelmiştir. Hu, bu duruma karşı uyum ve istikrarı vurgulayan “harmonik toplum” anlayışını geliştirse de özellikle yoksul toplumsal kesim tarafından ortaya konulan tepkilere ve protestolara engel olunamamıştır (O'Brien ve Stern, 2008: 21; Lei, 2018: 32-33). Genel anlamda dijital gözetimi içeren “Altın Kalkan” çerçevesinde yer alan ve daha çok internet kullanımına odaklanan “Büyük Güvenlik Duvarı (Great Firewall)”, bu dönemde oluşturulmuştur ve kurumsallaşmıştır.

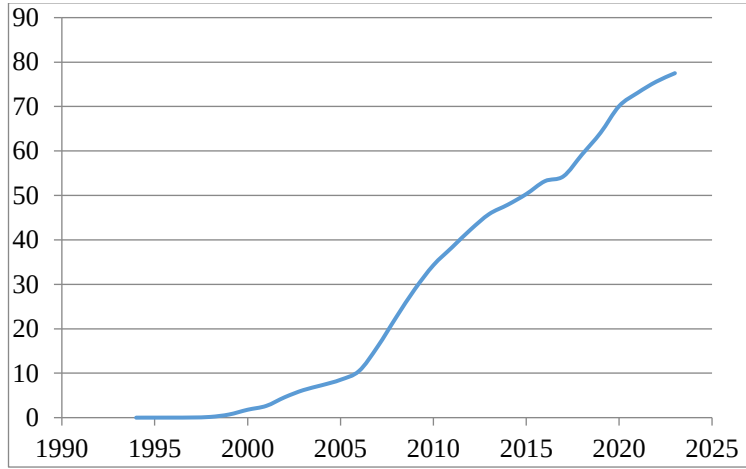
Büyük Güvenlik Duvarı

Büyük Güvenli Duvarı, Çin'in interneti kamu erişimine açmasıyla birlikte gelişen bir sansür sistemidir ve temel olarak Batı'dan gelen ve zararlı görülen içerikleri engellemek amacıyla oluşturulmuştur. Şekil 1'de görüldüğü üzere, 1994 yılında başlayan Çin'deki internet kullanımı 2000'lerin ortasından itibaren hızla yükselmiştir ve 2023 yılında internet kullanıcılarının nüfusa oranı yüzde 77,5'e kadar çıkmıştır. Çin'in nüfusunun büyüklüğü ve teknolojisinin gelişmişliği düşünüldüğünde, internetin Çin vatandaşlarının sadece günlük hayatının bir parçası değil aynı zamanda toplumsal hayatın, iletişimin ve ekonomik büyümenin önemli bir ögesi olması daha çok önem kazanmaktadır (Feng, Yu ve Xu, 2023: 53). Bu durum, “güçlü devletin” internet üzerinde uygulayacağı belirli bir kontrolü gerekli kılmıştır (Erixon ve Lee-Makiyama, 2011: 7). Bilginin serbestçe dolaşımı, Çin gibi otoriter bir devletin kontrol gücünü zayıflatabilir; ancak internet üzerinde çok sert baskı kurulmasının ekonomik küreselleşme koşullarında ülke ekonomisine zarar vereceği de açıktır. Bu nedenle, Çin sansür faaliyetlerine ihtiyaç duymaktadır (Anderson, 2012). Aslında Büyük Güvenlik Duvarı sisteminin teknik ve yasal altyapısı 1990'ların sonlarında Sanayi ve Bilgi Teknolojileri Bakanlığı kontrolünde kurulmaya başlanmıştır. Pek çok üniversite, kurum ve bilgi teknolojisi firması sistemin kurulmasına katkıda bulunmuştur. Çin'de internet servis sağlayıcılarının temel olarak devlet mülkiyetinde olması da gözetim ve sansür sistemlerinin engel ile karşılaşmasını önlemektedir (Anderson, 2012).

1996 yılında, Çin hükümeti, internet erişimi ile ilgili ilk düzenleyici yasaları “Devlet Konseyi Emri No. 195” çerçevesinde çıkararak internetin yurt dışına bağlanmasında sıkı devlet kontrolü öngörmüştür (Creemers, 1996). 1998 yılında Büyük Güvenlik Duvarı'nın temelini oluşturacak olan “Altın Kalkan” projesi resmen başlatılmıştır. “Altın Kalkan”, polis teşkilatı için kurulmuş bir ağ oluşturmuştur ve sansürü içermemiştir (Chepenko, 2020). Aslında, bu dönemde Çin devlet başkanı olan Hu Jintao, 2008 yılında People's Daily'ye verdiği bir röportajda interneti kamuoyu görüşlerini anlamak için önemli bir araç olarak gördüğünü ifade etmiştir ve bu dönemde farklı seviyelerde Çinli otoriteler kamuoyu ile çevrimiçi görüşmeler yapmıştır. Bu dönemde de siyasi sistem hakkında eleştirilere ya da siyasi reform taleplerine karşı gözetim ve sansür mekanizmaları işlerken Çin'in Twitter'ı olan Weibo'da resmi hesaplar açılmıştır. Ancak bu konuda önemli bir kırılma noktası 2011 yılında Wenzhou kentinde en az 40 kişinin ölümüne ve neredeyse 200 kişinin yaralanmasına neden olan bir hızlı tren kazası olmuştur. Çinli

internet kullanıcıları Weibo üzerinden yoğun bir şekilde kazanın yolsuzluk ve suiistimal yüzünden kaynaklandığını tartışmaya başlamışlardır ve Çin hükümeti bu tepkinin protestolara ve genel olarak siyasi sistemi sorgulamaya dönüşmesini engellemek amacıyla hem geleneksel hem de yeni medya araçlarını eleştirel paylaşımlar konusunda uyarmıştır (MacKinnon, 2012: 66-67).

Şekil 1. Çin’de Internet Kullanıcısı Sayısının Nüfusa Oranı (%)



Kaynak: World Bank (2025).

Dünyadaki en gelişmiş internet sansür sistemi olan Büyük Güvenlik Duvarı ile yabancı internet servislerinin sağladığı her türlü bilgi ve içerik kontrol edilmekte, filtrelenebilmekte ve engellenmektedir ve bu özelliğiyle teknik olmanın ötesinde siyasi bir araçtır. Bu çerçevede, BBC ve New York Times gibi Batı medyası, Facebook, Twitter, Instagram, Youtube, Google ve diğer eleştirel içerikler engellenmiştir. Google 2006 yılında Çin hükümetinin sansür tercihlerini kabul etmiştir. Buna göre, Çin sınırları içinde bir internet kullanıcısı siyasi açıdan hassas konularda, örneğin “Tiananmen Meydanı katliamı” ya da daha yakın zamanda yaşanmış bir protestoya ilişkin bir arama yaptığında sayfa engellenmektedir (MacKinnon, 2012: 59). Popüler tartışma forumu Reddit, Ağustos 2018’de engellenmiştir; tüm dillerdeki Wikipedia ise 2019 Nisan ayı sonunda engellenmiştir. 2022 yılı itibariyle, Google’ın Haritalar, Çeviri, Takvim, Dokümanlar, Drive, Akademik ve Analytics gibi birçok hizmeti engelli kalmaya devam etmiştir (Freedom House, 2022).

Gözetim ve sansür, yabancı propagandasından korunmak ve siber güvenliği sağlamak açısından meşrulaştırmaktadır (Freedom House, 2022). Çin hükümeti, bu engellemeyi internette gelebilecek ideolojik riskleri önlemek için bir yöntem olarak sunmaktadır (Chepenko, 2020). Çin’de internet büyüyen ekonomiyi destekleyecek kadar kullanırken siyasi sistemde gücün tekelleşmesine internet aracılığıyla zarar verebilecek her türlü tehdide karşı önlem alınmaktadır (Goldsmith and Wu, 2006: 89). Vatandaşların zararlı içeriklerden korunması ve güvenli bir dijital ortam yaratılmasına vurgu yapılırken ifade özgürlüğünün zarar görmesi üzerine tartışmalar da ortaya çıkmaktadır ve bu konuda denge kurulması konusunda internet sağlayıcı şirketlere önemli yasal sorumluluklar yüklenmektedir. Bu dengenin oluşması için bu tür konuları düzenleyen yasalarda açıklık ve şeffaflığın artırılmasını savunanlar bulunduğu gibi, iyi tanımlanmış yasal sınırlar içinde daha fazla ifade özgürlüğü talep edenler ya da katı düzenlemeleri zararlı içeriklerden korunmak ve düzenin sağlanması açısından olumlu görenler bulunmaktadır. Bu karmaşık sorunun farklı görüşlere sahip olanlar arasında geliştirilecek diyalog ve kamu katılımı ile çözümlenebileceği değerlendirilmektedir. Ayrıca bu tür düzenlemelerin düzenli olarak gözden geçirilmesi ve internetin getirdiği sorunlara karşı küresel iş birliği yapılması önerilmektedir (Feng, Yu ve Xu, 2023: 54, 56-58).

Genel olarak Çin toplumunun bu durumu kabullendiği belirtilse de içinde bulunulan küresel koşullarda akademik araştırma, gazetecilik ve yabancılarla kurulan ekonomik ilişkiler bu tür engellerden büyük zarar görmektedir (Feng, Yu ve Xu, 2023: 55). Hem sıradan internet kullanıcıları hem de gazeteciler yaygın bir şekilde çevrim içi yorumları nedeniyle hesap kapatmaları, yasal cezalar ve gerçek hayatta tepkilerle karşı karşıya gelmektedirler (Freedom House, 2022). Milliyetçi internet kullanıcıları, Çin’in itibarına zarar verdiğini düşündükleri kişilerle çevrim içi platformlarda karşı karşıya gelmektedir. Bu durum bazen hükümet baskısı ile ortaya çıksa da genellikle kendiliğinden ve gönüllü olarak gerçekleşmektedir. Komünist Parti gençlik örgütü çerçevesinde kurulmuş “elli-sent parti” adlı bir grup bulunmaktadır. Bu adın, bloglarda ve konuşma odalarında yayınladıkları her vatansever ve hükümet yanlısı gönderi için elli Çin senti ödeme aldıkları için konulduğu ifade edilmektedir. Ayrıca pek çok vatansever Çinli genç çevrimiçi topluluklar kurmaktadır. Pekin’deki prestijli bir üniversite olan Tsinghua

Üniversitesi'nden mezun olmuş olan Rao Jin tarafından yönetilen April Media bu tür topluluklara bir örnektir ve Batı medyası tarafından geliştirilen “Çin karşıtı önyargıya” karşı durmaktadır (MacKinnon, 2012: 67).

Çinli internet kullanıcıları, bazı durumlarda tepkilerini gösterecek de çoğunlukla cezalarla karşı karşıya gelmemek için muhalif içerikler yayınlamak, hükümet politikalarını eleştirmek, bazı hassas konularda açık tartışmalara girmekten ve belirli kelimeleri kullanmaktan kaçınarak oto sansür uygulamaktadırlar (Freedom House, 2022; Feng, Yu ve Xu, 2023: 55). Sonuç olarak Tüfekçi (2017)'nin ifade ettiği “ağ bağlantılı kamusal alan” yerine, Çin’de şeffaf olmayan, kamu-özel işbirliğinde yürütülen sansür ve gözetim ile işleyen “ağ bağlantılı otoriterlik” ortaya çıkmaktadır (MacKinnon, 2012: 54). Bu nedenle, Çinli internet kullanıcıları, Çin hükümetinin tepkisi ile karşılaşmalar da bu engelleri ortadan kaldırmak için çeşitli yöntemler geliştirmektedir.

Xi Jinping Dönemi

Genel olarak Çin’in Xi Jinping döneminde daha otoriter bir yönetim altına girdiği tartışılmaktadır. Dijital totalitarizm de bu durumun hem araçlarından hem de sonuçlarından biri olarak görülmektedir. Xi’nin 2012 yılında Çin Komünist Partisi (ÇKP) genel sekreterliği görevine başlamasından kısa süre sonra, internette yer alan karşıt söylemleri ve yorumları izlemek ve cezalandırmak için araçlar geliştirilmeye başlanmıştır. Özellikle, bu dönemde geliştirilen Sosyal Kredi Sistemi, dijital teknolojinin dijital gözetime dönüşmesine ilişkin önemli bir örnek oluşturmaktadır. Bu sistem ile vatandaşların toplumsal, ekonomik ve siyasi faaliyetleri algoritmik denetime tabi tutulmaktadır. Yüz tanıma sistemleri, yapay zekâ ile entegre çalışan kameralar ve çevrim içi sansür uygulamaları ile Çin vatandaşları dijital gözetim altında tutulmaktadır. Bireysel mahremiyeti ortadan kaldırmasının yanında, bu sistemi ilginç ve aslında korkutucu kılan özelliği gözetim sonucunda vatandaşların puanlanmasıdır. Sosyal Kredi Sistemi, gözetimle kalmayıp bir tür “toplumsal puanlama” ya da “ödül-ceza mekanizması” ortaya çıkarmıştır (Taşdan, 2023: 168). Bu sistemde vatandaşların finansal hareketleri, çevrim içi davranışları, sosyal ilişkileri ve kamuya açık faaliyetleri merkezi bir veri sistemi tarafından izlenmekte ve puanlanmaktadır. Orwell’in 1984’ünün yanında bir bilim kurgu dizisi olan Black Mirror’u anımsatacak şekilde, yasalara ya da toplumsal kurallara uymamaları ya da siyasi aktiviteleri nedeniyle otoriteler tarafından fark edilen bireylerin oluşturduğu kara listeler bulunmaktadır (Creemers, 2018). Sosyal Kredi Sistemine göre, düşük puan alan bireyler kredi alma, işe girme, vize alma gibi haklardan mahrum bırakılabilmektedir (Qiang, 2019: 56-58). Hatta iyi otellerde kalmaları, internet kullanımları ya da çocuklarını iyi okullara göndermeleri bile engellenebilmektedir (Chan, 2018).

Bu sistemin işleyişini sağlamak amacıyla çeşitli dijital teknoloji araçları bulunmaktadır. 2005 yılında başlatılan “Gökyüzü Ağı” video gözetim ağı üzerine 2015 yılında inşa edilen “Keskin Gözler” video gözetim programı da önemli bir örnek oluşturmaktadır. Çin’in gözetim kameralarını en hızlı kullanan ülke haline gelmesi, ses tanıma yazılımlarının ve DNA veri tabanının gelişmesi mahremiyete ciddi anlamda zarar vermekte ve özellikle etnik azınlıklar üzerindeki baskının artmasında rol oynamaktadır. Bu durumun Çin devletini “dijital totaliter devlete” dönüştürdüğü değerlendirilmektedir. Dijital teknoloji geliştikçe Çin devlet kurumlarının ve internet şirketlerinin vatandaşlar hakkında sistematik ve geniş çaplı verilere ulaşmaları da artmaktadır (Qiang, 2019: 56-58, 63). Sosyal Kredi Sistemi ve diğer tüm büyük veri toplama faaliyetleriyle gözetim altında olduklarının farkında olan ve sonuçlarını bilen bireylerin ve kurumların davranışlarının kontrol altında tutulması hedeflenmektedir (Creemers, 2018). Sosyal Kredi Sistemi’ni savunanlar bulunmaktadır ve sistemin pek çok toplumsal sorunun çözülmesinde önemli rol oynayacağını düşünmektedirler (Kostka, 2019: 23). Ayrıca sistemin Çin’deki uygulaması incelenirken Çin’in siyasi ve kültürel değerleri ile Batı değerleri arasındaki farklılıkların dikkate alınması önem kazanmaktadır ((Mac Síthigh ve Siems, 2019: 21-22).

Çin’de Xi döneminin başından itibaren dijital teknolojilerin gözetim ve sansür amaçlı kullanımını geliştirmek için ortaya çıkan gelişmeleri özetlemek gerekirse öncelikle 2012 yılının sonunda Ulusal Halk Kongresi Daimi Komitesi’nin düzenlemeleriyle cep telefonları aracılığıyla internete erişmek veya sosyal medya hesapları açmak isteyenlerin internet sağlayıcılarına gerçek isimlerini vermelerini zorunlu kılınmasını belirtmek gerekmektedir. Bu süreçte, Büyük Güvenlik Duvarı yeni teknolojilerle güçlendirilmiştir. 2013 yılında, beş yüz kez paylaşılan veya beş bin kişi tarafından görüntülenen yorumlara üç yıla kadar hapis cezası verilebilmesinin önü açılmıştır. Gönderilerin protesto düzenlemek veya etnik huzursuzluk çıkarmak amacı taşıması durumunda da hapis cezası uygulanabilmektedir. Bunlara ek olarak, devlet medyası, 2013 yılında Çin hükümetinin iki milyondan fazla kişiyi “mikroblog izleyicisi” olarak işe aldığını açıklamıştır (Qiang, 2019: 55).

Esas olarak Çin Siber Uzay İdaresi (Cyberspace Administration of China) ve ÇKP’ye bağlı ve Xi’nin başkanlığını yaptığı Merkez Siber Uzay İşleri Komisyonu, telekomünikasyon sektörünü denetlemektedir ve internet içeriğini düzenlemektedir. Bu komisyon, 2014 yılından itibaren Sanayi ve Bilgi Teknolojileri Bakanlığı’na bağlı idari bir kurum olan ve dijital sertifika verme yetkisine sahip olan Çin İnternet Ağı Bilgi Merkezini de denetlemektedir (Freedom House, 2022). Ayrıca 2014 yılının başlarında, yine ÇKP’ye bağlı olarak ve teknolojinin gelişimiyle siber

güvenliğin sağlanmasını “bir kuşun iki kanadı” olarak tanımlayan Xi’nin başkanlığında Siber Uzay İşleri Merkezi Liderlik Grubu kurulmuştur. Bu grup, ekonomik, siyasi, kültürel ve askeri boyutlarıyla her türlü siber konuya odaklanmayı hedeflemektedir (Tiezzi, 2014).

2015 yılında Çin Siber Uzay İdaresi, haber ve bilgi hizmeti veren internet kuruluşlarının sorumlularıyla büyük ihlaller sonrası görüşmeler yapacağını duyurmuştur. Bu görüşmelerde uyarılar yapılmakta ve talimatlar verilmektedir. Bu yöntemlerin yetersiz olduğu düşünüldüğünde ise ek uyarıların yapıldığı, para cezası verildiği, iş lisanslarının askıya alındığı ya da iptal edildiği görülmektedir (Qiang, 2019: 55-56; Feng, Yu ve Xu, 2023: 56). 2016 yılının sonuna doğru kabul edilen ilk siber güvenlik yasası ile internet şirketlerine suç teşkil eden paylaşımları kaldırmak ve yetkililere bildirmek konusunda daha büyük sorumluluk yüklenmiştir. 2017 ortalarından itibaren bu gözetimin hedefine çevrim içi haber portallarının yanında eğlence ve video platformları da eklenmiştir. Aynı yılın başlarında, Çin Sanayi ve Bilgi Teknolojileri Bakanlığı, özellikle, Büyük Güvenlik Duvarı’nın uyguladığı sansürü aşmak için kullanılan sanal özel ağı (VPN) etkisiz hale getirmek için aldığı önlemleri arttırdığını duyurmuştur. Hizmet sağlayıcıların, hükümet onayı olmadan VPN kurmaları yasaktır ve yasa dışı VPN faaliyetleri engellenmektedir (Qiang, 2019: 56).

2020 yılının sonuna doğru, Çin uygulama mağazalarından TripAdvisor da dahil olmak üzere 105 uygulamayı kaldırmıştır. Çin Siber Uzay İdaresi’ne göre, bu uygulamaların “pornografi, şiddet, terör ve diğer yasadışı bilgileri yaydığı ve hileli kumar ve fuhuş gibi yasadışı çevrimiçi hizmetler sunduğu tespit edilmiştir.” (Khaliq, 2020). 2021 ve 2022 yıllarında, Alibaba, Tencent ve Baidu gibi teknoloji devlerine tek el karşıtı kurallara uymadıkları için önemli cezalar uygulanmıştır (Disis, 2021; Reuters, 2022).

2022 yılının ortalarına gelindiğinde, Çin’de içerik çıkarmalar, internet sitesi kapatılması ve sosyal medya hesabının silinmesi vakaları artmıştır. Sansüre uğrayan konular ÇKP, ÇKP yetkilileri, dış meseleler, sağlık güvenliği, sivil toplum ve uzun zamandır tabu olan konular ile ilgili haberler, yorumlar ve eleştiriler olmaktadır. Tiananmen Meydanı Katliamı, Tayvan’ın bağımsızlığı ya da Uygur Türklerine uygulanan baskı gibi konular örnek oluşturmaktadır. Bu tür bir sansür, bireylerin kendi tarihlerini ve güncel konuları anlamalarını engellemektedir (Feng, Yu ve Xu, 2023: 55). Örneğin, Çin’deki arama motoru Baidu, “kötü niyetli bilgi” olma gerekçesiyle 2020 yılında 51.6 milyar ögeyi, 2021 yılında 56 milyar ögeyi sildiğini duyurmuştur (Freedom House, 2022). Yukarıda da belirtildiği üzere, yabancı şirketler de Çin hükümetinin sansür uygulamalarına uyum sağlamak durumunda kalmaktadır.

2024 yılında, 1 Ocak 2025’te yürürlüğe girecek olan Ağ Veri Güvenliği Yönetim Düzenlemeleri (Network Data Security Management Regulations) duyurulmuştur. Bu düzenlemeler, yerli ve yabancı tüm şirketlerin kişisel bilgi koruması ve sınır ötesi veri transferleri konusunda daha sıkı önlemler getirmelerini gerektirmektedir. China Briefing’in haberine göre, bu düzenlemeler ile bireylerin ve kurumların haklarının korunması, aynı zamanda da ulusal güvenlik ve kamu çıkarlarının sağlanması hedeflenmektedir ve düzenlemelere uymayanlara çeşitli miktarlarda para cezaları uygulanacağı belirtilmektedir (Interesse, 2024).

Bütün bu oluşturulan kurumlar ve yapılan düzenlemeler Çin’de gözetim ve sansür konusunda sistemli bir bürokratik yapı oluşturulduğunu göstermektedir. Bu yapının uyguladığı dijital kısıtlamalara örnek olarak Çin otoriteleri tarafından özellikle Covid-19 pandemi döneminde alınan önlemlere karşı internet kullanıcılarının, gazetecilerin ve aktivistlerin bilgi paylaşımının ve eleştirilerinin engellenmesi verilebilir. 2021 yılında yürürlüğe giren Kişisel Bilgilerin Korunması Kanunu ve Veri Güvenliği Kanunu, internet şirketlerinin kullanıcı verilerini toplama, saklama ve paylaşma biçimlerini daha katı bir şekilde düzenlemiştir. Bu süreçte, yetkililerin lisanslı internet kafeler üzerinde sıkı denetim uyguladıkları belirtilmektedir. 2021 yılı başı itibarıyla toplam internet kafe sayısının yaklaşık 125.000 olduğu tahmin edilmektedir ve internet kafelerin video oyuncularını için buluşma mekânları olmaya devam ettiği ifade edilmektedir (Freedom House, 2022).

2022 Kış Olimpiyatları’nın Çin’de gerçekleştirildiği dönemde, Çin otoriteleri bir yanda eleştirel içerikleri engellerken diğer yanda da hükümet yanlısı yorumcuları cesaretlendirmiştir (Dou, 2022). 2022 yılı Mart ayında teknoloji platformlarının ÇKP ideolojisine karşı olan ve istenmeyen içerikleri kaldırmaları konusunda yeni düzenlemeler getirilmiştir. İnternet faaliyetleri nedeniyle önde gelen gazeteciler, insan hakları avukatları, aktivistler, dini ve etnik azınlıklar gözaltına alınmaktadır ve hapis cezaları almaktadır (Freedom House, 2022). Ayrıca bölgesel kısıtlamaların getirildiği de görülmektedir. Örneğin, 2022 yılında Henan eyaletinde banka hesaplarının dondurulması nedeniyle gerçekleştirilen geniş çapta gösterilerle ilişkili olduğu imasıyla Kasım 2023 ile Mart 2025 arasında yapılan testlerde eyaletteki internet alanlarında Çin’deki tüm kısıtlamanın beş katından fazla engelleme uygulandığı tespit edilmiştir (Hawkins, 2022; Hawkins, 2025).

Ayrıca 2022 yılında yürürlüğe girmek üzere çevrim içi dini bilgi hizmetlerini standartlaştırmak ve vatandaşların din özgürlüğünü garanti altına almak amacıyla yapılan düzenlemelerle yurt dışındaki kuruluşların ve bireylerin Çin

toprakları içinde çevrim içi dini bilgi hizmetleri yürütmesi yasaklanmıştır. Bu düzenlemelere göre, çevrim içi vaazlar, sadece İnternet Dini Bilgi Hizmet İzni almış olan dini topluluklar, tapınaklar ve kiliseler ile dini okullar tarafından yürütülebilecektir. Katılımcıların gerçek isimle kayıt olmak zorunda olması da şartlardan biridir. Bunun dışında, misyonerlik, dini eğitim, internet üzerinden din adına bağış toplanması, dini törenlerin canlı yayını ve videolarının canlı paylaşımı ve devlet otoritesine karşı içerikler yasaktır (Global Times, 2021).

2024 yılının Mayıs ayında, Çin'deki Tencent, Douyin, Kuaishou, Sina Weibo, Bilibili, and Xiaohongshu gibi bazı büyük sosyal medya platformları zenginlik gösterisi yapmak ve maddecilik gibi olumsuz içeriklerle mücadele etme konusundaki kararlılıklarını vurgulamıştır. “Akılcı tüketim değerlerini teşvik etmek ve sağlıklı bir çevrimiçi ekosistem oluşturmak” amacıyla yürütülen daha geniş kapsamlı bir çabanın parçası olarak değerlendirilen açıklamalarda, bu kuralları ihlal eden hesapların silineceği veya yasaklanacağı belirtilmiştir (Global Times, 2024). Hintli bir haber sitesi olan Firstpost’a göre, bu açıklamalar Çin hükümetinin 2016 yılında başlattığı “internet kültürel ortamını arındırmak” yaklaşımından kaynaklanmıştır (Firstpost, 2024). 2025 yılının Temmuz ayında, başlatılan yeni dijital kimlik sistemi ile çevrimiçi faaliyetlerin takip edilmesinin daha kolay hale geldiği devlet gözetiminin daha da sıkılaştığı ifade edilmektedir (Thibault, 2025). Ayrıca, 2019 yılından itibaren, özellikle de 2021 yılında çıkarılan Reşit Olmayanları Koruma Kanunu ile çocukların yerli ve yabancı sosyal medya platformlarına ulaşma durumu ve çevrim içi bilgi mahremiyetinin korunması konuları düzenlenmektedir. 2023 yılının Ağustos ayında çocukların ve 18 yaş altındaki gençlerin ekran başında geçirdikleri ve internete ulaşma sürelerini kısıtlama planları açıklanmıştır (Zheng ve Shu, 2024). 2025 yılının Ağustos ayında Siçuan eyaletindeki Jiangyou kentinde yaşanan ve sosyal medyaya yansıyan akran zorbalığı görüntüleri bu düzenlemeleri anlamlı kılmaktadır. Öte yandan, bu olay yüzünden gerçekleşen protestoda Çin polislerinin sert müdahalesi de internete ve dünya basınına yansımıştır. BBC haberine göre, bu olay Weibo’da en çok konuşulan ikinci konu olmuştur; ancak bu konu başlığı ve ilgili etiketler kısa sürede sansürlenmiştir. Son yıllarda, Çin’de ebeveynlerin öncülük ettiği veya çocuk güvenliği endişeleriyle tetiklenen başka protestolar da gerçekleşmiştir. Örneğin, 2023 yılında Henan eyaletine bağlı Shangqiu kentinde, 14 yaşındaki bir öğrencinin ölümünün ardından binlerce kişi protesto düzenlemiştir. Okul, öğrencinin intihar ettiğini açıklasa da, ailesi oğullarının bedeninde fiziksel şiddet izleri bulunduğunu ve saldırıya uğradığını öne sürmüştür (Bicker, 2025). Bu olaylar, internetin amacı ne olursa olsun düzenlemeye tabi tutulmasının teknik olduğu kadar siyasi ve toplumsal bir mesele de olduğunu bir kere daha açıkça göstermektedir.

Çin yönetiminin toplum üzerinde kurduğu bu dijital gözetim ve sansür mekanizmalarının bir de politik ekonomik yönü bulunmaktadır. 2019 yılında, BT Çin hükümetinin ilk olarak internet hizmeti sunma lisansı vereceği uluslararası şirket olarak duyurulmuştur (CGTN, 2019). Öte yandan, devlete ait China Mobile, China Telecom ve China Unicom mobil pazara hakim durumda olmaya devam etmektedir. Çin ekonomisinde, genel olarak stratejik sektörlerde bu durumun geçerli olduğu bilinmektedir. Eylül 2020’de Devlet Konseyi, yabancı firmaların Pekin’de yabancı şirketlere VPN hizmetleri sağlayan ortak girişimlerde yüzde 50’ye kadar hisseye sahip olmasına izin veren bir planı onaylamıştır. Bu çerçevede, Çin’in internet hizmet sektörünün yabancı yatırımcılara açılmaya başlandığı belirtilmiştir (Global Times, 2020). Yabancı bir internet servisi sağlayıcı şirketin Çin’de faaliyet gösterebilmesi için, bir Çinli kuruluşla ortaklık kurması gerekmektedir ve işletme ruhsatı olarak faaliyet gösterme hakkını onaylatmak için Devlet Sanayi ve Ticaret İdaresi’ne (State Administration for Industry and Commerce) kayıt yaptırmaları gerekmektedir (Nguyen, 2024). Çin’de internet sağlayıcısı şirketler, kullanıcı bilgisi toplama, gözetim, filtre ve sansür yöntemleriyle yasal düzenlemelerin sağlanması açısından aracı konumunda bulunmaktadır. Ayrıca, tüm bunları sağlayabilmek amacıyla siber ataklara karşı gerekli teknolojiyi de kurmaları beklenmektedir (Feng, Yu ve Xu, 2023: 54).

Freedom House’un Freedom on the Net 2024 raporuna göre, Çin, 10 yıl aradan sonra internet özgürlüğü açısından dünyanın en kötü ortamı olarak birinci sıradan ikinci sıraya geçmiştir. Bu durum, Myanmar’da bu alandaki baskıların artması ve bu ülkenin internet özgürlüğü konusunda en düşük seviyeye gerilemesi sonucunda gerçekleşmiştir. Çin hükümeti, Çin’in yerel internetini dünyanın geri kalanından izole etme ve bazı resmi siteleri uluslararası etkilerden arındırma çabasını sürdürmektedir. Ayrıca Çin hükümeti VPN kullananlara ağır cezalar uygulayarak muhalefeti sistematik şekilde bastırmaya da devam etmektedir (Freedom House, 2024: 2).

SONUÇ

İnternet, toplumsal, siyasi ve ekonomik alanların önemli bir parçası haline gelmiştir ve en azından yakın gelecekte bu durumun değişmeyeceği açıktır. Totaliter siyasi sistemler ele alındığında internetin bu üç alan ile kurduğu karmaşık ilişki daha da karmaşık hale gelmektedir. Dijital totalitarizm kavramı bu çerçevede ortaya çıkmıştır. Dijital totalitarizm, otoriter siyasi iktidarların dijital teknolojilerden oluşan yeni araçlar edinmesi anlamına gelmiştir. Bu durum, internetin bireysel özgürlükleri arttıracak ya da toplumları daha açık hale getireceği şeklindeki varsayımları tartışmalı hale getirmiştir. Dijital totalitarizmin Hu döneminden itibaren ve özellikle Xi

döneminde Çin'in önemli bir örneğini oluşturduğu düşünülmektedir. Büyük Güvenlik Duvarı ve Sosyal Kredi Sistemi dijital totalitarizm ile oluşturulan gözetim ve sansür mekanizmalarının uç noktası olarak görülmektedir. Öte yandan, Çin hükümeti yetkilileri ve devlete ait medya kuruluşları, gelen eleştirilere karşı çok partili "Batı tipi" demokrasi anlayışından farklı olan Çin'e özgü "internet demokrasi"sinden söz etmektedir (MacKinnon, 2012: 65). "Çin'e özgü" ifadesinin 1980'lerin başından itibaren pek çok kavram ile bir araya getirildiği bilinmektedir. Goldsmith ve Wu (2006) da daha devlet odaklı bir yaklaşımla Çin'deki internetin kendine özgülüğüne vurgu yapmaktadır. Buna göre, Çin'de Batı'dan farklılaşan ulusal bir internet ortaya çıkmaktadır ve bu durumu basitçe önceki dönemlerde de pek çok durumda uygulanan devletin fiziksel zorlaması olarak görmek mümkündür (Goldsmith ve Wu, 2006: 180, 184).

Çin'in Mao döneminde totaliter bir sisteme sahip olduğu, reform sürecinde bu yapının kısmen yumuşadığı tartışılmaktadır. Öte yandan, tek parti sisteminin değişmemiş olması Batı tarafından eleştirilmeye devam etmiştir ve Xi döneminde Çin'in çok daha merkezîyetçi ve otoriter hale geldiği değerlendirilmektedir. Dijital teknolojilerin gözetim, denetim ve sansür amacıyla kullanımıyla ortaya çıkan dijital totalitarizm bu durumun hem aracını hem de sonucunu oluşturmaktadır. Çin'in tarihsel koşullarının yanında, yirmi birinci yüzyılın başından itibaren internet kullanımının yaygınlaşmasıyla birlikte ortaya çıkan siyasi, toplumsal ve ekonomik dönüşüm ve bunların birbirleriyle ilişkileri dijital totalitarizm eğiliminin ortaya çıkmasında ve artmasında etkili olmuştur. İfade özgürlüğünü sınırlayan bu tür uygulamalar ve düzenlemeler toplumun belirli kesimleri tarafından tepkiyle karşılanırken, bunları Çin hükümetinin çıkarlarını koruma ya da toplumsal düzenin sağlanması açısından meşru

KAYNAKÇA

- Anderson, D. (2012, 30 Kasım). Splinternet behind the Great Firewall of China. *ACM Queue*, 10(11). <https://queue.acm.org/detail.cfm?id=2405036>
- Aradau, C., & McCluskey, E. (2021). Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes. *International Political Sociology*, 16(1), 1–31. <https://doi.org/10.1093/ips/olab024>
- Arendt, H. (1951). *The origins of totalitarianism*. New York: Harcourt, Brace & Company.
- Aron, R. (1965). *Democracy and totalitarianism: A theory of political regimes*. Garden City, NY: Doubleday & Company.
- Bicker, L. (2025, 5 Ağustos). Protests in China over viral school bullying case. *BBC News*. <https://www.bbc.com/news/articles/c5yeg864g54o>
- Cadwalladr, C., & Graham-Harrison, E. (2018, 17 Mart). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Chan, T. F. (2018, 21 Mayıs). China's social credit system has blocked people from taking 11 million flights and 4 million train trips. *Business Insider*. <https://www.businessinsider.com/china-social-credit-system-blocked-people-taking-flights-train-trips-2018-5>
- Chepenko, D. (2020, 21 Temmuz). Demystifying the Great Firewall of China. *Medium*. <https://medium.com/mobile-asia/demystifying-the-great-firewall-of-china-22f4a97550cc>
- CGTN. (2019, 29 Ocak). BT becomes first foreign telecoms firm to secure Chinese license. *China Daily*. <https://www.chinadaily.com.cn/a/201901/29/WS5c4fbdfca3106c65c34e70b2.html>
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Creemers, R. (2018). China's social credit system: An evolving practice of control. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3175792>
- Creemers, R. (Çev.). (1996, February 1). Provisional management regulations for the international connection of computer information networks of the People's Republic of China [Çeviri]. *DigiChina, Stanford University*. <https://digichina.stanford.edu/work/provisional-management-regulations-for-the-international-connection-of-computer-information-networks-of-the-peoples-republic-of-china/>
- Deibert, R. (2016). Authoritarianism goes global: Cyberspace under siege. *Journal of Democracy*, 26(3), 64–78. <https://doi.org/10.1353/jod.2015.0061>
- Deibert, R. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi.

- Disis, J. (2021, 22 Kasım). China fines Alibaba, Tencent and Baidu for more antitrust violations. *CNN Business*. <https://edition.cnn.com/2021/11/22/tech/alibaba-tencent-fines-intl-hnk/index.html>
- Dou, E. (2022, 19 Ocak). China warns foreign Olympic athletes against speaking out on politics at Winter Games. *The Washington Post*. <https://www.washingtonpost.com/sports/olympics/2022/01/19/china-winter-olympics-politics-speech/>
- Erixon, F., & Lee-Makiyama, H. (2011). Digital authoritarianism: Human rights, geopolitics and commerce (ECIPE Occasional Paper No. 5/2011). *European Centre for International Political Economy*.
- Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, 30(1), 40–52.
- Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
- Feng, J., Yu, Y., & Xu, T. (2023). Content regulation laws for Chinese ISPs: Legal responsibilities in free speech and filtering of harmful content. *Law and Economy*, 2(11), 53–59. <https://doi.org/10.56397/LE.2023.11.07>
- Firstpost. (2024, 20 Mayıs). Chinese social media companies crack down on posts showing off wealth. *Firstpost*. <https://www.firstpost.com/explainers/chinese-social-media-companies-crackdown-on-posts-showing-off-wealth-13772777.html>
- Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Çev.). New York: Pantheon Books.
- Foucault, M. (1978). *The history of sexuality: An introduction* (R. Hurley, Çev.). New York: Pantheon Books.
- Freedom House. (2022). *China: Freedom on the Net 2022 Country Report*. <https://freedomhouse.org/country/china/freedom-net/2022>
- Freedom House. (2024). *Freedom on the Net 2024: The struggle for trust online* [Digital booklet]. <https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>
- Friedrich, C. J., & Brzezinski, Z. K. (1956). *Totalitarian dictatorship and autocracy*. Cambridge, MA: Harvard University Press.
- Global Times. (2020, Eylül 7). *China opens up VPN joint venture to foreign investors*. Global Times. <https://www.globaltimes.cn/content/1200193.shtml>
- Global Times. (2021, 21 Aralık). *Overseas organizations, individuals not allowed to operate online religious info services within the Chinese territory: regulations*. Global Times. <https://www.globaltimes.cn/page/202112/1242971.shtml>
- Global Times. (2024, May 16). *Chinese social media vows to crack down on online content that flaunts wealth, create healthy ecosystem*. Global Times. <https://www.globaltimes.cn/page/202405/1312456.shtml>
- Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.
- Greitens, S. C. (2020). Surveillance, security, and liberal democracy in the post-COVID world. *International Organization*, 74(S1), E169–E190. <https://doi.org/10.1017/S0020818320000417>
- Hawkins, A. (2022, 11 Temmuz). ‘Alarming’ rise in regional internet censorship in China, study finds. *The Guardian*. <https://www.theguardian.com/world/2022/jul/11/china-violent-clashes-at-protest-over-frozen-rural-bank-accounts>
- Hawkins, A. (2025, 24 Mayıs). ‘Alarming’ rise in regional internet censorship in China, study finds. *The Guardian*. <https://www.theguardian.com/world/2025/may/24/alarming-rise-in-regional-internet-censorship-in-china-study-finds>
- Hendrikse, R. (2021). The rise of neo-illiberalism. *Krisis: Journal for Contemporary Philosophy*, 41(1), 65–93. <https://doi.org/10.21827/krisis.41.1.36983>
- Hintz, A., Dencik, L., & Wahl-Jørgensen, K. (2019). *Digital citizenship in a datafied society*. Polity Press.

Huang, E., & Horwitz, J. (2022, 21 Temmuz). Beijing said Facebook and Google are welcome back to China as long as they “respect China’s laws”. *Quartz*. <https://qz.com/808130/beijing-said-facebook-and-google-are-welcome-back-to-china-as-long-as-they-respect-chinas-laws>

Interesse, G. (2024, 2 Ekim). China issues new regulations on network data security management, effective January 1, 2025. *China Briefing*. <https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/>

Khalik, R. u. (2020, 8 Aralık). China takes down 105 apps, including US’ TripAdvisor. *Anadolu Ajansı*. <https://www.aa.com.tr/en/asia-pacific/china-takes-down-105-apps-including-us-tripadvisor/2069781>

Kohn, J. (2002). Arendt’s concept and description of totalitarianism. *Social Research*, 69(2), 634.

Kostka, G. (2019). China’s social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21(7), 1565–1593. <https://doi.org/10.1177/1461444819826402>

Lei, Y.-W. (2018). *The contentious public sphere: Law, media, and authoritarian rule in China*. Princeton University Press.

Levine, Y. (2018). *Surveillance Valley: The secret military history of the Internet*. PublicAffairs.

Li, J., & De Silva, M. (2022, July 21). This is the blacklist Apple uses to censor the internet in China. *Quartz*. <https://qz.com/1737232/apple-and-tencent-use-this-blacklist-to-censor-safari-in-china>

Longo, A. (2024). Reversing the primacy of political action: Thinking politics and technology with Arendt. *Arendt Studies*, 8, 89–113. <https://doi.org/10.5840/arendtstudies20248759>

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

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom*. Basic Books.

Mac Síthigh, D. & Siems, M. (2019). The Chinese social credit system: A model for other countries? *Modern Law Review*, 82(6), 1034–1071. <https://doi.org/10.1111/1468-2230.12462>

Mann, J. (2023, 10 Kasım). Meta is returning to China 14 years after Facebook was blocked by striking a deal with Tencent to sell its VR headsets. *Business Insider*. <https://www.businessinsider.com/meta-returns-china-striking-deal-tencent-2023-11>

Miller, C. (2018). *The death of the gods: The new global power grab*. William Heinemann.

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. PublicAffairs.

Nguyen, H. C. (2024, 11 Kasım). Main concerns about China data protection regulations for ISPs. *Cloudi Fi*. <https://www.cloudi-fi.com/blog/main-concerns-about-china-data-protection-regulations-for-isp>

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>

O’Brien, K. J., & Stern, R. E. (2008). Introduction: Studying contention in contemporary China. In *Popular protest in China* (pp. 11–25). Harvard University Press. <https://doi.org/10.4159/9780674041585-intro>

Orwell, G. (2019). 1984 (N. Arık, Çev.). Can Yayınları. (Orijinal eser 1949’da yayımlandı)

Padden, M. (2023). The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy. *Internet Policy Review*, 12(3). <https://doi.org/10.14763/2023.3.1720>

Peron, A. E. d. R., de Magalhães, D. A. M., & Caetano, G. F. (2025). Beyond digital repression: Techno-authoritarianism in radical right governments. *Cogent Social Sciences*, 11(1), Article 2528457. <https://doi.org/10.1080/23311886.2025.2528457>

Qiang, X. (2019). The road to digital unfreedom: President Xi’s surveillance state. *Journal of Democracy*, 30(1), 53–67.

Reuters. (2022, 10 Temmuz). China regulator fines Alibaba, Tencent for disclosure violations. *Reuters*. <https://www.reuters.com/world/china/china-regulator-fines-alibaba-tencent-disclosure-violations-2022-07-10/>

- Taşdan, M. (2023). Sosyal kredi sisteminin eğitim ve okul yönetimine yansımaları. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi*, 23(2), 166–176. <https://doi.org/10.53629/sakaefd.1348301>
- Thatcher, J., O’Sullivan, D., & Mahmoudi, D. (2017). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, 34(6), 990–1006. <https://doi.org/10.1177/0263775816633195>
- Thibault, H. (2025, 18 Temmuz). China’s new digital identity system boosts the government’s control over citizens online. *Le Monde*. https://www.lemonde.fr/en/international/article/2025/07/18/in-china-a-new-digital-identity-has-increased-the-government-s-control-over-citizens-online-activities_6743473_4.html
- Thomas, A. (2024). *The politics and ethics of transhumanism: Techno-human evolution and advanced capitalism*. Bristol University Press.
- Tiezzi, S. (2014, 28 Şubat). Xi Jinping leads China’s new Internet security group. *The Diplomat*. <https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/>
- Tüfekçi, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- Tymchyshyn, B. (2020). Totalitarian threats of digital age. *The Journal of V.N. Karazin Kharkiv National University. Issues of Political Science*, 37, 88–95. <https://doi.org/10.26565/2220-8089-2020-37-12>
- World Bank. (2025). Individuals using the Internet (% of population) – China [Indicator IT.NET.USER.ZS]. *World Development Indicators*. Retrieved January 24, 2025, from <https://data.worldbank.org/indicator/IT.NET.USER.ZS>
- Zheng, G., & Shu, J. (2024). In the name of protection—A critical analysis of China's legal framework of children's personal information protection in the digital era. *Computer Law & Security Review*, 53, Article 105979. <https://doi.org/10.1016/j.clsr.2024.105979>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.