T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU BİLİM DALI

DİJİTALLEŞMENİN EGEMENLİK ÜZERİNDEKİ AŞINDIRICI ETKİSİ

Doktora Tezi

MUHAMMET SEFA MUTLU

İstanbul, 2026

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU BİLİM DALI

DİJİTALLEŞMENİN EGEMENLİK ÜZERİNDEKİ AŞINDIRICI ETKİSİ

Doktora Tezi

MUHAMMET SEFA MUTLU

Tez Savunma Jürisi

1. Tez Danışmanı: Prof. Dr. Rükiye AKKAYA
2. Üye: Prof. Dr. Nihat BULUT
3. Üye: Doç. Dr. Oya BOYAR
4. Üye: Doç. Dr. Alper IŞIK
5. Üye: Dr. Öğr. Üyesi Arda ATAKAN

İstanbul, 2026

ÖZET

Bu tez, dijitalleşmenin modern devlet egemenliği üzerindeki etkisini ne teknolojik determinizme ne de devletin kaçınılmaz çözülüşü anlatısına indirgemeden ele almıştır. Dijitalleşme, egemenliği ortadan kaldıran dışsal bir güç değil; onun klasik varsayımlarını, işleyiş biçimini ve meşruiyet temelini eşzamanlı olarak aşındırarak geleneksel formunu sürdürülemez hâle getiren tarihsel bir dönüşüm olarak değerlendirilmiştir. Bu anlamda dijitalleşme, egemenliğin sonunu değil; normatif olarak düzenlenmediği takdirde hem devlet hem de yurttaş açısından ciddi riskler barındıran bir aşınmayı ifade etmektedir.

Çalışma, dijitalleşmenin salt teknik bir ilerleme olmadığını; bilginin üretimini, dolaşımını ve denetimini yeniden örgütleyen yapısal bir iktidar dönüşümü yarattığını ortaya koymuştur. Algoritmalar, yapay zekâ ve siber alan, tarafsız araçlar değil; yeni bir siyasal ve normatif düzenin kurucu unsurlarıdır. İnternetin dağıtık mimarisi ile dijital şirketlerin algoritmik karar süreçlerinin merkezîleştirici etkisi arasındaki gerilim, egemenliğin hukuk ve zor kullanımının ötesinde veri, kod ve altyapı denetimi üzerinden icra edilmesine yol açmaktadır.

Tez, dijital egemenlik kavramının ancak klasik kamu hukuku geleneği içinde ve egemenliğin öznesi olarak devlet korunarak tutarlı biçimde ele alınabileceğini göstermiştir. Dijital kapitalizmin yükselişi; hukuki egemenlik ile fiilî dijital iktidar arasında derin bir ayrışma yaratmakta; yurttaşları demokratik denetimden yoksun, görünmez tahakküm biçimlerine açık hâle getirmektedir.

Sonuç olarak dijital çağda egemenlik ne mutlak devlet yetkisi ne de sınırsız ağ özgürlüğüdür. Egemenliğin geleceği, dijital iktidarın hukuk, demokrasi ve insan onuru ile yeniden bağlanabilmesine bağlıdır.

Anahtar Sözcükler: Dijitalleşme, dijital egemenlik, dijital iktidar, dijital devlet, bilgi toplumu, dijital kapitalizm, platform egemenliği, algoritmik yönetişim, veri egemenliği, tekno feodalizm, kişisel veriler, algoritmik ayrımcılık, dijital gözetim, dezenformasyon, sermayesiz kapitalizm, veri yerelleşmesi, egemenliğin aşınması.

ABSTRACT

This dissertation examines the impact of digitalization on modern state sovereignty without reducing it either to technological determinism or to the narrative of the inevitable dissolution of the state. Digitalization is not treated as an external force that abolishes sovereignty; rather, it is conceptualized as a historical transformation that simultaneously erodes the classical assumptions, operational modes, and legitimacy foundations of sovereignty, thereby rendering its traditional form increasingly unsustainable. In this sense, digitalization does not signify the end of sovereignty but rather an erosion that, unless normatively regulated, entails significant risks for both the state and its citizens.

The study demonstrates that digitalization is not merely a technical advancement; it constitutes a structural transformation of power that reorganizes the production, circulation, and control of knowledge. Algorithms, artificial intelligence, and cyberspace are not neutral tools; they are constitutive elements of a new political and normative order. The tension between the distributed architecture of the internet and the centralizing effects of algorithmic decision-making processes employed by digital corporations leads to the exercise of sovereignty not only through law and coercion but also through the control of data, code, and digital infrastructures.

The thesis further shows that the concept of digital sovereignty can only be coherently addressed within the classical tradition of public law while preserving the state as the subject of sovereignty. The rise of digital capitalism generates a profound divergence between legal sovereignty and de facto digital power, exposing citizens to forms of invisible domination that remain largely beyond democratic oversight.

In conclusion, sovereignty in the digital age is neither absolute state authority nor unlimited network freedom. The future of sovereignty depends on the ability to reconnect digital power with law, democracy, and human dignity.

Keywords: Digitalization, digital sovereignty, digital power, the digital state, the information society, digital capitalism, platform sovereignty, algorithmic governance, data sovereignty, techno-feudalism, personal data, algorithmic discrimination, digital

surveillance, disinformation, capitalism without capital, data localization, erosion of sovereignty.

TEŞEKKÜR

Bu tez, dijitalleşmenin modern devlet egemenliği üzerindeki etkilerini anlama çabasının ve uzun bir araştırma sürecinin sonucunda ortaya çıkmıştır. Çalışma ilerledikçe dijital teknolojilerin yalnızca teknik bir dönüşümü değil, aynı zamanda siyasal iktidarın işleyişini ve egemenliğin kullanım biçimlerini derinden etkileyen bir değişimi ifade ettiği daha açık biçimde görülmüştür.

Araştırmanın önemli bir bölümü, TÜBİTAK 2214-A Yurt Dışı Araştırma Burs Programı kapsamında Hollanda'da Leiden Üniversitesi Alan Araştırmaları Enstitüsü'nde (LIAS) yürütülmüştür. Yabancı literatüre ve karşılaştırmalı ülke uygulamalarına erişim imkânı sağlayan bu destek için TÜBİTAK'a teşekkür etmeyi bir borç bilirim.

Araştırmanın yurtdışı aşamasında, beni Regensburg Üniversitesi'ne davet ederek eşsiz kaynak tarama imkanı sunan Prof. Dr. Jürgen Kühling'e; Leiden Üniversitesi Alan Araştırmaları Enstitüsü'ne (LIAS) davet ederek araştırma imkanı sunan ve dijitalleşmenin ABD, Çin ve Avrupa Birliği açısından karşılaştırmalı ele alınmasına yönelik değerli yönlendirmeleri için Prof. Dr. Florian A. Schneider'a; ve Amsterdam Üniversitesi Bilgi Hukuku Enstitüsü'ne (IViR) davet ederek zengin araştırma ekosisteminde bulunmamı sağlayan ve küresel veri akışları konusundaki katkıları kapsamında Doç. Dr. Kristina Irion'a içten teşekkür ederim.

Çalışmanın ortaya çıkmasında akademik katkısı ve emeği en büyük olan; sabrı ve titizliğiyle her aşamada yol gösteren tez danışmanım Prof. Dr. Rükiye Akkaya'ya özellikle teşekkür etmek isterim. Ayrıca tez jürisi üyeleri Prof. Dr. Bihterin Dinçkol, Prof. Dr. Nihat Bulut ve Dr. Arda Atakan'a da değerli katkıları için teşekkür ederim.

Doktora sürecinin en büyük gücü ise ailem olmuştur. Bu uzun ve yoğun yolculukta beni sabırla destekleyen sevgili eşim Sümeyye'ye ve hayatımıza neşe katan çocuklarımız Muhammed Alperen ve Aybüke Nur'a sevgilerimi sunarım.

İstanbul, 2026 Muhammet Sefa Mutlu

İÇİNDEKİLER

Sayfa No.

ÖZET ..... **i**

ABSTRACT ..... **ii**

İÇİNDEKİLER ..... **v**

KISALTMALAR ..... **ix**

GİRİŞ **1**

BİRİNCİ BÖLÜM

DİJİTALLEŞME: KAVRAMSAL ÇERÇEVE, ETKİLERİ VE AKTÖRLERİ

I. KAVRAMSAL ÇERÇEVE **10**

II. HİBRİT BİR TANIMLAMA: DİJİTAL EGEMENLİK **17**

III. ÜRETİM SÜREÇLERİNİN VE SİYASAL İKTİDARIN BİRLİKTE DÖNÜŞÜMÜ **30**

A. MODERN DÖNEMDEN POST MODERN DÖNEME DÖNÜŞÜMÜN İZLERİ 30

1. Modern Dönem 31

2. Postmodern Dönem 35

B. KÜRESELLEŞME ÖTESİ YENİ ÜRETİM VE YÖNETİM TARZI: DİJİTAL KAPİTALİZM 39

IV. VERİ ODAKLI DİJİTAL TEKNOLOJİLERİN TEMEL BİLEŞENLERİ VE ETKİLERİ **46**

A. BÜYÜK VERİ ANALİTİĞİ VE ENDÜSTRİSİ: VERİNİN YAPAY ZEKÂ ALGORİTMALARIYLA İŞLENMESİ 46

1. Verileşme (Datafication) ve Büyük Veri 46

2. Dijital Profilleme: Kişiselleştirme ve Hedefleme Pratikleri 51

a. Veri Temelli Profilleme Tekniği 53

b. Profillemenin Uygulama Alanları 55

3. Bulut Bilişim: Küresel Veri Akışı ve Veri Egemenliği 58
B. KÜRESELLEŞMİŞ KİTLESEL MEDYA VE İLETİŞİMİN DÖNÜŞÜMÜ .. 62
C. BLOK ZİNCİR (BLOCKCHAİN) TEKNOLOJİLERİ: KRİPTO PARA, NFT VE AKILLI SÖZLEŞME 64
D. ROBOTİK VE OTONOM SİSTEMLER 66
V. DİJİTAL ALANIN AKTÖRLERİ: DEVLETLER VE DİĞERLERİ 67
A. DEVLETLER: EGEMENİN DİJİTAL BİR AKTÖR OLARAK AĞ VE BİLGİ TOPLUMUNU HAKİMİYET ALTINA ALMA ÇABASI 67
1. Dijital Alanda Kontrol ve Hakimiyet: Zorunluluklar 67
2. Dijital Egemenliğe Devlet Yaklaşımları: ABD, Çin ve AB Perspektifleri 74
a. Farklılaşan Yaklaşımlar ve Ulusal Stratejiler 74
b. ABD: Askerî Kökenlerden Neoliberal Küresel Yönetişime 79
c. Çin: Otoriter Ulus-Devlet Merkezli Bilgi Güvenliği Modeli 88
d. AB: Hak ve Değer Temelli Bir Dijitalleşme Modeli 96
3. Dijital Egemenlik Konuları: Devletin Dijital Alanı Düzenleme Araçları 103
a. Ulusal ve Uluslararası Hukuki Mekanizmalar 103
(1) Veri Akışının ve Platform Ekosisteminin Regülasyonu 104
(2) Veri Akışından Para Akışına: Dijital Ekonominin ve Rekabetin Korunması Düzenlemeleri 113
(3) Dijital Suç ve Siber Güvenlik Düzenlemeleri 119
(4) Milli Teknoloji Kullanımını Zorunlu Kılan Düzenlemeler 129
b. Teknik Mekanizmalar 131
(1) Gözetim Teknolojisi ve İçerik Denetim Araçları 132
(2) Dijital Adalet Mekanizmaları 137
(3) Siber Güvenliğe Yönelik Teknik Araçlar 139
c. Egemenlik ile Ekonomik Rasyonalite Arasında Korumacı Politika İkilemi: Veri Yerelleşmesi 141
B. DÜZENLEYİCİ TEKNİK KURULUŞLAR 146
C. BÜYÜK TEKNOLOJİ (BİG TECH) ŞİRKETLERİ 149
D. KULLANICILAR 153
E. SİVİL TOPLUM ÖRGÜTLERİ 156

İKİNCİ BÖLÜM

MODERNİTEDEN POST MODERNİTEYE: DEVLETİN KLASİK UNSURLARININ DÖNÜŞÜMÜ VE EGEMENLİĞİN ETKİ ALANININ YENİDEN DEĞERLENDİRİLMESİ

I. DÖNÜŞÜMÜN DİNAMİĞİ: TARTIŞMAYI MÜMKÜN KILAN ETKENLER 159

II. İNSAN UNSURUNUN DÖNÜŞÜMÜ 167

A. ULUSTAN YENİ TOPLUM BİÇİMLERİNE: DİJİTAL CEMAATLER 169
1. Ulus, Yurttaş ve Küreselleşme 169
2. Yurttaşın Verileşmesi: Küresel Yurttaşlıktan Dijital Yurttaşlığa Dönüşüm 172

B. DİJİTALLEŞMENİN İNSANA VE TOPLUMA ETKİSİ 177
1. Ontolojik Bir Dönüşüm: Homo Juridicus'tan Homo Digitalis'e 177
2. Kapitalist Aklın Dehümanizasyonu: Algoritmik Tahakküm Karşısında Nesneleşme ve Gerçeklik Algısının Kaybolması 180
3. Küreselleşmiş Bilgi Toplumunda Kimlik ve Kültür 183
4. Kontrol Devrimi: Özgürlük Yanılsaması ve Kişiselleştirilmiş Tahakküm 185
5. Tekno-Feodalizm: Dijital Serfliğe Geçiş ve Platform Lordluğu 188

C. İNSAN ODAKLI YAKLAŞIM: TAHAKKÜM VEYA SÖMÜRÜ DEĞİL ERDEMLİ TOPLUM DÜZENİ 190

III. ÜLKE UNSURU: DİJİTALLEŞMENİN MEKÂN VE SINIR KAVRAMINA ETKİSİ 194

A. ÜLKENİN MODERN SİYASİ BİR DEĞER OLARAK VATANA DÖNÜŞÜMÜ 194

B. KÜRESELLEŞMENİN DEVLETİN ÜLKESEL SINIRLARINA ETKİSİ: POST-TERRİTORİAL TARTIŞMA 197

C. DİJİTALLEŞMENİN EGEMENLİĞİN MEKÂNSAL TEMELİNİ DÖNÜŞTÜRMESİ 199

IV. EGEMENLİK 2.0: EGEMENİN DİJİTAL YÜZÜ 207

A. DİJİTAL EGEMENLİK VE DİJİTAL EGEMEN 207
1. Dijital Egemenin Meşruiyet Krizi: Toplumsal Sözleşme Kuramlarının Aşılması 207
2. Yeni Güç Biçimi Olarak Dijital Egemen ve Çok Katmanlı Formu 213
3. Leviathan 2.0: Veri-Tanrı ve Dijital Teoloji 222

B. MODUS DİSRUPTİ: DİJİTALLEŞMENİN EGEMENLİK ÜZERİNDEKİ AŞINDIRICI ETKİSİ 226
1. Devletin Egemenlik Niteliği Açısından 226
a. Devletin; Hukuk, Yasa ve Zor Tekelinin Dijital Alanda Aşınması: Platformların Monist Hukuka Müdahalesi 226
b. Bilgi Üzerindeki Egemenliğin Aşınması 236
c. Dijital Çağda Egemenliğin Koruyucu Niteliğinin Aşınması: Siber Tehditler, Hibrit Savaş ve Veri Güvenliği 241
d. Sermayesiz Kapitalizmi Vergilendirme Sorunu 247
e. Ademimerkeziyetçi Dijital Paralar ve Parasal Egemenliğin Daralması 251
2. Dijital Çağda Temel Hak ve Özgürlükler: Demokratik Toplum Düzeninde Erozyon 254
a. Temel Hak ve Özgürlükleri Koruma ve Yerine Getirme Yükümlülüğünde Zafiyet ve Dijital Anayasacılık 256
b. Algoritmik Ayrımcılık ve Fırsat Eşitliğinin Derinleşmesi 264
c. Gözetim Çağında Kitle İletişimi ve Gizliliğin Çözülmesi 270
d. Dijitalleşmenin Gölgesinde İfade Özgürlüğü: Denetim, Manipülasyon ve Hak İhlalleri 294
e. Dijital Mekânda Kişilik Haklarının Kırılganlaşması 311
f. Veri Temelli Davranışsal Müdahaleler Karşısında Kişinin Maddi ve Manevi Varlığını Geliştirme Hakkının Aşınması 314
SONUÇ 319
KAYNAKÇA 330

KISALTMALAR

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
AI	Artificial Intelligence (Yapay Zekâ)
APEC	Asia-Pacific Economic Cooperation
ARPANET	Advanced Research Projects Agency Network
AYM	Anayasa Mahkemesi
AWS	Amazon Web Services
BAE	Birleşik Arap Emirlikleri
bkz.	Bakınız
BM	Birleşmiş Milletler
CAC	Cyberspace Administration of China
CBDC	Central Bank Digital Currency
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CCPA	California Consumer Privacy Act
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CERN	Avrupa Nükleer Araştırma Merkezi
CISA	Cybersecurity and Infrastructure Security Agency
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
COPPA	Children's Online Privacy Protection Act
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership

CSL	Cybersecurity Law of the People's Republic of China
çev.	Çeviren
DAO	Decentralized Autonomous Organization
DEPA	Digital Economy Partnership Agreement
DES	Data Encryption Standard
DNS	Domain Name System
DSL	Data Security Law of the People's Republic of China
DSA	Digital Services Act
DTÖ	Dünya Ticaret Örgütü
EU	European Union
FEMA	Federal Emergency Management Agency
G20	Group of Twenty
GAFAM	Google, Apple, Facebook (Meta), Amazon, Microsoft
GAIA-X	GAIA-X Data Infrastructure
GATT	General Agreement on Tariffs and Trade
GDPR	General Data Protection Regulation
GPAI	Global Partnership on Artificial Intelligence
GSÜHFD	Galatasaray Üniversitesi Hukuk Fakültesi Dergisi
GSYİH	Gayrisafi Yurt İçi Hasıla
HIPAA	Health Insurance Portability and Accountability Act
IAB	Interactive Advertising Bureau
IBM	International Business Machines
ICANN	Internet Corporation for Assigned Names and Numbers
İHA	İnsansız Hava Aracı

ISO	International Organization for Standardization
IoT	Internet of Things
ITU	International Telecommunication Union
KOBİ	Küçük ve Orta Büyüklükte İşletmeler
KVK	Kişisel Verilerin Korunması
LAWS	Lethal Autonomous Weapon Systems
MiCA	Markets in Crypto-Assets Regulation
m.	Madde
MIT	Massachusetts Institute of Technology
MİT	Millî İstihbarat Teşkilâtı
NATO	North Atlantic Treaty Organization
NetzDG	Netzwerkdurchsetzungsgesetz
NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
par.	Paragraf
PIPL	Personal Information Protection Law
s.	Sayfa
SBE	Sosyal Bilimler Enstitüsü
STK	Sivil Toplum Kuruluşu
TDK	Türk Dil Kurumu
TMK	Türk Medeni Kanunu
UN	United Nations

UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNIDROIT	International Institute for the Unification of Private Law
UYAP	Ulusal Yargı Ağı Bilişim Sistemi
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WHO	World Health Organization
WSIS	World Summit on the Information Society
WTO	World Trade Organization

GİRİŞ

Pisagor'un evrenin temel ilkesi olarak ortaya koyduğu "her şey sayıdır" önermesi, uzun süre metafizik bir varsayım olarak değerlendirilmiştir. Antik Çağ'da dile getirilen bu düşünce, evrenin sayısal bir düzen içinde kavranabileceği ve varlığın matematiksel bir yapı üzerinden açıklanabileceği inancına dayanıyordu. Aradan geçen iki bin yılı aşkın süre boyunca bu önerme daha çok felsefi bir spekülasyon alanında kalmış görünse de dijital çağda bilgisayar teknolojileri, algoritmalar, veri işleme teknikleri ve küresel internet ağlarının birleşimiyle birlikte, bu önerme somut bir tarihsel ve siyasal gerçekliğe dönüşme potansiyeli kazanmıştır. Bugün sayı, yalnızca doğayı betimlemenin ya da bilimsel kesinliğin dili değildir; aynı zamanda iktidarın, yönetimin, denetimin, tüketimin, iletişimin ve hatta insan davranışlarının öngörülmesinin de temel aracına dönüşmüştür. Sayıların soyut düzeni, fiziksel evreni açıklayan bir model olmanın ötesinde, bireyin toplumsal hayattaki görünürlüğünü, piyasanın tahakküm biçimlerini, insan davranışlarını, siyasal karar alma süreçlerini ve egemenlik ilişkilerini yapılandıran bir gerçeklik hâlini almıştır.

Bu nedenle dijitalleşme sadece sıradan bir teknolojik yenilik ya da iletişim araçlarının ilerlemesi olarak görülemez. Dijitalleşme, kökenleri yirminci yüzyılın başlarına kadar götürülebilecek olmakla birlikte, özellikle postmodern çağda etkisini yoğun biçimde hissettiren ve yaşamın neredeyse tüm alanlarını ikili (binary) kod sistemine dayalı teknik bir dile tercüme eden çok katmanlı bir dönüşüm sürecidir. Bu süreçte, maddi gerçeklik bilgisayarın işlem mantığına uygun biçimde veriye, koda ve algoritmik işleme tabi kılınmakta; somut olan dijital ortamın teknik dili içinde sayısal temsillere dönüştürülmektedir. Böylece birey, toplum ve devlet arasındaki ilişkiler yeni bir teknik dil, yeni bir etkileşim zemini ve yeni bir iktidar mimarisi üzerinden yeniden kurulmaktadır. İnternetin ve veri odaklı dijital teknolojilerin iletişim, ticaret, siyasal katılım, kültürel dolaşım, güvenlik, eğitim, sağlık ve kamu yönetimi gibi hayatın neredeyse bütün alanlarına nüfuz etmesi bu dönüşümün kapsamını ve derinliğini göstermektedir. Bununla birlikte bu süreçte bireysel irade, mahremiyet ve kamusal

denetim giderek kırılganlaşmış; bireylerin ve dijitalleşmede başat aktör konumunda olmayan birçok devletin denetim kapasitesi aynı anda zayıflamaya başlamıştır.

Dijitalleşmenin vaat ettiği hız, erişim ve verimlilik onun yalnızca görünen yüzünü oluşturmaktadır. Dijital teknolojiler günlük yaşamı kolaylaştırırken aynı zamanda bireyin dikkatini, davranışlarını ve tercihlerini izlenebilir, ölçülebilir, sınıflandırılabilir ve yönlendirilebilir hâle getirmektedir. İnsan düşüncesinin ürünü olan algoritmalar tarafsız ve nötr araçlar gibi görünseler de onları tasarlayan ekonomik, kültürel ve siyasal akıllardan bağımsız değildir. Aksine algoritmalar belirli değer seçimleri, ticari hedefler ve iktidar mantıkları içinde inşa edilmekte; bireyin karşılaştığı bilgiyi, maruz kaldığı içerikleri, kurduğu ilişki biçimlerini ve çoğu zaman siyasal kanaatlerini de biçimlendirmektedir. Bu çerçevede dijitalleşme; özgürleştirici potansiyeller taşıdığı kadar gözetimi derinleştiren, eşitsizlikleri yeniden üreten, toplumsal farklılıkları verileştirerek sınıflandıran ve yeni bağımlılık ilişkileri yaratan yapısal bir dönüşüm olarak ortaya belirmektedir.

Dijitalleşmenin anlamı yalnızca bireysel yaşam pratiklerindeki değişimde aranamaz. Bu süreç aynı zamanda küresel kapitalist üretim ilişkilerinin yeni bir evresine işaret etmektedir. Sanayi kapitalizmiyle kurulan modern üretim ilişkileri küreselleşme ile ulusötesi bir niteliğe bürünmüş; sermaye, emek, üretim, dolaşım ve karar alma süreçleri ulusal sınırları aşan ağlar içinde yeniden örgütlenmiştir. Postmodern dönemde bilgi ve veri; üretimin yardımcı unsurları olmaktan çıkıp asli girdisi hâline gelerek ekonomik ve siyasal iktidarın başlıca kaynakları arasına girmiştir. Bilginin bilgiye uygulanması olarak tanımlanabilecek bu aşama, ekonomik üretim tarzlarının yanında yönetim tekniklerini, toplumsal denetim biçimlerini ve siyasal otoritenin işleyişini de dönüştürmüştür. Bu nedenle dijitalleşme kapitalizmin teknik evriminin ötesinde yeni birikim stratejileri, yeni mülkiyet biçimleri ve yeni tahakküm mekanizmaları yaratan tarihsel bir kırılmadır.

Küreselleşme söylemi uzun süre insan hakları, demokrasi, iletişim özgürlüğü, bilgiye erişim ve sınırların aşılması gibi olumlu değerler etrafında meşrulaştırılmıştır. Ancak pratikte küreselleşme, çoğu durumda eşitsizlikleri azaltan değil, onları yeni biçimlerde yeniden üreten; emperyal ilişkileri görünmezleştirip derinleştiren, ekonomik ve kültürel hegemonya biçimlerini evrensellik söylemi içinde dolaşıma sokan bir düzen

yaratmıştır. Dijitalleşme küresel kapitalist düzenin daha yoğun, daha sofistike ve daha görünmez işleyen bir toplumsal mühendislik evresine karşılık gelmektedir. Çünkü günümüzde ortaya çıkan platform kapitalizmi ve veri temelli iş modelleri; mal ve hizmet üretiminin ötesine geçip davranış, yönelim, dikkat, etkileşim, toplumsal ilişki ve yaşam biçimlerini de üretmektedir.

Küresel ölçekte oligopol kurmuş teknoloji şirketleri, sundukları hizmetler aracılığıyla bireylere ait büyük miktarda veriyi toplamakta, sınıflandırmakta, işlemekte ve ekonomik değer üretimine dönüştürmektedir. Ancak bu süreç piyasa için olduğu kadar siyasal iktidar bakımından da önemlidir. Çünkü veri birikimi, ekonomik tahakkümün dışında; davranışsal öngörü ve yönlendirme imkânı da yaratmaktadır. Büyük veri analitiği, dijital profilleme, kişiselleştirme, hedefleme, içerik sıralama, tavsiye sistemleri ve bulut bilişim altyapıları, bireyin dijital ortamda neyi göreceğini, neyi önemseyeceğini, neye maruz kalacağını ve neye tepki vereceğini belirleyebilecek bir etki alanı oluşturmaktadır. Böyle bir düzende bilgi; sınıflandıran, yönlendiren ve denetleyen bir güç hâline gelmektedir. Bu yeni tekno-ekonomik paradigma karşısında bireyler ve devletler, çoğu zaman sürecin asimetrik ve denetimsiz niteliğini ancak geri dönülmesi güç bir aşamada fark etmektedir. Bilginin bilgiye uygulandığı bu yeni üretim düzeni; klasik siyasal, ekonomik ve hukuki kategorileri zorlayan bir bilgi toplumu ortaya çıkarmıştır.

Dijital kapitalizmin kâr, erişim ve veri mülkiyeti üzerine kurulu teleolojisi; insan hakları, mahremiyet ve demokratik meşruiyet bakımından ciddi riskler üretmektedir. Devletin ülkesindeki denetim kapasitesini aşan iktidar odaklarının ortaya çıkması; egemenlik ile yurttaş ve egemenlik ile ülke arasındaki kurucu bağları zayıflatmaktadır. Bu bağlamda tehlike, teknolojinin kendisinden ziyade onu araçsallaştıran ve devletlerin denetimi altında olmayan yeni kapitalist mantıktan kaynaklanmaktadır. Dolayısıyla dijitalleşmenin olumsuz etkilerinin giderilmesi; teknolojik araçların normatif ve hukuki çerçeveler içinde yeniden ele alınmasını zorunlu kılmaktadır.

Bu tezin çıkış noktası tam da burada belirginleşmektedir: Dijitalleşme yalnızca teknik, ekonomik veya iletişimsel bir dönüşüm değildir; aynı zamanda egemenliğin doğasını, araçlarını, sınırlarını ve meşruiyet zeminini dönüştüren siyasal-hukuki bir olgudur. Bu dönüşümün en önemli sonuçlarından biri, modern devlet egemenliğinin

klasik dayanaklarının sarsılmaya başlamasıdır. Modern devlet teorisinde egemenlik, belirli bir ülke ve halk üzerinde nihai, bağımsız ve üstün otoriteyi ifade eder. Jean Bodin'den itibaren siyaset ve hukuk düşüncesinin merkezinde yer alan bu kavram; norm koyma tekelini, zor kullanma yetkisinin merkezîleşmesini ve kamusal düzenin nihai merciini ifade eden kurucu bir ilke olarak kabul edilmiştir. Ancak dijital çağ, egemenliğin uygulanma araçlarını ve sınırlarını önemli ölçüde zorlamakta; bu kavramın teorik ve kuramsal temellerini yeniden tartışmaya açmaktadır. Modern dönemde beşikten mezara kadar toplumun her aşamasını düzenleyerek biyopolitik bir karakter kazanan egemenlik, dijitalleşme ile yalnızca ulus-devletler tarafından kullanılan bir iktidar biçimi olmaktan kısmen uzaklaşmaktadır. İnternetin sınır aşan doğası, küresel veri akışları, bulut altyapıları ve platform ekosistemleri gibi yeni teknolojik yapılar; egemenliğin klasik mekânsal ve işlevsel sınırlarını belirsizleştirmektedir. Blok zincir tabanlı yapılar, dijital para biçimleri, siber saldırılar, otonom sistemler ve küreselleşmiş dijital kitle iletişimi de bu dönüşümü derinleştiren unsurlar arasında yer almaktadır.

Nitekim küresel ölçekte faaliyet gösteren büyük teknoloji şirketleri; veri, algoritma ve dijital altyapılar üzerindeki denetimleri sayesinde ekonomik ve siyasal etki üretebilen yeni güç merkezleri hâline gelmişlerdir. Bu şirketlerin sahip olduğu veri birikimi ve algoritmik yönlendirme kapasitesi, bireylerin davranışlarını, tercihlerini ve hatta siyasal kanaatlerini dolaylı biçimde etkileyebilmektedir. Böyle bir ortamda bilgi ekonomik bir kaynak olmanın ötesinde aynı zamanda yönlendiren, sınıflandıran ve denetleyen bir iktidar aracına dönüşmektedir. Bu gelişmeler devlet egemenliğinin klasik biçimde işleyişini zorlaştırmakta ve egemenliğin bazı alanlarda aşınmasına yol açmaktadır.

Bir zamanlar ülke, halk ve siyasal iktidar arasındaki sıkı bağ üzerinden kavranan egemenlik artık veri merkezleri, dijital platformlar, algoritmik arayüzler ve sınır aşan enformasyon akışları üzerinden yeniden düşünülmek zorundadır. Bu bağlamda egemenlik meselesi yalnızca belirli bir ülke üzerinde münhasır hâkimiyet kurma sorunu olmaktan çıkmakta; veri, bilgi, dijital altyapı ve ağ mimarileri üzerinde denetim kurma meselesine doğru kaymaktadır. Bu dönüşüm, devletin klasik egemenlik araçlarının bazı

alanlarda zayıflamasına yol açarken kamusal otoritenin farklı aktörlerle paylaşılmak zorunda kaldığı yeni bir düzenin ortaya çıkmasına neden olmaktadır.

Bununla birlikte dijitalleşmenin egemenlik üzerindeki etkisi tek yönlü değildir. Bu çalışma, dijitalleşmenin egemenliği bazı alanlarda aşındırırken bazı alanlarda ise hukuki ve teknik araçlar yoluyla pekiştirdiğini de özellikle görünür kılmaktadır. Veri toplama, eşleştirme ve analiz teknikleri devletin gözetim kapasitesini artırarak idarenin toplumu daha ayrıntılı izlemesine imkân tanımaktadır. E-devlet uygulamaları, dijital kamu hizmetleri, veri temelli idari koordinasyon araçları ve yapay zekâ destekli karar sistemleri ise yönetsel kapasiteyi güçlendirerek kamu karar süreçlerini hızlandırmaktadır. Aynı şekilde siber güvenlik araçları, istihbarat teknolojileri ve içerik denetim mekanizmaları devletin güvenlik kapasitesini artırırken; veri yerelleştirmesi, dijital piyasa düzenlemeleri ve rekabet hukuku araçları ekonomik ve düzenleyici kapasitenin güçlenmesine katkı sağlamaktadır. Bu nedenle dijitalleşme, egemenliği yalnızca zayıflatan değil, aynı zamanda yeni araçlar ve kurumsal düzenekler üzerinden yeniden yapılandıran bir süreç olarak ortaya çıkmaktadır. Bununla birlikte bu pekişme normatif bakımdan kendiliğinden olumlu değildir; zira aynı teknolojik araçlar temel hak ve özgürlükler üzerinde yoğun gözetim ve müdahale riskleri de doğurabilmektedir.

Bu çalışma, dijitalleşmenin devlet egemenliği üzerindeki etkisini Genel Kamu Hukuku perspektifinden ele almaktadır. Dijital egemenlik kavramına ilişkin temel sorun, bu kavramın kamu hukukunun kuramsal çerçevesi içine nasıl yerleştirileceğidir. Egemenliğin devlet dışı aktörlere atfedilmesi ya da salt fiilî kontrol kapasitesine indirgenmesi, kavramın hukuki ve siyasal içeriğini aşındırmaktadır. Oysa Genel Kamu Hukuku disiplini, devleti yalnızca betimleyen değil; onu hukuk, adalet ve meşruiyet ilkeleriyle birlikte değerlendiren normatif bir bakış açısına sahiptir. Bu nedenle dijitalleşmenin egemenlik üzerindeki etkilerinin analizi, "olan" ile birlikte "olması gerekeni" de tartışmayı gerektirmektedir.

Bu tez, dijitalleşmenin devlet egemenliğini tamamen ortadan kaldırdığı yönündeki indirgemeci yaklaşımları reddetmektedir. Ancak aynı zamanda dijitalleşmenin egemenliği klasik biçimiyle sürdürülemez hâle getirdiğini savunmaktadır. Çalışmanın amacı; dijitalleşmenin egemenlik üzerindeki etkisini tarihsel, ekonomik, siyasal ve

normatif boyutlarıyla birlikte analiz ederek; modern ulus-devlet teorisi ve insan hakları bağlamında yarattığı tahribatı görünür kılmaktır. Bu çerçevede dijitalleşmenin devlet ile birey arasındaki ilişkiyi nasıl dönüştürdüğü, farklı siyasal sistemlere sahip devletlerin dijitalleşme karşısındaki tutumları ve bu sürecin ulusal ve uluslararası düzeydeki yansımaları karşılaştırmalı olarak incelenmektedir.

Bu bağlamda araştırma problemi, dijitalleşmenin modern ulus-devlet egemenliğini hangi yönlerden aşındırdığı, hangi yönlerden dönüştürdüğü ve hangi koşullarda onu yeni teknik araçlarla pekiştirdiği sorusunda düğümlenmektedir. Çalışma şu temel soruların peşinden gitmektedir: Egemenliğin, dijital çağda klasik unsurları nasıl aşınmakta ve yeniden üretilmektedir? Veri, algoritma ve dijital altyapı üzerinde kontrol kurma kapasitesi, egemenliğin yeni bir görünümü olarak değerlendirilebilir mi? Büyük teknoloji şirketlerinin fiilî güç yoğunlaşması, devlete rakip bir egemenlik yaratmakta mıdır, yoksa bu durum egemenliğin değil yalnızca iktidar kümelenmelerinin çoğalmasına mı işaret etmektedir? Dijitalleşme devletin birey üzerindeki müdahale kapasitesini artırırken, küresel dijital sermaye karşısında aynı anda devleti zayıflatan çelişkili bir süreç mi üretmektedir? İnsan hakları, özgürlük, eşitlik, demokrasi ve insan onuru bakımından dijital çağda devletin rolü nasıl yeniden tanımlanmalıdır?

Tez bu sorulara cevap ararken; kavramsal ve tarihsel çözümleme, karşılaştırmalı inceleme ve normatif değerlendirmeyi birlikte kullanan çok katmanlı bir yöntem izlemektedir. Bu bakımdan çalışma, salt pozitif hukuk incelemesi değildir; kamu hukuku temelli, tarihsel-sosyolojik verileri dikkate alan, fakat nihai olarak normatif sonuçlara yönelen bir metodoloji takip etmektedir. Siyaset bilimi, devlet teorisi, kamu hukuku, insan hakları teorisi, küreselleşme tartışmaları ve dijital kapitalizm literatürü bir arada okunmakta; ancak analiz, nihai olarak Genel Kamu Hukuku disiplininin kavramsal ve normatif çerçevesi içinde yürütülmektedir. Bu tercih özellikle önemlidir. Çünkü dijitalleşme üzerine yürütülen birçok tartışma ya teknik determinizme ya ekonomik indirgemeciliğe ya da yalnızca güvenlik merkezli okumaya kaymaktadır. Oysa bu tez, dijitalleşmeyi; devlet, toplum, birey ve piyasa arasındaki iktidar ilişkilerini yeniden kuran tarihsel bir dönüşüm süreci olarak ele almaktadır.

Tezin ana iddiası şudur: Dijitalleşme, egemenliği ortadan kaldıran dışsal bir teknik dalga değil; onu aynı anda hem aşındıran hem merkezîleştiren, hem zayıflatan hem güçlendiren, hem sınırlarını delen hem de yeni sınırlandırma teknikleri üreten tarihsel bir yeniden yapılanma sürecidir. Bu nedenle dijital çağın temel meselesi, devletin var olup olmayacağı değil; ne tür bir devletin, hangi araçlarla, hangi meşruiyet temelinde ve kimin yararına dijital alanı düzenleyeceğidir. Tez, dijital alanın hukuk dışı bırakılamayacağını; fakat aynı zamanda salt güvenlik ve kontrol mantığına da teslim edilemeyeceğini savunmaktadır. Esas mesele, dijitalleşmenin yarattığı yeni iktidar kümeleri karşısında insan haklarını ve demokratik meşruiyeti koruyabilecek kamusal-hukuki çerçevenin ne olacağıdır.

Kapsamı açısından bu çalışmanın odak noktası, dijitalleşmenin teknik ayrıntılarından ziyade egemenlik, devlet teorisi, insan hakları, meşruiyet, kamusal düzen ve siyasal iktidar bakımından ne ifade ettiğidir. Bu kapsamda tez; dijital egemenlik kavramı, dijital kapitalizm, veri temelli yönetim, platform gücü, devletlerin dijital alanı düzenleme araçları, dijital gözetim, veri yerelleşmesi, bilgi üzerindeki egemenliğin aşınması, dijital çağda temel hak ve özgürlüklerin kırılganlaşması, dijital yurttaşlık, dijital cemaatler, mekân ve sınır kavramının dönüşümü, dijital egemen figürü ve egemenliğin dijital yüzü gibi meselelere temas etmektedir.

Buna karşılık çalışma, bilinçli olarak bazı alanları kapsam dışında bırakmaktadır. Öncelikle pekiştirdiğini kabul etmekle birlikte bu çalışma merkez odağına dijitalleşmenin egemenlik üzerindeki aşındırıcı etkisini almıştır. Çalışmanın amacı yazılım mühendisliği, bilgisayar bilimi ya da yapay zekâ algoritmalarının teknik mimarisi üzerine ayrıntılı bir teknik inceleme yapmak değildir. Keza siber güvenliğin salt operasyonel ve teknik boyutu, kriptografik protokollerin ayrıntıları, blok zincir sistemlerinin mühendislik mantığı veya dijital piyasalardaki mikro işletme stratejileri de tezin asli konusu değildir. Bunlara yalnızca egemenlik ve kamu hukuku tartışmasını açıklamaya katkı sağladıkları ölçüde değinilmektedir.

İçindekiler kısmındaki bölümleme de tezin düşünsel güzergâhını ortaya koymaktadır. İlk olarak kavramsal çerçeve ve dijital egemenliğin hibrit karakteri tartışılmakta; böylece kavramın neden hem kullanışlı hem de teorik bakımdan riskli

olduğu gösterilmektedir. Ardından modern dönemden postmodern döneme uzanan tarihsel dönüşüm ve dijital kapitalizmin ortaya çıkışı incelenerek, dijitalleşmenin üretim süreçleriyle siyasal iktidarın birlikte dönüştüğü bir tarihsel uğrak olduğu savunulmaktadır. Sonraki aşamada veri odaklı dijital teknolojilerin temel bileşenleri, büyük veri, verileşme, profilleme, bulut bilişim, küresel iletişim dönüşümü, blok zincir, kripto paralar, akıllı sözleşmeler, robotik ve otonom sistemler üzerinden ele alınarak; egemenlik tartışmasının soyut bir düzlemde kalmaması için teknik zeminin siyasal anlamı açıklanmaktadır.

Bunun ardından dijital alanın aktörleri olarak devletler, düzenleyici teknik kuruluşlar, büyük teknoloji şirketleri, kullanıcılar ve sivil toplum örgütleri incelenmektedir. Özellikle devletlerin dijital egemenliğe yaklaşımı bağlamında ABD, Çin ve AB örnekleri üzerinden farklı siyasal akılların siber alanı nasıl kavradığı ve düzenlediği gösterilmektedir. Bu kısım, tezin yalnızca teorik değil, somut kamu politikaları ve hukuki düzenleme araçları bakımından da karşılaştırmalı bir zemin üzerinde ilerlediğini göstermektedir. Ulusal ve uluslararası hukuki mekanizmalar, veri akışı ve platform ekosistemi regülasyonları, dijital ekonomi ve rekabet hukuku araçları, dijital suç ve siber güvenlik düzenlemeleri, milli teknoloji kullanımını teşvik eden politikalar, teknik gözetim ve içerik denetim araçları, dijital adalet mekanizmaları ve veri yerelleşmesi gibi araçlar, egemenliğin dijital çağda nasıl yeniden kurulduğunu ya da savunulduğunu göstermesi bakımından merkezi önemdedir.

Tez daha sonra dijitalleşmenin modern devletin kurucu unsurlarına etkilerine yönelmekte ve öncelikle insan unsurunun dönüşümünü analiz etmektedir. Çünkü egemenlik devletin kurumsal varlığının yanında aynı zamanda ulus, yurttaşlık, aidiyet, kimlik ve insan tasavvuruyla da ilgilidir. Dijital cemaatlerin yükselişi, yurttaşın verileşmesi, küresel yurttaşlıktan dijital yurttaşlığa geçiş, homo juridicus'tan homo digitalis'e dönüşüm, algoritmik tahakküm, dehümanizasyon, özgürlük yanılsaması, kişiselleştirilmiş tahakküm ve tekno-feodalizm gibi tartışmalar, dijital çağda insanın artık yalnızca hukukun öznesi değil, aynı zamanda verinin nesnesi hâline gelme riskini taşıdığını göstermektedir. Bu nedenle tez, dijital egemenlik meselesini salt devlet merkezli değil, insan onuru ve erdemli toplum düzeni bakımından da ele almaktadır.

Ülke unsurunun dönüşümü de tezin temel eksenlerinden biridir. Modern siyasal düzende vatan, sınır, toprak ve ülkesellik, egemenliğin mekânsal temelini oluşturmuştur. Oysa küreselleşme ve dijitalleşme, post-territorial tartışmaları gündeme getirerek devletin ülkesel sınırlarının işlevini tartışmalı hâle getirmiştir. Veri akışları, siber uzam, bulut altyapıları ve ağ mimarileri, egemenliğin mekânsal temelini yeniden düşünmeyi gerektirmektedir. Tez bu nedenle yalnızca egemenlik ve insan unsurunu değil, modern devletin üçüncü klasik ayağı olan ülke unsurunu da dijital çağ bakımından yeniden değerlendirmektedir.

Nihayet tez, "Egemenlik 2.0" başlığı altında egemenliğin dijital yüzünü, dijital egemen figürünü ve meşruiyet krizini tartışmaktadır. Dijital egemenin çok katmanlı formu, Leviathan 2.0, veri-tanrı ve dijital teoloji gibi kavramsallaştırmalar, yalnızca metaforik değil, çağdaş siyasal düzenin yeni meşruiyet problemlerini görünür kılan analitik araçlar olarak kullanılmaktadır. Buradan sonra, dijitalleşmenin egemenlik üzerindeki aşındırıcı etkileri devletin; hukuk, yasa ve zor tekeli, bilgi üzerindeki egemenliği, koruyucu kapasitesi, vergilendirme gücü, parasal egemenliği ve temel hak ve özgürlükleri koruma yükümlülüğü bakımından ayrıntılı olarak incelenmektedir. Böylece tezin asıl iddiası, yani dijitalleşmenin egemenliği aşındıran niteliği, devletin kurucu unsurları ve temel hak rejimi üzerinden test edilmektedir.

Bu çalışma, genel bir iktidar teorisi sunma iddiasında değildir. Bunun yerine, dijitalleşmenin egemenlik üzerindeki etkilerini kavramsal, tarihsel, karşılaştırmalı ve normatif bir düzlemde tartışarak çağdaş siyasal düzende yaşanan dijital dönüşümün bir haritasını çıkarmayı amaçlamaktadır. Bu çabanın sınırlılıkları olduğu açıktır. Dijitalleşme son derece hızlı, çok katmanlı ve disiplinler arası bir alandır; dolayısıyla bu alana ilişkin hiçbir tez son söz olma iddiasında bulunamaz. Bununla birlikte; özgürlük, demokrasi, insan onuru ve kamusal meşruiyet bakımından dijitalleşmenin doğurduğu sorunların ertelenemez olduğu da açıktır. Bu nedenle bu tez, dijitalleşmenin egemenlik üzerindeki aşındırıcı etkilerini görünür kılarak, devletin dijital çağda neden hâlâ vazgeçilmez; ancak artık eskisi gibi klasik kavramlarla yetinilerek düşünülemeyecek bir kurum olduğunu ortaya koymayı amaçlamaktadır.

BİRİNCİ BÖLÜM

DİJİTALLEŞME: KAVRAMSAL ÇERÇEVE, ETKİLERİ VE AKTÖRLERİ

I. KAVRAMSAL ÇERÇEVE

Dijitalleşmenin doğasını, kapsamını ve egemenlik üzerindeki etkilerini açıklayabilmek için öncelikle dijitalleşme ile bir küme halinde dolaşan temel kavramların (dijital, internet, bilişim, algoritma, yapay zekâ ve siber alan) açıklığa kavuşturulması ve aralarındaki ilişkinin ortaya konulması gerekir. Her kavram tanımı aynı zamanda bir sınırlandırmadır. Postmodern çağın kavramları akışkan nitelik taşır; tanımlandıkça anlamlarının bir bölümü dışarıda kalır. Bu nedenle söz konusu kavramları sabit kategoriler olarak değil, tarihsel bağlam içinde şekillenen ve sürekli genişleyen bir kavramsal kümenin parçaları olarak ele almak daha anlamlıdır[1].

Tezin merkezindeki "dijital" (İngilizce *digital;* Fransızca *numérique*[2]) kavramı, *digit*[3] isim kökünden gelen; sayı ile ilgili sanal ve sayısal anlamına gelen bir sözcüktür[4]. Tarihsel kökeni Orta Çağ'ın sonlarına kadar (15. yy) uzanmakta olup ayrık birimler

---

[1] Arif Dirlik, **Küresel Modernite: Küresel Kapitalizm Çağında Modernite,** Ahmet Fethi Yıldırım (çev.), 1. Basım, İstanbul: Akademim Yayınları, 2024, s.15-16.

[2] Byung-Chul Han, **Enfokrasi: Dijitalleşme ve Demokrasinin Krizi,** Mustafa Özdemir (çev.), İstanbul: Ketebe, 2022, s.56.

[3] Digit, İngilizce kökenli bir isim olup iki anlamı bulunmaktadır. Bunlardan birincisi ve yaygın kullanımı, ***"0'dan 9'a kadarki herhangi bir Arap rakamı"*** anlamına gelmektedir. İkincisi ***"başparmak, el veya ayak parmağı"*** anlamına gelmektedir. Latince'de sayı saymak için parmaklar kullanıldığından aslında parmak anlamına gelen digit kelimesi sayı ve saymak kelimelerine de kaynaklık ettiği anlaşılmaktadır. Bkz.: **Dictionary.com,** "Digit"; **Oxford Learner's Dictionaries,** "Digit"; **Merriam-Webster Dictionary,** "Digit (Word History)", https://www.dictionary.com/browse/digit; https://www.oxfordlearnersdictionaries.com/definition/english/digit; https://www.merriam-webster.com/dictionary/digit (Erişim Tarihi: 31.01.2026).

[4] TDK ve Dil Derneği'ne göre, dijital kelimesi bir sıfat olarak sanal ve sayısal anlamına gelmektedir. Merriam-Webster'a göre sıfat anlamıyla ***"elektroniğin ilkeleri ve metotlarına göre çalışan veya yapılandırılmış araçların kullanımı ile ilgili olmak veya özellikle ikili sayı dizimleri şeklindeki verilerden oluşan"*** anlamına gelir. Cambridge Dictionary'e göre, ***"sesleri ya da fotoğrafları depolamadan ya da göndermeden önce numaralar formunda işaretlere dönüştüren elektronik sistemlerin kullanılması"***dır. Merriam-Webster'a göre isim anlamıyla ***"bir dijital formatta bir fotoğraf gibi kitle iletişim aracı veya dijital teknoloji tarafından çalıştırılabilen veya nitelendirilebilen bir aygıt gibi herhangi bir şey"*** demektir. Bkz.: **Türk Dil Kurumu, Güncel Türkçe Sözlük,** "Dijital", https://sozluk.gov.tr; Dil Derneği Türkçe Sözlük, "Dijital", http://www.dildernegi.org.tr; **Merriam-Webster Dictionary,** "Digital", https://www.merriam-webster.com/dictionary/digital; **Cambridge Dictionary,** "Digital", https://dictionary.cambridge.org/tr/sözlük/ingilizce-türkçe/digital (E.T.: 13.12.2024).

üzerinden hesaplama yapma anlamına gelir[5]. Günümüzde dijital nitelik; başta bilgisayar[6] teknolojileri olmak üzere analog olmayan ve arka planında 1 ve 0'dan oluşan ikili sayı sistemine dayalı kodlama bulunan tüm teknolojik sistemleri ifade eder. Dijital olanı çağımızın belirleyici fenomeni hâline getiren ise bu teknik özellikten ziyade dijitalleşme sürecidir.

Dijitalleşme veya TDK'ya göre eş anlamlısı olan sayısallaşma[7] en dar anlamıyla analog verilerin sayısal forma dönüştürülmesi sürecidir[8]. Ancak bu tanım yalnızca teknik dönüşümü açıklar. Dijitalleşmenin asıl önemi, bu teknik dönüşümün toplumsal, ekonomik ve siyasal yapılarda yarattığı köklü değişimde yatar[9]. Dijitalleşme; bilgi

[5] Merriam-Webster'a göre etimolojik açıdan Latince'de parmak anlamına gelen digitus ve ***"bir parmağın genişliğini ölçmek"*** anlamına gelen digitālis kelimeleri ödünç alınarak, Orta Çağ sonu İngilizcesinde rakam anlamına gelen "digitalle" kelimesinden sıfat olarak türetilmiştir. Bkz.: **Merriam-Webster Dictionary,** "Digital (Word History)", https://www.merriam-webster.com/dictionary/digital (E.T.: 13.12.2024).

[6] Bilgisayar; TDK'ya göre belleğine yüklenen program uyarınca aritmetik ve mantık işlemleri yapabilen elektronik aygıt; Cambridge Dictionary'ye göre verileri depolayan ve işleyen elektronik makine; Dictionary.com ve Merriam-Webster'a göre ise programlanabilir veri işleme cihazı olarak tanımlanmaktadır. Tarihteki ilk elektromekanik programlanabilir bilgisayar Z3, 1941'de Konrad Zuse tarafından geliştirilmiş; ilk genel amaçlı dijital bilgisayar ENIAC, 1946'da ABD'de yapılmış; Colossus adlı bilgisayar ise 1943'te Britanya'da şifre çözme amacıyla üretilmiştir. Dijitalleşme açısından bilgisayarın önemi; veri analizi ve bilgiye eş zamanlı erişimi mümkün kılmasıdır. Bkz.: **Türk Dil Kurumu, Güncel Türkçe Sözlük,** "Bilgisayar", https://sozluk.gov.tr (E.T.: 13.12.2024); **Cambridge Dictionary,** "Computer", https://dictionary.cambridge.org (E.T.: 13.12.2024); **Dictionary.com,** "Computer", https://www.dictionary.com (E.T.: 13.12.2024); **Merriam-Webster Dictionary,** "Computer", https://www.merriam-webster.com (E.T.: 13.12.2024); **Encyclopaedia Britannica,** "ENIAC", https://www.britannica.com/technology/ENIAC (E.T.: 13.12.2024); "Colossus Computer", https://www.britannica.com/technology/Colossus-computer (E.T.: 13.12.2024); Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.51; Roger Penrose, **Bilgisayar Ve Zeka: Kralın Yeni Usu, Cilt 1,** Tekin Dereli (çev.), Ankara: Gökçe Ofset, 1997, s. Sunuş.

[7] Türk Dil Kurumu, Güncel Türkçe Sözlük, "Dijitalleşme; sayısallaşma", https://sozluk.gov.tr (E.T.: 13.12.2024).

[8] Kökeni İngilizce'de digitalization (veya digitalisation) kelimelerine dayanan dijitalleşme kavramı, ***"belge gibi bir şeyi bilgisayarlar tarafından saklanabilen ve okunabilen dijital bir forma dönüştürmek"*** anlamına gelen ve bu anlamıyla 1920'lerden itibaren kullanımda olan digitalize (veya digitalise) fiilinden türetilmiş bir isimdir. Bunun dışında, bilgileri genellikle bir bilgisayar tarafından anlaşılabilmesi ve kullanılabilmesi için 0 ve 1 sayılarından oluşan bir dizi biçimine dönüştürmek anlamındaki digitize (veya digitise) fiili de bulunmaktadır. Bkz.: **Cambridge Dictionary,** "Digitalize" https://dictionary.cambridge.org/tr/sözlük/ingilizce/digitalize (E.T.: 13.12.2024); **Cambridge Dictionary,** "Digitize",; https://dictionary.cambridge.org/tr/sözlük/ingilizce/digitize (E.T.: 13.12.2024); **Dictionary.com,** "Digitalize" https://www.dictionary.com/browse/digitalize (E.T.: 13.12.2024).

[9] Kristina Irion, "Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms The (Legal) Relationship Between Individuals And Their Personal Records", **International Journal of Law and Information Technology,** Vol: 23, No: 4, 2015, ss.348-371, s.351.

üretimi, paylaşımı ve denetimi biçimlerini yeniden şekillendirerek bireylerin, kurumların ve devletlerin işleyişine nüfuz eden dönüştürücü bir süreçtir[10].

Bu noktada dijitalleşmeden ayrışan fakat onunla ilişkili olan "dijital dönüşüm" kavramı ortaya çıkar. Dijital dönüşüm, yalnızca verilerin sayısallaştırılmasını değil; kurumların, üretim ilişkilerinin ve toplumsal etkileşim biçimlerinin dijital ortama göre yeniden yapılandırılmasını ifade eder[11]. Dijital çağın başlangıcını tek bir ana indirgemek mümkün değildir; hesaplama tarihinin 17. yüzyıla kadar uzanan algoritmik düşünce geleneği, günümüzdeki dijital evrenin tarihsel arka planını oluşturur[12].

Dijitalleşme sürecini hızlandıran temel unsur *genel ağ*[13] yani internettir[14]. İnternet, dünya çapında ağların birbirine bağlanmasını sağlayan küresel bir iletişim altyapısıdır[15]. Askerî kökenli bir proje olarak ortaya çıkan bu ağ mimarisi, merkezi olmayan yapısı sayesinde kesintilere karşı dayanıklılık hedefiyle tasarlanmıştır[16].

---

[10] Abdurrahman Eren, "Dijital Egemenlik Kavramı ve Anayasa Mahkemesinin Dijital Egemenliğe Yaklaşımı", **Anayasa Yargısı,** Cilt: 42, Sayı: 1, 2025, ss.557-582, s.557.

[11] Fahri Bilal Yankın, "Dijital Dönüşüm Sürecinde Çalışma Yaşamı", **Trakya Üniversitesi İktisadi Ve İdari Bilimler Fakültesi E-Dergi,** Cilt: 7, Sayı: 2, Aralık 2018, s.14-15.

[12] Florian Schneider, dijital çağın tek bir başlangıç anı olmadığını, modern ve modern öncesi teknolojik biçimlerin günümüzde iç içe işlemeye devam ettiğini savunur. Peter F. Drucker ise dijitalleşmenin kökenlerini 19. yüzyılda Babbage ve Lovelace'ın analitik makine çalışmalarına ve daha geride Leibniz'in ikili sayı sistemi ile mekanik hesaplama girişimlerine kadar götürür. Bkz.: Florian A. Schneider, **China's Digital Nationalism,** New York: Oxford University Press, 2018, s.34; Peter F. Drucker, **Kapitalist Ötesi Toplum,** Belkıs Çorakçı (çev.), İstanbul: İnkılap Yayınları, 1994, s.40-41.

[13] Türk Dil Kurumu, Güncel Türkçe Sözlük, "internet", https://sozluk.gov.tr (E.T.: 13.12.2024)

[14] İnternet kelimesi, kendi aralarında bağlantılı ağlar anlamına gelen "interconnected networks" teriminin kısaltmasıdır. Eymen Görgülü, "İnternetin Öyküsü: Geçmişten Günümüze", *Bilişim Dergisi*, https://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/internetin-oykusu-gecmisten-gunumuze.html (E.T.: 13.12.2024).

[15] Cambridge Dictionary, interneti; insanların bilgi paylaşmasına ve iletişim kurmasına olanak tanıyan büyük bir küresel bilgisayar sistemi olarak tanımlar; Merriam-Webster ise dünya çapındaki bilgisayar ağlarını ve kurumsal bilgisayar tesislerini birbirine bağlayan bir elektronik iletişim ağı olduğunu belirtir. Bkz.: **Cambridge Dictionary,** "Internet", https://dictionary.cambridge.org/tr/sözlük/ingilizce/internet (E.T.: 13.12.2024); **Merriam-Webster Dictionary,** "Internet", https://www.merriam-webster.com/dictionary/Internet (E.T.: 13.12.2024).

[16] İnternetin kökeninin askerî amaçlı bir projeye dayanması dikkat çekicidir. 1969'da ABD Savunma Bakanlığı İleri Araştırma Projeleri Kurumu (ARPA/DARPA) tarafından geliştirilen ARPANET, olası bir nükleer saldırı halinde merkezi olmayan iletişim kurabilen bir ağ mimarisi olarak tasarlanmıştır. Castells'e göre bu yapı, merkezsiz ve özerk ağlardan oluşan elektronik bir stratejik modeldi. Varoufakis ise internetin kapitalist düzeni korumak amacıyla, paradoksal biçimde, başlangıçta ticari olmayan ve ortak kullanıma dayalı bir sistem olarak kurulmasını ironik bulur. Bkz.: Andrew L. Shapiro, **The Control Revolution: How The Internet is Putting Individuals in Charge and Changing The World We Know,** New York: PublicAffairs, 1999, s.20; Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.60; Yanis Varoufakis, **Technofeudalism: What Killed Capitalism,** London: The Bodley Head, 2023, s.69.

Zamanla akademik ve sivil kullanıma açılan internet, teknik bir iletişim sistemi olmaktan çıkarak küresel ölçekte bir tekno-sosyal ağ hâline gelmiştir[17]. Web teknolojilerinin gelişmesiyle birlikte internet, sınır aşan bilgi akışını mümkün kılan ve toplumsal ilişkileri dönüştüren bir altyapıya dönüşmüştür.

İnterneti çalıştıran teknik kurallar, donanım ve yazılım standartları tek bir devletin ya da kuruluşun mutlak yetkisinde değildir[18]. 1998'de ABD'de alan adı tahsisi için IANA/ICANN kurulmuş olsa da günümüze kadar dünyada internet üzerinde yetkisi kesin ve tartışmasız bir otorite bulunmamıştır. 2000'li yıllardan sonra Web 2.0 internet teknolojilerinin yarattığı sosyal ağlar, ülkeleri adeta sınırları ortadan kaldırır gibi birbirine bağlamıştır[19]. İnternet sayesinde verilerin paylaşıma sokulması, nesnelerin birbirine bağlanması (Internet of Things[20]), yapay zekâ ve robot teknolojisinin hızla gelişmesi dijitalleşmeyi hızlandırmış ve eşyaları akıllandırmıştır[21]. İnternetin açık yapısı, ağ üzerindeki her uç noktanın diğerleriyle merkezi bir dağıtım sistemi olmaksızın iletişim kurmasını sağlar[22].

Her ne kadar bulut metaforuyla soyutlaştırılsa da internet; somut ve mekânsal bir fiziksel altyapıya dayanır. Veri merkezleri, kablolar ve yönlendiricilerden oluşan bu yapı, belirli coğrafyalarda yoğunlaşmıştır[23]. Ancak interneti yalnızca fiziksel altyapı

---

[17] World Wide Web'in 1991'de CERN'de geliştirilerek kamuya açılmasıyla internet yaygın kullanıma girmiştir. Askerî kökenli ağ sistemi başlangıçta bilimsel paylaşım ve güvenlik iletişimi için kullanılmış; 1990'larda kitlesel iletişim aracına dönüşmüş ve 1993'te ABD hükümetinin kararıyla ticari kullanıma açılmıştır. Bkz.: Peter Ferdinand, "The Internet, Democracy And Democratization", **Democratization,** Vol: 7, No: 1, 2000, s.1. Türkiye 1993 yılında Devlet Planlama Teşkilatı projesi çerçevesinde internete bağlanmıştır.

[18] Duygu Hatipoğlu Aydın, **Siber Alan ve Hukuk**, İstanbul: On İki Levha Yayıncılık, 2022, s.18.

[19] Batu, Mikail, "Sosyal Medya ve Dijital Toplumun Güvenliğine Yönelik Bir Tartışma", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya,** içinde (5-9), Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, Vol.Ocak, Sayı.9, s.5.

[20] ***"İnterneti kullanarak birbirine bağlanabilen ve veri alışverişi yapabilen, içinde bilgi işlem cihazları bulunan nesneler"*** anlamında gelmektedir. **Cambridge Dictionary,** "Internet of Things", https://dictionary.cambridge.org/tr/sözlük/ingilizce/internet-of-things (E.T.: 13.12.2024).

[21] Elif Küzeci, **Sayısal Fil**, 1. Baskı, İstanbul: İnkılap Kitapevi, 2021, s.43.

[22] Alper Işık, **İnternet Aktörleri ve Egemenliğin Değişen Boyutları**, Güncellenmiş 2. Baskı, İstanbul: On İki Levha Yayıncılık, 2025, s.3.

[23] Küresel internet trafiğinin ve veri akışlarının bağlandığı bu fiziksel altyapının büyük çoğunluğu ABD'de bulunmakta ve devlet-özel şirketler el ele yönetilmektedir. ABD'deki veri merkezleri, klasik Orwell 2.0 gözetim anlayışından çok daha kapsamlı, adeta Orwell XXL boyutlarında bir denetim ve kontrol mekanizmasıdır. ABD'nin veri üzerindeki

üzerinden anlamak eksik kalır. Ağın işleyişini belirleyen asıl unsur koddur. Yazılım, protokoller ve ağ tasarımları; bilginin nasıl dolaşacağını ve kimlerin bu akış üzerinde kontrol sahibi olacağını belirler[24]. Bu yönüyle internet, teknik olduğu kadar politik bir mimaridir[25].

Dijitalleşmeyle sıklıkla karıştırılan bilişim kavramı ise bilginin teknolojik araçlarla işlenmesini ifade eden daha dar bir disiplindir[26]. Bilişim; bilgi toplama, işleme ve iletme süreçlerine odaklanırken dijitalleşme, bu süreçlerin toplumsal yapılar üzerindeki dönüştürücü etkisini kapsar[27]. Dijitalleşme; ekonomi, kamu yönetimi, toplumsal yapılar ve hukuk gibi geniş alanlara yayılırken[28] bilişim daha çok bilgisayar bilimi, yazılım, donanım ve iletişim gibi teknik disiplinlerle sınırlı ve çeşitli endüstrilerle ilişkilidir. Bilişim kavramından üretilen bilgi teknolojisi (IT: information technology) kavramı, bilgi ve iletişim teknolojisinin bir araya gelmesini belirtirken[29] bilişim sistemi kavramı, araçsal bir bakış açısıyla bilginin otomatik makinalar aracılığıyla otomatik olarak işlenmesini sağlayan sistemleri[30] ifade eder. Bilgi teknolojileri ve bilişim

---

fiziksel tesis büyüklüğüne ilişkin açıklamalar için ayrıca bkz: Stefan Aust ve Thomas Ammann. **Dijital Diktatörlük.** Erdinç Yücel ve Hasan Yılmaz (Çev.) Ankara: Hece Yayınları, 2018, s.29-33.

[24] Shapiro, s.14.

[25] İnternet, yalnızca bir iletişim aracı değil; teknik altyapıyla toplumsal etkileşimi birleştiren tekno-sosyal bir ağdır. Ademimerkeziyetçi, bağımsız ve eşitlikçi mimarisi sayesinde önceki iletişim araçlarından ayrılarak demokratik uygulamalara elverişli bir yapı sunar. Cemre Edip Yalçın, **Klasik Kamusal Alandan Sanal Kamusal Alana: Demokrasi ve İnsan Hakları İdeali İçin Normatif Bir Değerlendirme,** İstanbul: On İki Levha Yayıncılık, 2022, s.112-113.

[26] Bilişim kavramı, bilmek fiilinin türevidir. TDK'ya göre, ***"birbirini tanımak; muarefesi olmak"*** anlamındaki bilişmek fiilinden türetilmiş olup ***"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi; enformatik"*** olarak tanımlanmaktadır. Türk Dil Kurumu Güncel Türkçe Sözlük, "Bilişim", https://sozluk.gov.tr (E.T.: 13.12.2024) Bilişim kavramının karşılığı İngilizce'de: computer science, informatics ve information systems; Almanca'da: informatik ve Fransızca'da: informatique kelimeleri olup Türkçe'de enformatik (bilişim) kelimesi bunlardan türetilmiştir. Türkçe'de ilk defa Türkiye Bilişim Derneği'nin kurucularından olan Aydın Köksal tarafından kullanılmıştır. 22 Nisan 1971 tarihinde kurulan Türkiye Bilişim Derneği, bilişim konusunda dünyada kurulan ilk derneklerdendir.

[27] Päivi Parviainen ve Diğerleri, "Tackling the Digitalization Challenge: How to Benefit From Digitalization in Practice", **International Journal of Information Systems and Project Management,** Vol.5, No.1, ss. 63-77, (2017), s.64.

[28] OECD, Going Digital: Shaping Policies, Improving Lives, 2019, https://www.oecd.org/en/publications/going-digital-shaping-policies-improving-lives_9789264312012-en.html (E.T.: 13.12.2024), s.3.

[29] TDK'ya göre, ***"bilginin toplanmasını, işlenmesini ve saklanmasını, herhangi bir yere iletilmesini, herhangi bir yerden bilgiye erişilmesini, elektronik vb. yollarla sağlayan teknolojiler bütünü"*** demektir. Türk Dil Kurumu, Güncel Türkçe Sözlük, "Bilgi teknolojisi", https://sozluk.gov.tr (E.T.: 13.12.2024).

[30] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları,** İstanbul: Adalet, 2008, s.11.

sistemleri, dijitalleşmenin teknik omurgasını oluşturur. Bu alanın etik boyutu (hackerlık[31] veri paylaşımı, lisans rejimleri ve dijital özgürlük tartışmaları) dijital çağın normatif meselelerini gündeme getirir[32].

Algoritma kavramı, dijital evrenin mantıksal çekirdeğini oluşturur. Algoritma[33] belirli bir problemi çözmek için izlenen sonlu ve tanımlı adımlar dizisidir[34]. Alan Turing'in çalışmaları modern algoritma ve bilgisayar biliminin kilometre taşı olmuştur[35]. Evrensel bir dile sahip olan algoritmalar, günlük yaşamdan karmaşık yapay zekâ sistemlerine kadar uzanan geniş bir uygulama alanına sahiptir[36]. Günümüzde özellikle dijital veri analizlerinde kullanılmakta olan algoritmalar yalnızca teknik araçlar değil; ekonomik, sosyal ve siyasal karar alma süreçlerinde belirleyici rol oynayan iktidar teknolojileridir[37].

---

[31] Hacker kelimesinin Türkçe karşılığı bilgisayar korsanıdır. TDK'ya göre bilgisayar korsanı, ***"erişim izni ve yetkisi olmamasına karşın bilgisayar ve çevre birimlere erişerek buralardaki verileri okuma, silme ve değiştirme eylemlerinde bulunan veya bilgisayarın çalışmasını engelleyen kimse"*** olarak tanımlanmaktadır. Türk Dil Kurumu, Güncel Türkçe Sözlük, "hacker", "bilgisayar korsanı", https://sozluk.gov.tr (E.T.: 13.12.2024).

[32] Bilgisayar Etik Enstitüsü (Computer Ethics Institute) tarafından geliştirilen ve bilgisayar kullanım etik ilkelerinin temelini oluşturan 10 ilke bulunmaktadır: Bilgisayar başka insanlara zarar vermek için kullanılamaz. Başka insanların bilgisayar çalışmaları karıştırılamaz. Bilgisayar ortamında başka insanların dosyaları karıştırılamaz. Bilgisayar hırsızlık yapmak için kullanılamaz. Bilgisayar yalan bilgiyi yaymak için kullanılamaz. Bedeli ödenmeyen yazılım kopyalanamaz ve kullanılamaz. Başka insanların bilgisayar kaynakları izin almadan kullanılamaz. Başka insanların entelektüel bilgileri başkasına mal edilemez. Kişi yazdığı programın sosyal hayata etkilerini dikkate almalıdır. Kişi, bilgisayarı, diğer insanları dikkate alarak ve saygı göstererek kullanmalıdır. Computer Ethics Institute, The Ten Commandments of Computer Ethics, 2011, http://cpsr.org/issues/ethics/cei/ (E.T.: 13.12.2024).

[33] Algoritma, bir matematik terimi olup, TDK tarafından ***"Orta Çağ'da ondalık sayı sistemine göre, son zamanlarda ise iyi tanımlanmış kuralların ve işlemlerin adım adım uygulanmasıyla bir sorunun giderilmesi veya sonuca en hızlı biçimde ulaşılması işlemi; Harezmi yolu"*** şeklinde tanımlanmaktadır. Türk Dil Kurumu, Güncel Türkçe Sözlük, "Algoritma" https://sozluk.gov.tr (E.T.: 13.12.2024). Fransızca'da ***"Arap sayılarıyla aritmetik işlem yapma yöntemi"*** anlamına gelen algorithme (Eski Fransızcada algorisme) kelimesi, İslam matematikçisi Harezmi'nin ismine dayanır (الخورزمي). Nişanyan Sözlük, "Algoritma" https://www.nisanyansozluk.com/kelime/algoritma (E.T.: 13.12.2024). Fakat Penrose, algoritmaların el Harezmi'nin kitabından çok önce de M.Ö. 300'lerde Eski Yunan'dan beri bilindiğini ve iki sayının en büyük ortak bölenini (EBOB) bulma yöntemi olarak bilinen Eukleides algoritmasının buna örnek olduğunu belirtir. Penrose, s.35-36.

[34] Fatma Önay Koçoğlu ve Çiğdem Selçukcan Erol, "Algoritma", Nilgün Bozbuğa ve Sevinç Gülseçen (Ed.) **Tıp Bilişimi** içinde (Bölüm 13). İstanbul: İstanbul Üniversitesi Yayınları, 2021, s. 249, 251.

[35] Cem Sefa Sütçü, "Önsöz", **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021, s.vii.

[36] Alper Aytekin ve Diğerleri, "Algoritmaların Hayatımızdaki Yeri ve Önemi", **Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi,** Sayı.5, No.7, ss. 151-162, (2018), s.151, 153.

[37] Osman Gökhan Antalya, "Eşya Olarak Dijital Veriler: Dijital Eşya", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.29, Sayı.2, Özel Sayı, (Aralık 2023), ss. 1208-1222, s.1208.

Dijitalleşme sürecine yeni bir boyut getiren yapay zekâ, bir bilgisayarın, bilgisayar kontrolündeki bir robotun[38] veya programlanabilir bir aygıtın insana benzer işlevleri sergileyebilme yeteneği[39] demektir. Algoritmalarla nasıl davranacağı önceden belirlenen bir yazılım olan yapay zekâ, algoritmik sistemlerin en gelişmiş biçimlerinden biridir[40]. Yapay zekâ; cihaz ve sensörlerin sürekli bağlantılı olduğu ve insan müdahalesi olmaksızın otonom biçimde işleyen sistemlerdir[41]. İnsan zekâsının belirli işlevlerini taklit eden bu sistemler, veri istatistiğine dayalı determinist çıkarımlar[42] yaparak öğrenme ve karar verme kapasitesi gösterir[43]. Üretken yapay zekâ teknolojileriyle birlikte dijital dönüşüm, endüstriyel üretimden ticarete kadar birçok alanda yeni bir aşamaya ulaşmıştır[44]. Bununla birlikte yapay zekâ, insan bilinci ve öznelliğinin yerini alabilecek bir varlık değildir; hesaplama gücü ile insan zihninin niteliksel özellikleri arasında ontolojik bir fark bulunmaktadır[45]. Yapay zekâ çok iyi hesaplama yapabilse de insan aklının melekelerini taşımaz. Bu ayrım, teknolojik ilerlemenin sınırlarına ilişkin felsefi tartışmaları canlı tutmaktadır.

---

[38] Robot, elektronik ve mekanik birimlerden oluşan, algılama yeteneğine sahip olan, otonom veya önceden programlanmış görevleri yerine getirebilen cihazdır. TDK, ***"belirli bir işi yerine getirmek için manyetizma ile kendisine çeşitli işler yaptırılabilen otomatik araç"*** olarak tanımlamıştır. Türk Dil Kurumu, Güncel Türkçe Sözlük, "Robot", https://sozluk.gov.tr (Erişim tarihi: 13.12.2024); İnsanlık tarihinde robotlar uzun zamandır kullanımda olsa da yapay zekâ desteğinin gelmesi robot kullanımında büyük atılım yaşatmıştır. İnsansı robotların ve insan-makine sistemi olan siborgların geliştirilmesinde yükseliş söz konusudur.

[39] Türk Dil Kurumu, Güncel Türkçe Sözlük, https://sozluk.gov.tr. (E.T.: 13.12.2024).

[40] Alan Turing'in 1950 yılında yayınlanan "Computing Machinery and Intelligence" makalesine dayanan Turing testi, bir zekanın doğal ya da yapay olup olmadığını belirlemek için kullanılmaktadır. Turing testi, bir varlığın insan davranışlarını ne ölçüde taklit edebildiğini ölçmeye yarar; testi geçmek, yapay zekânın bilinçli olduğunu değil, insan gibi davranabildiğini gösterir. Penrose, s.5.

[41] Mehmet Akçaal, "Profilleme Kavramının Kişilik Hakkı ve Kişisel Verilerin Korunması Bağlamında Değerlendirilmesi", Şerafettin Ekici ve Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (487-500), İstanbul: Adalet, 2021, s.490.

[42] George Dyson, **Turing's Cathedral: The Origins of the Digital Universe**, New York: Pantheon, 2013, s.310.

[43] **Cambridge Dictionary,** "Artificial intelligence", https://dictionary.cambridge.org/tr/sözlük/ingilizce/artificial-intelligence (E.T.: 13.12.2024). Yapay zekâ, ***"özellikle akıllı bilgisayar programları olmak üzere akıllı makineler yapmanın bilimi ve mühendisliği"***dir. bkz. John McCarthy, "What Is Artificial Intelligence?", Stanford University Computer Science Department, 2007, https://www-formal.stanford.edu/jmc/whatisai.pdf, s. 2 (E.T.: 14.12.2024).

[44] Fatih Kaplanhan, "Dijitalleşme, Vergi ve Egemenlik Sorunu", **Bilişim Teknolojileri ve İletişim: Birey ve Toplum Güvenliği,** (2020), s.173.

[45] Elif Karakoç, "Algoritmalardaki Cinsiyet Yanlılığına Queer Teori Perspektifinden Bakmak", **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021, s.21.

Dijitalleşmenin bütün bu bileşenleri nihayetinde siber alan (cyberspace) kavramında birleşir[46]. Siber alan, bilgisayar ağları üzerinden kurulan iletişimden doğan küresel sanal ortamı ifade eder[47]. Sınırsız görünmesine rağmen fiziksel altyapıya dayanır ve bu altyapı ulus-devletlerin egemenlik alanları içinde yer alır[48]. Kavramın etimolojik kökleri kontrol ve yönlendirme fikrine dayanır. Bu nedenle siber alan yalnızca bir iletişim ortamı değil; kontrol, yönetim ve özerklik ilişkilerinin yeniden tanımlandığı bir mekândır[49]. Birey burada pasif bir alıcı değil, dijital akışın etkin bir öznesidir[50]. Böylece siber alan, dijital çağda egemenlik, özgürlük ve iktidar tartışmalarının merkezî sahnesi hâline gelmektedir.

II. HİBRİT BİR TANIMLAMA: DİJİTAL EGEMENLİK

Hukuk ve siyaset bilimi alanında yaşanan veri odaklı dijital dönüşümün nasıl anlamlandırılacağı, dijital egemenlik kavramının nasıl tanımlandığıyla doğrudan ilişkilidir. Dijital egemenlik, dijitalleşmenin yarattığı postmodern krizde ortaya çıkan, henüz yerleşik bir anlam birliğine kavuşmamış kavramlardan biridir. Tanımlanmaya

---

[46] Sanal veya siber alem/uzay/ortam gibi kavramlarla da ifade edilmekle birlikte en yaygın kullanımı siber alan kavramıdır.

[47] Siber Güvenlik Kanunu'ndaki tanıma göre siber alan, ***"doğrudan ya da dolaylı olarak internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan tüm bilişim sistemlerini ve bunları birbirine bağlayan ağlardan oluşan ortamı"*** ifade etmektedir; bkz. Siber Güvenlik Kanunu, m. 3/1(i), https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm. Britannica'ya göre ise siber alan, ***"bilgisayarlar, internet özellikli cihazlar, sunucular, yönlendiriciler ve internet altyapısının diğer bileşenleri arasındaki bağlantıların oluşturduğu şekilsiz, sanal dünya"*** anlamına gelmektedir; bkz. Britannica, "Cyberspace", https://www.britannica.com/topic/cyberspace, (E.T. 30.01.2026).

[48] Hatice Kübra Ecemiş Yılmaz, "Siber Uzay, Siber Güvenlik, Dijital Egemenlik Kavramlarının Uluslararası Hukuk Bağlamında Değerlendirilmesi", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya,** içinde (21-26), Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, Vol.Ocak, Sayı.9, s.24.

[49] İnternetten de web'den de farklı anlamı olan siber alan (cyberspace) kelimesi, ilk kez 1982'de bilim kurgu yazarı William Gibson tarafından kullanılmıştır. "Serdümen, vali, pilot veya dümen" anlamlarına gelen Eski Yunanca "kybernetes" kelimesinden ve kontrol ve iletişim teorisi bilimi olan siber bilimden (cybernetics) türetilmiştir. Hatipoğlu Aydın, s.26; Shapiro, s.32. Yönetim ve hükümet kavramlarının kökeni olan Latince "gubernaculum" (dümen/kumanda merkezi), siyasal otoritenin özündeki yön verme ve sevk etme (government) işlevini simgeleyen güçlü bir etimolojik bağ sunar. Rukiye Akkaya, "Devleti Öğretme Biçimi Olarak Siyaset Bilimi ve Fransa'daki Kökleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.26, Sayı.1, (Haziran 2020), ss. 1-12, s.11.

[50] Siberbilim, geçmiş davranışlar ve veriler üzerinden geleceğin öngörülebileceği varsayımına dayanır; bkz. Aust ve Amman, s.40. Shapiro'ya göre siber alan, kontrol ve iletişim sistemlerini inceleyen siberbilimden türeyen ve bireysel kontrolü merkeze alan bir "kontrol devrimi"nin kavramsal ifadesidir; bkz. Shapiro, s.32.

direnç göstermesi, uygulamada yeknesaklık bulunmaması ve ampirik gerçekliğin kavramsal çerçeveye sığdırılmasındaki zorluklar, kavramı ikircikli hâle getirmektedir. Bununla birlikte dijital egemenliği açıklayabilmenin en tutarlı yolu, klasik egemenlik kuramından hareket etmektir.

Egemenlik; siyasi-hukuki temel metinlerin ve modern dönem siyaset felsefecilerinin ana kavramı olarak yalnızca tanımlama çeşitliliği bakımından özel bir incelemeyi hak eder[51]. Ancak çalışmanın temas ettiği kavramlarımızdan biri olarak üzerinde hemen hemen uzlaşı sağlanmış bir hukuki tanımdan hareket etmek zorunluluğu vardır. Çünkü hukuki zemine oturtulmuş egemenlik kavramı, modern devlet düşüncesini şekillendiren temel ölçüttür.

Egemenlik, modern siyaset teorisinin kurucu kavramıdır. Devletin kurucu varlık koşulu ve meşruiyet zemini olarak işlev görür[52]. Modern ulus-devlet düşüncesinde egemenlik, siyasal iktidarın en üstün ve kapsayıcı niteliğini ifade eder ve onu önceki toplum düzenlerindeki iktidar biçimlerinden ayırır[53]. Devlet ile egemenlik arasında kurucu bir bağ vardır: egemenliğin olmadığı yerde devletten söz edilemez[54]. Bu nedenle egemenlik yalnızca bir hukuki terim değil, devlet iktidarının ontolojik temelidir[55]. Devlet, egemenlik sayesinde varlık nedenini ve amacını kendi içinde temellendirebilen bir siyasal iktidar tipidir[56].

---

[51] Egemenlik ya da hâkimiyet, TDK'ya göre **"*egemen olma durumu ya da milletin ve onun tüzel kişiliği olan devletin yetkilerinin hepsi; buyruk, hüküm, hükümranlık*"** anlamına gelmektedir. Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr. (13.12.2024).

[52] Rukiye Akkaya Kia, **Moderniteden Postmoderniteye Egemenlik ve Hukuk,** İstanbul: Beta, 2006, s.15.

[53] Oktay Uygun, **Devlet Teorisi,** Gözden Geçirilmiş 8. Baskı, İstanbul: On İki Levha Yayıncılık, 2021, s. 11.

[54] Mehmet Ali Ağaoğulları, **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler,** İstanbul: İletişim, 2019, s.407.

[55] Bununla birlikte bütün kültürler, meslekler ve bilim disiplinleri için geçerli olabilecek tek bir egemenlik tanımını önermek mümkün değildir. Egemenlik; gazeteciler, politikacılar, uluslararası örgütler ve hukukçular açısından aynı anlamda aynı içerikle kullanılmamaktadır. Kavram hem farklı kültürlerde yaşayan insanlar için hem de farklı dönemlerde aynı toplumda yaşayanlar için farklı anlamlara gelmekteyken bilim alanları ve diğer ilgili alanlarındaki kullanımı da farklılaşabilmektedir. Nagan ve Hammer; egemenlik kavramı üzerine hukuk ve siyaset düşüncesi kapsamında yapılan tanımlardan çıkanları şu şekilde listeler: kişileşmiş monark; en üst, sınırsız kontrol veya güç; politik meşruiyet; siyasi otorite; ulusal bağımsızlık; yönetim gücü ve anayasal düzen; uygulanan hukuk kurallarının en üst meşruluk dayanağı; devletlerarası egemen eşitliğin hukuki tüzel kişiliği; uluslararası tanınma; yasal dokunulmazlık; hukuku yapmada ve uygulamada yargısal yetki; yürütme yetkisi olarak egemenlik. Winston P. Nagan ve Craig Hammer, "The Changing Character of Sovereignty in International Law and International Relations", **Columbia Journal of Transnational Law**, Vol.39, (2004), s.141-143.

[56] Akal, *Devlet, Yasa, Hakimiyet*, s.26.

Kamu hukuku, merkezine devleti alan bir hukuk dalıdır[57]. Kamu hukuku disiplininde egemenlik, bir mekân üzerinde meşru kural koyma gücü ve hukuk yaratma kudreti olarak tanımlanabilir[58]. Toplum içindeki güç düzenlemeleriyle, özellikle de vatandaşlar ile devlet arasındaki ilişkiyle ilgilidir[59]. Bu zeminde hukuk, egemen tarafından yaratılır ve uygulanır. Modern devletin kuramsal meşruiyet kalıbı olan egemenlik, köken olarak Latince'de "en üstte, diğerlerinin üstünde" anlamına gelen "*superanus*" sözcüğünden gelir[60]. Egemenlik modern siyaset teorisinin bir kavramı olduğundan Antik Yunan'da bu kavrama rastlanmaz[61]. Tarihî süreçte, Batı Avrupa'da farklı aktörler arasında yüzyıllar boyu cereyan eden güç mücadelesinin sonucunda olgunlaşarak ortaya çıkmıştır[62].

Egemenlik kuramının klasik formülasyonu Jean Bodin'e kadar uzanır. Devlet iktidarını egemenlik kavramıyla nitelendiren ilk düşünür[63] olan Bodin egemenliği, yurttaşlar üzerinde en yüksek, mutlak ve sürekli güç olarak[64] tanımlamış; tek ve bölünemez bir iktidar olarak kuramsallaştırmıştır. Mutlak monarşiyi dinsel temellere dayandıran ve dinsel kurallarla sınırlandıran kralların tanrısal hakları kuramına karşılık, mutlak monarşiye dinsel olmayan, laik bir kuram armağan etmiş, mutlak monarşinin egemenlik kavramını formülleştirirken hukuki düşünüşü siyaset kuramına sokmuştur[65]. Egemenliğin nişaneleri; örf-adet ve geleneklerden sınırlanmadan yasa yapmak; başka hiç

---

[57] Ali Fuad Başgil, "Devlet Nedir?: Realist Bir Tarif Denemesi", **İstanbul Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.12, Sayı.4, ss. 981-990, (2011), s.982.

[58] Kaplanhan, *"Dijitalleşme, Vergi ve Egemenlik Sorunu",* s.177.

[59] Paul Timmers, "Sovereignty in the Digital Age", Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem, Allison Stanger (Ed.) **Intrduction to Digital Humanism** içinde (571-592), Springer, 2023, s. 572.

[60] Ozan Erözden, **Ulus-Devlet,** 3. Basım, İstanbul: On İki Levha Yayıncılık, 2013, s.173; Kavramın Fransızcadaki karşılığı "souveraineté" kelimesi de kökünü "superanus" sözcüğünden alır. Münci Kapani, **Politika Bilimine Giriş,** 59. Baskı, Ankara: Serbest Akademi, 2020, s. 66.

[61] Mehmet Akad ve Diğerleri, **Küreselleşme ve Türkiye (Türkiye'de Devletin Gelişimi),** ed. Cevat Okutan, Ankara: Seçkin Yayıncılık, 2007. s.48.

[62] Kapani'ye göre, "***Fransa krallarınca ülke içinde kendi iktidarlarına rakip olabilecek bir iktidar, ülke dışında da kendilerinden üstün bir kudret tanımadıklarını ifade eden bir hukuki formül olarak kullanılmıştır***". Kapani, s.65.

[63] Uygun, s.207.

[64] Mehmet Akad, Bihterin Dinçkol ve Nihat Bulut, **Genel Kamu Hukuku,** Gözden Geçirilmiş 16. Basım, İstanbul: Der Yayınları, 2020, s.102; Uygun, s.210. Mehmet Ali Ağaoğulları ve Levent Köker, **Kral-Devlet ya da Ölümlü Tanrı,** 5. Baskı, Ankara: İmge Kitabevi, 2018, s.27.

[65] Akad, Dinçkol ve Bulut, s.126; Şenel, s.311.

kimsenin onayı olmadan genel ve özel olarak herkese yönelik kanun koymaktır[66]. Kanun koyma ve ilga etme erki; savaş ilan etme ve barış yapma, herhangi bir yargıcın kararlarına ilişkin itirazlara nihai karar verme, yüksek makam sahiplerini atama ve görevden alma, tebaaları vergi ve harç salma veya bunlardan muaf tutma, af çıkarma, paranın değerini ve ölçüsünü belirleme gibi egemenliğin diğer tüm haklarını ve ayrıcalıklarını içerir[67]. Egemenlik, eylemleri bir başkasının denetimine bağlı olmayan, yaptıkları bir başkasının iradesiyle geçersiz kılınamayan bir güçtür[68].

Bodin'in ardından Hobbes, Spinoza ve Locke'un toplum sözleşmesi teorileri egemenliği farklı yönlerden temellendirmiştir[69]. Hobbes egemenliği güvenlik karşılığında mutlak otorite olarak ve Tanrısal özellikler atfederek savunurken[70] Spinoza özgürlük, akıl ve ifade özgürlüğü temelinde daha rasyonel bir siyasal düzen tasavvur etmiştir[71]. Her iki düşünür de doğa durumu ve egemenlik üzerinden siyasal toplumun temellerini tartışır, ancak Hobbes otoriteye bağlı, Spinoza ise bireysel varoluş ve dokunulmaz haklara dayalı bir siyaset anlayışı geliştirir[72]. Locke ise egemenliği, bireyin devredilemez doğal haklarıyla (yaşam, özgürlük, mülkiyet) sınırlayarak modern anayasal devletin normatif temelini atmıştır[73]. Locke'u takip eden 18. yüzyılda egemenlik erkleri, Fransız politik düşünür Montesquieu'nün yeniden formalize ettiği kuvvetler ayrılığı ilkesi ile birbirinden çözülmüştür. Aynı dönemde bir diğer ünlü filozof Jean-Jacques Rousseau

---

[66] İlhan Akın, **Kamu Hukuku,** İstanbul: Beta, 1993, s.95; Ayferi Göze, **Siyasal Düşünceler ve Yönetimler,** Tıpkı 18. Bası, İstanbul: Beta, 2020, s.142; İlhan Akın, **Devlet Doktrinleri,** 3. Tıpkı Basım, İstanbul: Beta, 2016 s. 83.

[67] Göze, s.142.Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.29;

[68] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.101.

[69] 16. yüzyıldan itibaren egemenlik kuramı, Hobbes ve Spinoza ile toplumsal sözleşmeye dayalı dünyevi bir temele oturmuş, Locke ile doğal haklar yoluyla sınırlandırılmıştır. Hobbes, Leviathan'da düzeni sağlamak için egemenliği sınırsız ve bölünemez kılmış; böylece egemenliğin kaynağını Tanrı'dan alıp insan iradesiyle kurulan devlete taşıyarak teolojik meşruiyetten hukuk felsefesine geçişi temsil etmiştir.

[70] Orta Çağ'da Kilise ile krallar arasındaki üstünlük tartışması, Hobbes'un egemenliği akla ve doğal yasalara dayalı bir toplumsal düzen olarak temellendirmesiyle aşılmış; bu yaklaşım 17. yüzyılda mutlak monarşileri meşrulaştırarak dünyevi iktidarın (bedenin) yalnızca ruha değil her şeye üstünlüğünü savunmuştur. Rukiye Akkaya, **Küreselleşme Olgusu Karşısında Ulus Sorunu,** İstanbul: Legal Yayıncılık, 2004, s.54.

[71] Mehmet Ali Ağaoğulları, Filiz Zabcı ve Reyda Ergün, **Kral-Devletten Ulus-Devlete,** 3. Baskı, Ankara: İmge Kitabevi, 2017, s.55-59. Spinoza'ya göre devletin amacı itaat sağlamak değil, bireylerin özgürce akıl yürütebildiği bir düzen kurmaktır; bireyler doğaları gereği sahip oldukları ve güçleriyle sınırlı olan haklarından vazgeçemezler. Uygun, s.224-225.

[72] Blandine Kriegel, **Klasik Siyasi Felsefe Metinleri,** Zühre İlkgelen (çev.), İstanbul: İletişim Yayınları, 2010, s. 40-45, 71.

[73] Akad, Dinçkol ve Bulut, s.134.

tarafından egemenliğin kökeni genel iradeye dayandırılarak modern ulus-devlet öğretisi haline getirilmiştir[74]. Fakat kısa süre içinde genel irade söylemi; anayasa ve temel haklarla çizilen sınırları aşan bir "sınırsız çoğunluk" iddiasına dönüşmüş; genel-soyut yasa biçimi altında dahi belirli kişi ve gruplar lehine/aleyhine sonuçlar üretmeye elverişli hale gelmiştir. Bu nedenle çağdaş liberal-çoğulcu demokrasiler, egemenliği "kayıtsız-şartsız milli irade"ye değil; hukuk devleti, insan hakları, anayasanın üstünlüğü, yargısal denetim ve uluslararası yükümlülükler gibi kurumsal güvencelere dayalı olarak sınırlandırmaktadır[75].

Rousseau'ya kadar gelen süreçte egemenlik sekülerleşmeye devam eder; ancak teolojik iz tamamen silinmez, biçim değiştirir. Modern devlet, Tanrı'nın otoritesinin boşalttığı yeri dolduran, düzen ve güvenlik ihtiyacının dünyevi karşılığı olmuştur. Carl Schmitt'e göre, modern devlet teorisinin egemenlik, yasa, kader, bağışlama gibi tüm temel kavramları aslında sekülerleştirilmiş teolojik kavramlardır. Tanrı'nın adı silinmiş, ama kavramsal yapısı devletin içinde yaşamaya devam etmiştir[76]. Dolayısıyla süreç içerisinde meşruiyetin temelinde ilahi iradenin olduğu düşüncesi terk edilmiş, yerini insan aklı ve bireysel haklar almıştır. Devletin ayırt edici niteliği, bütünüyle modern ve bir soyutlama olan egemenlik kavramı sayesinde yasa ile uygulama arasındaki siyasal ilişkinin tamamen dünyevi bir zeminde kurulmasıdır. Böylece egemenlik, kamu hukukunun bilimsel bir disiplin haline gelmesine yardımcı olmuştur.

Bodin'in klasik egemenlik kuramında egemenlik, tanrısal ya da metafizik bir kaynağa dayanan, mutlak ve tekil bir iktidar olarak "yukarıdan" gelirken; modern egemenlik kuramında egemenlik, toplum sözleşmesi yoluyla halkın rızasından doğan, hukuk ve bireysel haklarla sınırlı, temsili ve anayasal bir iktidar olarak "aşağıdan" ortaya çıkar. Bu durum, tarihsel seyirle birlikte okunduğunda, egemenliğin statik değil, toplumsal koşullara uyum sağlayan dinamik bir kavram olduğunu gösterir.

---

[74] Rousseau'da genel irade, bireysel çıkarları aşan ve siyasal birliği kuran üstün ortak iradedir; ona uymak özgürlüğün kaybı değil, bireyin egemenliğin parçası hâline gelmesidir. Politik bedene itaat, sözleşmeden doğan bir borçtan ziyade ahlaki bir yükümlülüktür. Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.60.

[75] Arda Atakan, "Putlaştırılmış Bir Kavram: Milli İrade", **Marmara Üniversitesi Hukuk Fakültesi Mehmet AKAD'a Armağan** içinde (143-276), İstanbul: Der Yayınları, 2012, s.273-276.

[76] Carl Schmitt, **Political Theology, Four Chapters on the Concept of Sovereignty,** George Schwab (çev.), Chicago: University of Chicago Press, 2005, s.36.

Küreselleşmenin ulus-devlet egemenliği üzerinde yarattığı aşınmanın ardından veri odaklı dijital teknolojiler egemenlik kuramını bir kez daha tartışmaya açmıştır. Bu cendere içerisinde bilimsel açıdan çok yönlü ve karmaşık niteliğe sahip olan, kabul edilmiş tek bir tanımı olmayan ve internetin yol açtığı yeni gelişmeleri karşıladığı düşünülen dijital egemenlik ve dijital anayasacılık gibi kavramlar, klasik egemenliğin dijital çağdaki görünümünü açıklama çabasının ürünüdür.

Dijital egemenlik kavramı ilk kez 2008'de Pierre Bellanger tarafından ortaya atılmış ve daha sonra farklı düşünsel geleneklerde genişletilmiştir[77]. Kavram kısa sürede teknolojik egemenlik, veri egemenliği, siber egemenlik ve ağ egemenliği gibi alt kavramları içeren bir şemsiye terime dönüşmüştür[78]. Bu çoğullaşma, kavramın teorik olgunluğa henüz ulaşmadığını göstermektedir. Literatürde dijital egemenliği tanımlama girişimleri sistematik olarak dört yaklaşım altında toplanabilir.

- **Devlet merkezli tanımlar:** Devlet merkezli tanımlarda dijital egemenlik, modern egemenliğin dijital ortama taşınmasıdır. Bu anlayışa göre devlet, dijital alan üzerinde kural koyma, uygulama ve yaptırım gücüne sahip olmalıdır. Dijital altyapılar, veri akışları ve platform ekonomisi üzerinde düzenleyici otorite kurma kapasitesi bu yaklaşımın temelidir. Çin'in siber egemenlik doktrini bu modelin en belirgin örneklerinden biridir.

Bu çerçevede dijital egemenlik; devletin büyük teknoloji şirketlerine bağımlılığını azaltma, kendi teknolojik kapasitesini geliştirme ve dijital kamusal alan üzerindeki kontrolünü sürdürme mücadelesi olarak görülür[79]. Kavram hem normatif (hukuki-siyasal yetki) hem de kapasite (teknik ve yönetsel imkânlar) boyutlarına

---

[77] Eren, s.558. Örneğin dijital alanların kendine özgü bir egemenlik sahası olduğu bağlamını yansıtacak şekilde 1990'larda "cyber sovereignty" veya "network sovereignty" şeklinde kullanılmış olduğu bilinmektedir.

[78] Johannes Thumfart, "The Norm Development of Digital Sovereignty Between China, Russia, the EU and the US: From the Late 1990s to the Covid-Crisis 2020/21 as Catalytic Event", Dara Hallinan, Paul de Hert ve Ronald Leenes (Ed.), **Data Protection and Privacy: Enforcing Rights in a Changing World** içinde (1-44), Oxford: Hart Publishing, 2021, s. 3.

[79] Theodore Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", *SSRN,* 2020, https://ssrn.com/abstract=3748098 (14 Aralık 2024), s.17.

sahiptir[80]. Devletin dijital egemenliği; veri yönetimi, altyapı kontrolü, siber güvenlik ve düzenleyici otorite alanlarında somutlaşır[81].

Eren'e göre dijital egemenlik, uluslararası büyük dijital platformlara karşı devletlerin kendi dijital kamusal alanları üzerindeki hâkimiyet kurma çabasıdır[82]. Işık'a göre, büyük teknoloji şirketlerinin devlet ile yurttaş arasındaki güç dengesini bozmasına karşı devletin yeniden düzenleyici kapasitesini tesis etme mücadelesidir[83]. Bu mücadele, devletlerin özgürlükçü ya da müdahaleci politikalarına göre farklı biçimlerde görülse de ortak payda devletin egemenliğini siber uzaya taşımasıdır.

Creemers, dijital egemenlik kavramının, devletin siber uzayda nasıl hareket edeceğini belirleyen hukukî-siyasî ilkeler ve bu ilkeleri uygulamaya imkân veren teknik yönetim süreçleri şeklinde iki boyuttan oluştuğunu tespit eder[84]. Bu mimari üzerinde dijital egemenlik, devletin; dijital alanlarda erişim, bilgi, iletişim, ağ ve altyapı üzerindeki kontrolünü[85] veri akışlarını merkezî biçimde yönetme çabasını[86] ve dijital alanda hukukî ve siyasî otorite kurma kapasitesini[87] içerir.

Kapasite bileşeni açısından kavram; veri, yapay zekâ, 5G, protokoller, bulut bilişim, dijital hizmetler, donanımlar, altyapılar gibi bütün dijital süreçlerin kontrolünü kapsar[88]. Normatif bileşen yani hukuki ve siyasi açıdan dijital egemenlik, modern

---

[80] Muhammad Jawad Hadi, "Digital Battlegrounds: Data Sovereignty and Regulatory Challenges in Armed Conflicts", *SSRN,* 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4608863 (14 Aralık 2024), s.3.

[81] Bedir Sala, "Dijital Çağda Devlet Egemenliğini Tartışmak: Dijital Feodalizm", **SDE Akademi Dergisi,** Cilt.5, Sayı.3, ss.373-399, s.391.

[82] Eren, s.559.

[83] Işık, s.25.

[84] Rogier J.E.H. Creemers, "China's Conception of Cyber Sovereignty: Rhetoric and Realization", Dennis Broeders ve Bibi van den Berg (Ed.), **Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics** içinde (107-142), Lanham: Rowman & Littlefield. 2020, s.109.

[85] Stephane Couture ve Sophie Toupin, "What Does the Notion of "Sovereignty" Mean When Referring to the Digital?", **New Media & Society,** Vol.21, No.10, (2019), s.2305.

[86] Nil Dikmengil, "Siber-Ulus: Dijital Egemenlik Alanı ve Barbados'un Metaverse Elçiliği", Aslı Şen Taşbaşı, Bahadır Er, Erol Ülker ve Özlem Kayhan Pusane (ed.), **Dünyada Birey, Toplum, Siyaset Kongresi Bildiri Kitabı** içinde (170-182), İstanbul: Işık Üniversitesi Yayınları, 2022, s.175.

[87] Huw Roberts ve Diğerleri, "Safeguarding European Values with Digital Sovereignty: an Analysis of Statements and Policies", **Internet Policy Review,** Vol.10, No.3, (2021), s.2.

[88] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU", **Philosophy & Technology,** Vol.33, No.3, (2020), s.371.

egemenlik teorisine dayanarak, düzenleyici otorite olarak devletin dijital alandaki meşru kural koyma gücünü ifade eder.

Kavramın uygulama ve meşruiyet alanı; büyük teknoloji şirketlerinin faaliyetlerini düzenlemek, dijital alanda kamu gücünü tesis etmek, uymayanlara yaptırım uygulamak[89] dijital bağımlılıklardan arınarak kendi ekonomik, politik ve toplumsal önceliklerini hayata geçirme biçimlerinde somutlaşır[90].

Kavramın amacı ve işlevi, devletin; dijital alanda ulusal çıkarlarını korumasını[91] dijital sömürüyü önlemesini[92] kendi vatandaşlarını ve işletmelerini dijital risklerden korumasını hedefler[93]. Dijital teknoloji şirketlerinin sahip olduğu patentler ve teknik altyapılar, ulus-devletlerin bu alan üzerindeki kontrolünü sınırlandırdığından devletler için temel sorun, teknoloji bağımlılığı ve egemenlik aşınmasıdır[94]. Birçok devlet, dijitalleşmede teknoloji üretmek yerine ithal eden konumdadır. Bu durum, veri kontrolünün zayıflaması, kişisel verilerin ve özel hayatın korunamaması, fikri mülkiyet, vergi ve ulusal egemenliğin aşınması ve devletlerin dijital sömürge haline gelme risklerini doğurmuştur[95].

Devlet merkezli dijital egemenlik tanımları içinde normatiflik odaklı yaklaşım, kavramı küresel dijital düzenin normatif mimarisi bağlamında ele alır. Bu perspektifte egemenlik; teknik kontrolün ötesinde, uluslararası standartları belirleyebilme, internet yönetişimine yön verebilme ve dijital alandaki kuralları şekillendirebilme kapasitesi olarak anlaşılır. Avrupa Birliği'nin stratejik dijital özerklik söylemi ile ABD'nin açık internet ve çok paydaşlı yönetişim vurgusu bu yaklaşımın başlıca örnekleridir. Bu bağlamda, özellikle AB açısından dijital egemenlik, ABD-Çin teknoloji rekabeti

---

[89] Ömer Anayurt, **Anayasa Hukuku Genel Kısım**, 5. Baskı, Ankara: Seçkin, 2022, s.272.
[90] Christakis, s.6.
[91] Tomáš Gábriš ve Ondrej Hamuľák, "Pandemics in Cyberspace: Empire in Search of a Sovereign?", **Baltic Journal of Law & Politics,** Vol.14, No.1, (2021), s.26.
[92] M'Bawine Atindande, "Digital Communication in Africa at Crossroads: From Physical Exploitation in the Past to Virtual Dominance Now", Kehbuma Langmia ve Agnes Lucy Lando (Ed.), **Digital Communications at Crossroads in Africa: A Decolonial Approach** içinde (41-70), Palgrave Pivot Cham, 2020, s.57.
[93] Julia Pohle ve Thorsten Thiel, "Digital Sovereignty", **Internet Policy Review**, Vol.9, No.4, (2020), s.2.
[94] David Tipper ve Prashant Krishnamurthy, "Digital Sovereignty and Resilience", *SSRN*, 2022, https://ssrn.com/abstract=4178621 (22 Aralık 2024), s.2-3.
[95] Christakis, s.6-7.

zemininde Avrupa'nın kendi dijital pazarını güçlendirme, kritik teknolojilerde dışa bağımlılığı azaltma ve değerleri doğrultusunda bağımsız tercihler yapabilme kapasitesini ifade eder[96]. Avrupa Komisyonu Başkanı Ursula von der Leyen dijital egemenliği "*kendi kurallarını koyabilme ve seçim yapabilme gücü*" olarak[97] tanımlarken, Avrupa Konseyi Başkanı Charles Michel ise "*bağımlılıkları azaltarak çıkarları ve değerleri savunma yeteneği*"[98] biçiminde yorumlamış ve dijital egemenlik olmadan stratejik özerkliğin sağlanamayacağını vurgulamıştır. Tambiama Madiega ise kavramı, AB'nin dijital alanda hem koruyucu hem iş birliğine açık araçlarla bağımsız hareket edebilme stratejisi olarak değerlendirmektedir[99]. Her ne kadar kavramın sınırları kesinleşmemiş ve AB belgelerinde tutarsız biçimde kullanılsa da dijital egemenlik, birliğin küresel rolünü güçlendiren ve temel değerlerini (insan onuru, özgürlük, demokrasi, eşitlik, hukukun üstünlüğü, insan hakları) koruyan bir dayanak olarak sunulmaktadır[100].

AB literatüründe dijital egemenlik, giderek stratejik özerklik[101] kavramı ile ilişkilendirilmektedir. Stratejik özerklik; kritik dijital alanlarda kapasite, yetenek ve altyapı inşa ederek dış bağımlılıkların karar alma süreçlerini sınırlamasını engelleme amacını taşır[102]. Bu bağlamda kuantum bilişim, yapay zekâ, blok zincir ve yarı iletken

---

[96] European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, 2020, https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf (15 Aralık 2024), s.4.

[97] European Commission, Shaping Europe's Digital Future, 2020, https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260. (15 Aralık 2025).

[98] European Council. Digital Sovereignty is Central to European Strategic Autonomy - Speech by President Charles Michel at 'Masters of digital 2021' online event, 2021 https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/ (15 Aralık 2025).

[99] European Parliamentary Research Service, Digital Sovereignty for Europe, 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (15 Aralık 2024), s. 1.

[100] Roberts ve Diğerleri, s.3.

[101] AB'de sıkça öne çıkarılarak kurumsallaştırılan bir kavram olan stratejik özerklik kavramı, bir ülkenin savunmadan ekonomiye, demokrasiden dijitalleşmeye kadar çeşitli politika alanlarında diğer ülkelere bağımlı olmadan hareket etme, önceliklerini belirleme ve karar alabilme kapasitesini ve yetkinliğini ifade eder. European Parliamentary Research Service, EU Strategic Autonomy 2013-2023: From concept to capacity, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf (15 Aralık 2024), s.1; Politika yapıcıları ve politikacılar stratejik özerkliği nihai karar vericilik yani egemenlik olarak görme eğilimindedir. Paul Timmers, "Ethics of AI and Cybersecurity when Sovereignty is at Stake", **Minds and Machines,** Vol.29, (2019), s.636.

[102] Sanja Ivic ve David Ramiro Troitiño, "Digital Sovereignty and Identity in the European Union: A Challenge for Building Europe", *European Studies: the Review of European law*, *Economics and Politics* 2022, Vol.9, No.2, https://doi.org/10.2478/eustu-2022-0015 (15 Aralık 2024), s.93-94.

teknolojilerinde üretim ve karar kapasitesi geliştirmek dijital egemenliğin somut göstergeleri olarak görülmektedir[103]. Paul Timmers'e göre, stratejik özerklik; egemenliğin kendisi değil, onu yeniden tesis etmeye yarayan bir araçtır. Stratejik özerklik, egemenliğin amacı değil aracıyken dijital egemenlik bu sürecin sonucudur. Dijital çağda, mutlak kontrol mümkün olmadığından bu kavram otarşi anlamına da gelmez. Önemli olan bağımlılıkları yönetmek ve karar gücünü korumaktır[104]. Bununla birlikte "özerklik" kavramı, tam bağımsızlıktan ziyade sınırlı hareket serbestisini çağrıştırdığı için kavramsal tartışmaya açıktır. Bu nedenle, dijital bağımsızlık veya teknolojik bağımsızlık ifadelerinin daha tutarlıdır.

Sonuç olarak devlet merkezli yaklaşımda kavramsal öz, devletin dijital alandaki üstün otoritesini[105] ve dijital varlıklar üzerindeki yargı yetkisini[106] ifade eder. Devletlerin dijital egemenlik kapsamında ele aldıkları stratejiler; veri akışının kontrolü, gizliliğin korunması, büyük teknoloji şirketlerinin gücünün sınırlanması, bağımsız dijital altyapıların kurulması, yapay zekâ ve yeni teknolojilerin geliştirilmesi ve siber güvenlik kapasitesinin artırılması alanlarında somutlaşmaktadır. Bu politikalar, yalnızca altyapı ve teknoloji değil, aynı zamanda kullanıcı özerkliği, veri mahremiyeti, ifade özgürlüğü, platform denetimi ve dijital self-determinasyon gibi alanlarda da kapsamlı bir normatif düzenlemeyi gerektirir. Bu kapsamda ulusal dijital pazarda yabancı teknoloji sağlayıcılar karşısında e-ticaret, rekabetin ve yerli firmaların korunması ekonomik egemenliğin dijital egemenliğe yansıyan boyutudur[107].

- **Teknolojik/altyapısal tanımlar:** Bu yaklaşım, dijital egemenliği salt teknik bağımsızlık ve altyapı kontrolü üzerinden tanımlar. Veri merkezleri, bulut sistemleri, ağ mimarisi ve algoritmalar üzerindeki fiili hakimiyet belirleyicidir. Kilit nokta, veri sahibinin kim olduğu değil veriler üzerinde kimin tahakküm kurup faaliyet yürütebilme

---

[103] Nathalie A. Smuha, "Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective", Gavin Barrett, Peter-Christian Müller-Graff, Jean-Philippe Rageade ve Viktor Vadasz (ed.) **European Sovereignty: The Legal Dimension** içinde (19-28), Springer, 2024, s.6.
[104] Timmers, *"Sovereignty in the Digital Age",* s.577, 580.
[105] Ali Shoker, "Digital Sovereignty Strategies for Every Nation", *Applied Cybersecurity & Internet Governance,* 2022, Vol.1, No.1, https://doi.org/10.5604/01.3001.0016.0943 (14 Aralık 2024), s.4.
[106] Tipper ve Krishnamurthy, s.1-2.
[107] Eren, s.561-563.

gücüne ve kapasitesine sahip olduğudur[108]. Ancak bu çerçeve, egemenliği devlete özgü bir hukuki kategori olmaktan çıkararak teknoloji şirketlerine de atfedebilir hâle getirir. Böylece egemenlik kavramı klasik anlamından uzaklaşır ve güç ilişkilerini açıklayan betimleyici bir kavrama dönüşür.

Teknoloji şirketlerinin erişim kısıtlama, platform kuralları koyma ve dijital alanı yönetme kapasitesi, devlet dışı aktörlerde egemenlik benzeri güç yoğunlaşmalarına yol açmaktadır. Teknolojinin bir sonucu olarak ortaya çıkan bu güç yalnızca teknoloji aracılığıyla sürdürebilir[109]. Devletin dijital alandan çekilmesi, bu fiili güç odaklarının düzenleyici aktörlere dönüşmesi riskini doğurur. Dijital alan, artık kamusal değerlerden değil, teknolojik sınırlarla tanımlanan özel çıkarlar üzerinden şekillenir.

Dijital alandaki otoriteyi tanımlamak için hukuki ve siyasi çağrışımlarla yüklü bir kavram olan egemenlik teriminin bu şekilde farklılaşarak devletin dışında özel aktörlere alan açarak benimsenmesi post modern çağın getirdiği yeni bir süreçtir[110].

- **Birey merkezli veya toplumsal tanımlar:** Bu yaklaşım dijital egemenliği, bireyin; veri ve kimliği üzerindeki kontrolü olarak yorumlar. Dijital öz-belirlenim, anonimlik, veri taşınabilirliği ve algoritmik şeffaflık temel kavramlardır. Ancak bireysel veri özerkliğinin sınır ötesi uygulanabilirliği ve yaptırım mekanizmalarının etkinliği hâlen tartışmalıdır[111].

Bu bağlamda, öne çıkan bir kavram dijital otonomidir[112]. Otonomi bireylere, topluluklara veya otonom araçlara atfedilebilirken; egemenlik tarihsel olarak kolektif bir iradeye dayanır. Dolayısıyla bireyin özgür iradesi özerklik; kolektif irade ise egemenlik

---

[108] Nicola Fabiano, "Digital Sovereignty Between Accountability and the Value of Personal Data", **Advances in Science, Technology and Engineering Systems Journal,** Vol.5, No.3, (2020), s.272.
[109] Cass Sunstein, **Republic.com**, Oxfordshire: Princeton University Press, 2001, s.135.
[110] Roberts ve Diğerleri, s.2.
[111] Kristina Irion, "Government Cloud Computing and National Data Sovereignty". **Policy and Internet,** Vol.4, No.3-4, (2012), s.62.
[112] Otonomi (Yunanca autos: kendi ve nomos:yasa) kelimesi daha çok felsefi, psikolojik veya teknik bağlamlarda kullanılır: otonom birey, otonom sistem, otonom araç gibi. Türkçede özerklik olarak karşılık bulan otonomi, özellikle hukuk ve siyaset bilimi alanlarında bireysel veya kurumsal düzeyde karar alma bağımsızlığını ifade eder: yerel yönetimlerin özerkliği, üniversite özerkliği gibi. Siyasal ve hukuki bağlamda özerklik kelimesini; teknik veya bireysel irade bağlamında otonomi kelimesini tercih etmek daha uygundur.

kavramlarıyla ifade edilmelidir[113]. Bununla birlikte, otonomi yalnızca birey düzeyinde değil, devletler arası ilişkilerde de kullanılabilir. Otonomi dış etkilerden bağımsız karar alma kapasitesini ifade eder ve egemenliğin bir boyutu olan dış bağımsızlıkla yakından ilişkilidir. Ancak egemenlik, hem iç (halk üzerindeki yetki) hem de dış (diğer devletlere karşı bağımsızlık) yönleriyle daha geniş bir kavramdır. Bu nedenle otonomi, egemenliğin yerine geçmez; onun ön koşulu veya bileşeni olarak dijital egemenliğin içinde yer alır. Veri altyapısında dışa bağımlılığın azaltılması, yerli dijital çözümlerin geliştirilmesi ve uluslararası platformlara karşı bağımsız bir duruş sergilenmesi hem egemenlik hem de otonomi alanına girer.

Sonuç olarak, dijital egemenlik bu yaklaşımlar ışığında tek boyutlu bir kavrama indirgenemez. Devlet yetkisini, teknik kapasiteyi, bireysel hakları ve küresel normatif mücadeleyi aynı anda içeren katmanlı bir yapıya sahiptir. Yapılan tanımlardan yola çıkarak belirtmek mümkündür ki araştırmacılar, dijital egemenlik kavramının tanımlanmasında bir gecikmeyi ve yaşanan zorluğu teslim etmişlerdir. Bu zorlukların nedeni, egemenliğin tanımlanmasını devletin dijital alandaki görünümleri üzerinden yapmaktan kaynaklanmamaktadır. Aksine gelinen süreç kavramın, çoğunlukla devletin somut biçimde hükmedip drije ettiği[114] çeşitli ve katmanlı kontroller yaptığı ve güdümlediği ampirik bir durum üzerinden temellendirilmesine itmektedir. Ancak dijital egemenliği kavramsal olarak analiz eden bu tanımlar, dijital egemenliği değerlendirmek için etkili bir şekilde uygulanabilir bir teorik anlayış ortaya koymaktan ziyade terim etrafındaki kafa karışıklığını veya söylemdeki uygulamaları açıklamaya odaklanmış görünmektedir[115].

Kavramın muğlaklığı hem anayasal güvenceleri güçlendirme potansiyeli taşır hem de otoriter uygulamaları meşrulaştırma riski barındırır. Devletlerin fiili uygulamaları dijital egemenliğin giderek yerleştiğini gösterse de küresel uyumluluk ve karşılıklı güven

---

[113] Jean-Gabriel Ganascia, Eric Germain ve Claude Kirchner, “Sovereignty in the Digital Age: Keeping Control Over Our Choices and Values”, *CERNA*, (2018), https://www.allistene.fr/files/2019/05/55817_Sovereignty_CERNA_2018.pdf (11 Ocak 2026), s.13.

[114] Drije etmek, Fransızca "*diriger*" fiilinin Türkçeye uyarlanmış bir biçimidir. Fransızca'da "*diriger*", yöneltmek; yönetmek, çekip çevirmek, idare etmek anlamına gelir. fransizcasozluk.net, “diriger”, https://www.fransizcasozluk.net/index.php?q=diriger (E.T. 13.12.2024).

[115] Roberts ve Diğerleri, s.5.

olmaksızın klasik (Vestfalyan) egemenlik anlayışının dijital alana taşınması ciddi maliyetler doğurabilir[116]. Bu nedenle dijital egemenliğin hukuki içeriğinin açık biçimde tanımlanması; şeffaflık, temel hakların korunması ve dijital ekonominin güvenliği açısından zorunludur.

Kavram, nesne ve olguların zihinde oluşturduğu, sınırları kesin olarak belirlenmemiş genel ve soyut tasarımı ifade eder. Nesnel gerçeklik ancak kavramlarla ifade edilebilir; ancak kavramlar dünyası gerçekliğin kendisi değil, onun soyutlanmış ve genelleştirilmiş bir temsilidir. Araştırmacı gerçekliği kavramlarla anlatır; ancak kavramlar gerçeklikle bire bir örtüşmez. Sözcükler çoğu zaman gerçekliği eksik çerçeveler, çarpıtır ya da boğar[117]. Terim ise muayyen bir bilim, meslek ya da sanat dalı içerisinde anlamı sınırlandırılmış ve teknik nitelik kazanmış kavramı ifade eder. Bu nedenle her terim bir kavram olmakla birlikte, her kavram terim değildir; terimler, kavramların belirli disiplinler çerçevesinde somutlaştırılmış alt kümesi olarak değerlendirilebilir[118]. Belirli alanlar içinde anlam kazanmış terimler keyfî değiştirilemez.

Modern siyasal-hukuki düşünce, Orta Çağ'ın skolastik kavramlarından kopuşla doğmuş; farklı bir nesnel gerçekliğe gönderme yapan devlet merkezli yeni bir terimsel alan (egemenlik, ulus, meşruiyet vb.) oluşmuştur[119]. Kelimeler ile düşünceler arasındaki bağın kopması, Locke'un "kelimelerin suistimali" olarak nitelediği hatalı, tutarsız veya kasıtlı olarak belirsizleştirilen kullanım biçimleriyle bilginin özünün zedelenmesine ve hakikatin çarpıtılmasına yol açar[120]. Bu çerçevede, dijital egemenlik bir kapasiteye işaret ettiğinden münhasıran devlet için mülkiyet ve hakimiyet ilişkisi kurulan/kurulması gereken dijital kapasite/uzam anlamında kullanılması tutarlı ve gereklidir. Fakat çağın getirdiği yenilikleri açıklamak için egemenlik kavramını ekleyerek yapılan kavramsallaştırmalar, modern devletten sonra yeni ve postmodern siyasal iktidar kuramı

---

[116] Rogier J.E.H. Creemers, **"China's Approach to Cyber Sovereignty",** Berlin: Konrad Adenauer Stiftung, 2020, s.20.
[117] Akal, *Devlet, Yasa, Hakimiyet*, s.19.
[118] Muhammet Sefa Mutlu, **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması,** İstanbul: Adalet, 2020, s.25.
[119] Akal, *Devlet, Yasa, Hakimiyet*, s.19-20.
[120] Rukiye Akkaya Kia, "'Dikizleme' Kültü ve 'Unutuş' Üzerine, **Hukuk Kuramı,** Cilt. 7, No.1-2, (Ocak-Ağustos 2020), s.50.

ortaya koymadığı müddetçe oksimorondur. Bu bağlamda dijital iktidar kavramının kullanımı daha uygundur.

Literatürde devleti odağına almayan tanımlar, kavramın teorik bir çerçeve oluşturmaktan çok dijital dönüşümün ortaya çıkardığı fiili güç ilişkilerini açıklamaya yönelmiştir. Teknolojik gelişmenin aktörlerinin veri odaklı dijital imkanları araçsallaştırarak güç devşirdikleri ve bu güç üzerinden bir iktidar kurdukları yadsınamaz bir gerçektir. Ancak buradan hareketle bu güç odaklarını; dijital egemenlik kavramı kapsamında egemen olarak açıklayan veya yönetişim kavramı üzerinden yönetimin karar verici bir parçasına dönüştüren yaklaşımlar, siyasal iktidarı meşru otorite niteliğiyle kuramlaştırmış kamu hukuku disiplininde egemenliğin özünü oluşturan siyasal bütün ve rıza ilkelerini göz ardı ettiği için sorunludur; bilimsel olarak oturmuş ve terim anlamı kazanmış bir alana girilmiştir. Dijital çağın yeni güç biçimlerini açıklamak için yeni kavramlara ihtiyaç vardır; ancak egemenlik terimi, meşru siyasal otoritenin ifadesi olarak devlete özgü kalmalıdır. Bu nedenle tez kapsamında dijital egemenlik kavramı, klasik kamu hukuku geleneğiyle uyumlu biçimde, egemenliğin öznesi olarak devleti merkeze alan bir çerçevede kullanılmaktadır.

III. ÜRETİM SÜREÇLERİNİN VE SİYASAL İKTİDARIN BİRLİKTE DÖNÜŞÜMÜ

A. MODERN DÖNEMDEN POST MODERN DÖNEME DÖNÜŞÜMÜN İZLERİ

İnsanlık tarihi, farklı üretim tarzları etrafında şekillenen tarihsel aşamalardan oluşur. Bu aşamalar; üretim araçları üzerindeki mülkiyet ilişkileri, emeğin denetim biçimleri ve toplum ile doğa arasında kurulan ilişki tarzları bakımından birbirinden

ayrılır[121]. Üretim ilişkilerindeki her dönüşüm, yalnızca ekonomik yapıyı değil, siyasal iktidarın örgütlenme biçimini ve meşruiyet zeminini de dönüştürmüştür.

Bu bölüm, modern dönemden günümüze üretim ilişkileri ile siyasal iktidarın nasıl eşzamanlı ve karşılıklı olarak dönüştüğünü ortaya koyarak, dijital çağda yaşanan dönüşümlerin tarihsel ve teorik arka planını kurmayı amaçlamaktadır.

1. Modern Dönem

Akal'a göre devleti ele almak, modern dönemin düşünce tarzını kavramak anlamına gelir; devlet üzerine düşünmek ise modern devlet anlayışını sorgulamaktır[122]. Modern devlet, kurumsal ve ideolojik kökenleri Antik Yunan ve Roma'ya uzanmakla birlikte[123] esas biçimini moderniteyle kazanmıştır. Modernite; Batı'da akıl, bilim ve ilerleme fikrine dayalı olarak şekillenen ve evrensellik iddiasıyla diğer toplumlara yayılan tarihsel bir projedir[124]. Döneme adını veren "modern" kelimesi büsbütün yeni olanı, Devrimi, sanayiyi ve makineyi anlatırken; modernite, ilerleme düşüncesi temelinde modern dünyayı oluşturan bireyselleşme, laikleşme, endüstrileşme ve kentleşme gibi süreçleri ifade eder[125]. Bu projenin merkezinde aklın, toplumsal düzeni rasyonel ilkelerle kurabileceği inancı yer alır[126]. Modernite, ulus-devletin idari-hukuki yapısının kapitalist üretim tarzıyla bütünleştiği, hukuki-bürokratik ve rasyonel düzen idealinin kurulduğu insanlığın çağ atladığı evredir.

Modern dönemde ekonomik iktidar ile siyasal iktidar arasındaki ilişki giderek yoğunlaşmıştır. Üretim ve dağıtım süreçlerini denetleyen ekonomik güçler, siyasal karar alma mekanizmaları üzerinde de belirleyici hâle gelmiştir. Ancak bu ilişki tek yönlü

---

[121] Ali Murat Özdemir ve Diğerleri, **Genel Kamu Hukuku: Kuramsal Yaklaşımlar,** 2. Baskı, Ankara: İmge Kitabevi, 2020, s.45.
[122] Akal, *Devlet, Yasa, Hakimiyet*, s.21.
[123] Bihterin Dinçkol, "Atina Demokrasisinden Roma Cumhuriyetine – 'Demos'tan 'Populus Romanus'a", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.23, Sayı.3, (2017), s.751.
[124] Christopher Pierson, **Modern Devlet,** Burcu Erdoğan (çev.), Ankara: Chiviyazıları Yayınevi, 2015, s.59; Rukiye Akkaya Kia, "Uygarlık, Modernite ve Medeniyet Sözcüklerinin Hukuka Bakan Yüzü", **Journal of Istanbul University Law Faculty,** Cilt.64, Sayı.2, (2011), s.112.
[125] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.28.
[126] Rukiye Akkaya Kia, "Doktor Lütfi Hakkında Zeyl ve 'Fikr-i Islahât' Eseri", **Marmara Üniversitesi Hukuk Araştırmaları Dergisi,** Cilt.24, Sayı.2, (Aralık 2018), s.482.

değildir: siyasal iktidarın kurumsal biçimi de ekonomik gelişmenin yönünü etkilemiştir. Ekonomik iktidarın ideolojik meşruiyet araçları feodal dönemde din ve gelenek iken, kapitalist dönemde bu rolü burjuva dünya görüşü ve liberal-demokratik değerler üstlenmiştir[127].

Manuel Castells'e göre ekonomik örgütlenme modelleri kültürel ve kurumsal yapılar içinde şekillenir; teknolojik dönüşümler toplumlar arasında etkileşim yaratarak melez örgütlenme biçimlerini ortaya çıkarır[128]. Tarihsel olarak üretim biçimleri düşünceyi, dili, siyasal örgütlenmeyi ve toplumsal yapıyı belirlemiş; feodal üretim ilişkilerinin çözülmesi burjuvazinin öncülüğünde ulus-devletin doğuşunu hazırlamıştır[129].

Feodalizm, toprak mülkiyetine dayalı ve serf emeğinin rant yoluyla sömürüldüğü bir üretim düzenidir. Ticaretin ve piyasa ilişkilerinin zayıf olduğu bu yapı, keskin sınıf ayrımlarına dayanır[130]. Karl Marx ve Friedrich Engels'e göre burjuvazi, feodal bağları çözerek üretim ilişkilerini dönüştüren devrimci bir sınıf olarak ortaya çıkmıştır. Ancak kapitalizmin yarattığı üretici güçler, özel mülkiyet ilişkileriyle çatışmış; aşırı üretim krizleri ve emek sömürüsü kapitalizmin içsel çelişkileri hâline gelmiştir. Kapitalizm, kendi karşıtı olan proletaryayı da üretmiştir[131].

16. yüzyılda ekonomi alanında feodal ilişkiler, tüm ve hızlı biçimde çözülmeye başlaması sonucunda ekonomik yapıda, kent uygarlığının gelişmesiyle birlikte yarı açık ekonomi düzeninde kentler dışına taşan ve çeşitli pazarlara ulaşan açık ekonomi düzenine geçilmiştir[132]. Feodal tarımsal ekonomi yerini ticarete ve ardından sanayi üretimine bırakmıştır. Sanayi üretimi, rasyonel-bilimsel düşünceyi ve merkezi siyasal yapıları güçlendirmiştir[133]. Kapitalizmin üretim araçlarını, ilişkilerini ve pazarları sürekli

---

[127] Akad ve Diğerleri, s.45.

[128] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.238; Manuel Castells, **Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,** Ebru Kılıç (çev.) İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2008, s.454.

[129] Mehmet Ali Ağaoğulları ve Levent Köker, **İmparatorluktan Tanrı Devletine,** 9. Baskı, Ankara: İmge Kitabevi, 2020, s.182.

[130] Şenel, s.212-218.

[131] Karl Marx ve Friedrich Engels, "Komünist Parti Manifestosu", *Eriş Yayınları*, https://www.antikapitalist.net/kutuphane/acik-kitaplik/marxengels/manifesto.pdf , (23.01.2026), s.24-36.

[132] Akad, Dinçkol ve Bulut, s.89.

[133] Şenel, s.276-283; Uygun, s.198.

devrimcileştiren yapısı; ekonomiyi ve kültürü ulusal sınırların ötesine taşıyarak dünya pazarını, kozmopolit üretim-tüketim ilişkilerini ve zihinsel üretimin uluslararasılaşmasını yaratmış; nüfusu, mülkiyeti ve üretim araçlarını merkezîleştirmiştir[134].

Ulus-devletin yükselişinde akılcı endüstriyel örgütlenme, başlangıçta siyasal güçten bağımsız biçimde gelişmiş, zamanla siyasal yapıya hâkim olmuştu[135]. Ticaret burjuvazisi, parçalı feodal pazarlar ile aşırı geniş imparatorluk ölçekleri arasında en elverişli alan olarak ulusal pazarı tercih etmiş; bu nedenle merkeziyetçi devlet biçimlerini desteklemiştir. Üretim ilişkilerinin gelişimi, siyasal olarak da geniş ölçekli ve bütünleşik bir yapıyı zorunlu kılmıştır[136]. Bu bağlamda, modern devletin ayırt edici bir özelliğinin çok sayıda yerel birimi siyasal bir merkez etrafında birleştirmesi olması rastlantı değildir. Ulusal bilinç ve sınırlar, ırktan çok dil ve ekonomik bütünleşme üzerinden oluşmuştur[137]. Ulus-devlet, bu bakımdan kapitalist gelişimin belirli bir aşamasında işlevsel hale gelen modern bir siyasal form olarak okunabilir[138].

Hardt ve Negri, modern üretim ilişkileri modern devletle eşzamanlı biçimde geliştiğini tespit eder: köylülerden ücretli emeğin doğuşu, üretim araçları üzerinde özel mülkiyetin güçlenmesi ve ulusal pazarların oluşması modern kapitalizmin temel dönüşümleridir. Atölyeden fabrikaya geçiş, rasyonel bürokrasi ve Fordist mekanik üretim modern egemenlik düşüncesinin ekonomik karşılığı olmuştur. Kapitalist üretim modelinin "tekil karar verici" mantığı, modern siyasal egemenlik anlayışıyla paraleldir. Kapitalist üretim düzeni; sermaye ile emek arasındaki karşılıklı bağımlılıktan kaynaklanan yapısal bir tenakuz üretir: sermaye emeğe muhtaçtır, emek de sermayeye. Ancak üretim sürecindeki sömürü, işçiyi hem ezilen hem de üretkenliği nedeniyle sistemin vazgeçilmez öznesi yapar[139].

---

[134] Marx ve Engels, s.25-26.
[135] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.34.
[136] Uygun, s.198.
[137] Şenel, s.283-284.
[138] Erözden, s.85.
[139] Michael Hardt ve Antonio Negri, **Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,** Barış Yıldırım (çev.), İstanbul: Ayrıntı Yayınları, 2004, s. 346-348.

Burjuvazinin mutlak monarşilerle kurduğu ittifak; feodalizmi tasfiye eden mutlak monarşilerin burjuvazi için zamanla engel hâline gelmesi nedeniyle bozulmuş ve bir siyasal mücadeleye dönüşmüştür. Üretici sınıf olarak güçlenen burjuvazi; krala karşı parlamentonun yetkilerini bazı ülkelerde liberal düşünceleri geliştirerek bazı ülkelerde tıkalı yolları devrim ile aşarak siyasal iktidarı ele almıştır. Bu süreçte Niccolò Machiavelli siyasal iktidarın laik ve bilimsel yönünü; Jean Bodin hukuki egemenlik kavramını; Thomas Hobbes toplum sözleşmesini; John Locke ve Jean-Jacques Rousseau ise özgürlük ve halk egemenliği düşüncesini modern devletin ideolojik temeli hâline getirmiştir[140]. Liberal görüş çerçevesinde kapitalizm; mülkiyet, sözleşme ve girişim özgürlüğüne dayanan rekabetçi sistem, açıkça bir piyasa sistemidir[141].

Aydınlanma düşüncesi; anayasal düzeni, hukukun üstünlüğünü ve yurttaşlığı kurumsallaştırmış; devrimlerle halk egemenliğini meşruiyetin temeli hâline getirmiştir. Fakat aynı zamanda bir ütopyadan ziyade zorla toplumsal yeniden inşa, biyopolitik kontrol ve otoriter devlet biçimleri de üretmiştir; Sovyet deneyimi ve modern totaliter rejimler bunun somut örnekleridir[142]. Michel Foucault'nun tanımladığı disiplinci iktidar (okul, ordu, hapishane gibi kurumlarla bedenin denetimi) ve biyopolitik yönetim (nüfusun düzenlenmesi, kontrolü ve yönetimi) belirgin biçimde yükselerek modern toplumsal düzeni şekillendirmiştir. Bu bağlamda Hardt ve Negri'nin tespiti önemlidir: modern egemenlik, toplumu aşkın ve merkezî bir güç olarak düzenlerken; sermaye içkin, akışkan ve sınır tanımaz bir nitelik taşır. Egemenlik sınırlar çizer; sermaye bu sınırları sürekli aşar. Modern dönemin tarihi, bu iki güç arasındaki gerilimin tarihidir[143]. Bu gerilim, ilerleyen bölümlerde post-modern dönemdeki dijitalleşmeyle birlikte yeni bir boyut kazanacaktır.

---

[140] Uygun, s.208; Şenel, s.284-288, 302.
[141] Akad ve Diğerleri, s.27.
[142] Christopher Pierson, **Modern Devlet,** Burcu Erdoğan (çev.), Ankara: Chiviyazıları Yayınevi, 2015, s.59.
[143] Michael Hardt ve Antonio Negri, **İmparatorluk,** Abdullah Yılmaz (çev.), İstanbul: Ayrıntı Yayınları, 2003, s.335-338.

2. Postmodern Dönem

Postmodern dönemde üretim ilişkileri ile siyasal iktidar arasındaki karşılıklı dönüşüm derinleşmiş; küreselleşmenin belirleyici olduğu bir bağlamda kapitalizm, ulusal sınırları zayıflatarak kültürel formları dönüştürmüş, kolonyal eşitsizlikleri yeni biçimlerde yeniden üretmiş ve ulus-devlet merkezli dünya tahayyülünü çözmüştür[144]. Bu süreç, yalnızca ekonomik yapıyı değil, toplumsal gelişimin yönünü de değiştirmiş; modern düşüncenin ürettiği değerler, toplumsal değişimin hızının gerisinde kalmıştır[145].

Bilgi çağında üretim süreçlerinin örgütlenmesinde bilimsel bilgi ve teknoloji belirleyici hâle gelmiştir[146]. Endüstri 3.0 aşamasında analog üretimden dijital ve robotik sistemlere geçiş yaşanırken; Endüstri 4.0 ile birlikte yapay zekâ, nesnelerin interneti, 3D yazıcılar ve nanoteknolojiye dayalı karanlık fabrikalarda[147] robotlarla yapılan akıllı üretim modelleri ortaya çıkmıştır[148]. Üretimin insan emeğine duyduğu gereksinim azalırken, hız ve doğruluk bakımından insan kapasitesini aşan makine sistemleri belirleyici hâle gelmiştir. Bu dönüşüm, üretim ilişkilerinin yanı sıra insan-makine ilişkisini ve emeğin ontolojik konumunu da yeniden tartışmaya açmıştır[149].

Postmodernitenin temel taşıyıcı olgularından biri olan küreselleşme, neoliberal ekonomik varsayımların küresel ölçekte hegemonik hâle gelmesiyle yakından ilişkilidir. Küreselleşme; devletin küçültülmesi, özelleştirme ve düzenlemelerin gevşemesi yoluyla sermayenin dolaşımını kolaylaştıran bir süreçtir. Ancak sermaye serbestleşirken emeğin

---

[144] Arif Dirlik, **Postkolonyal Aura: Küresel Kapitalizm Çağında Üçüncü Dünya Eleştirisi**, Galip Doğduaslan (çev.), İstanbul: Boğaziçi Üniversitesi Yayınevi, 2010, s.136-137.
[145] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.73.
[146] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.43.
[147] Karanlık fabrika, tamamen otomatik sistemlerle üretimde hata payını oldukça azaltan ve bünyesinde insanın varlığına ihtiyaç duymadan üretimin yapıldığı yapılardır. endustri40.com, "Karanlık Fabrikalar ile İnsansız Üretim", https://www.endustri40.com/karanlik-fabrikalar-ile-insansiz-uretim/ (Erişim tarihi: 13.12.2024).
[148] Suat Aksoy, "Değişen Teknolojiler ve Endüstri 4.0: Endüstri 4.0'ı Anlamaya Dair Bir Giriş", **SAV Katkı,** Cilt.Nisan, Sayı.4, (2017), s.37.
[149] Penrose, s.1.

aynı ölçüde özgürleşmemesi, devletin sosyal koruma kapasitesinin zayıflaması ve piyasa güçlerinin belirleyiciliğinin artması yapısal eşitsizlikleri derinleştirmiştir[150].

Dirlik'e göre küreselleşme, modernleşmenin Avrupa-merkezci tek merkezli dünya anlayışını aşmış gibi görünse de kapitalist üretim ilişkilerinin evrenselleşmesini kaçınılmaz bir son olarak sunarak gerçek alternatiflerin ortaya çıkmasını fiilen engellemiştir. Süreci ileriye taşıyan başlıca güç gelişmiş kapitalist ekonomiler olsa da Üçüncü Dünya ülkelerinin ve Çin gibi sosyalist bir devletin neoliberal modele uyum sağlaması bu hegemonyanın küresel ölçekte pekişmesini mümkün kılmıştır[151]. Bu süreç, kapitalizmin yaşadığı birikim krizlerine verilen stratejik bir yanıt olarak şekillenmiş; üretimin ulusötesileşmesi, şirket gücünün artışı ve ekonomik merkeziliğin çözülmesiyle sonuçlanmıştır. Sermaye, mekânsal bağımlılıktan kurtularak üretimi küresel ölçekte yeniden konumlandırmış; ulus-devletlerin ekonomik denetim kapasitesi daralmıştır[152].

Peter Drucker, bu dönüşümü enformasyon kapitalizmi kavramıyla açıklamaktadır. Ona göre bilgi; fiziksel emek ve sermayenin önüne geçerek temel üretim aracı hâline gelmiştir[153]. Postmodern üretim ilişkilerinde bilgi artık yalnızca üretim süreçlerine uygulanmaz; doğrudan bilgiye uygulanır[154]. Böylece ekonomik değer, emek yoğun üretimden yenilik, verimlilik ve bilgi işçiliğine kaymıştır[155].

Bu dönüşümü en kapsamlı biçimde analiz eden isimlerden biri olan Manuel Castells, enformasyon teknolojisi paradigmasının üretimi ağ temelli bir yapıya dönüştürdüğünü belirtir. Esnek, yeniden programlanabilir ve küresel ölçekte işleyen bu yapı, ağ toplumunun teknik ve ekonomik temelini oluşturmuştur. Enformasyon, yalnızca üretimi etkileyen bir unsur olmaktan çıkmış; bizzat üretimin çıktısı hâline gelmiştir[156]. Finansal sermaye, yüksek işlem kapasitesine sahip dijital altyapılar sayesinde saniyeler

---

[150] Murat Demircioğlu, "Günümüz Endüstriyel İlişkilerinde Çokuluslu Şirketlerin Etkileri", **Prof. Dr. Kenan Tunçomağ'a Armağan,** İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Eğitim, Öğretim ve Yardımlaşma Vakfı Yayını, Yayın No: 4, ss. 101-115, (1997), s.105.
[151] Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.26, 31-32.
[152] Dirlik, *Postkolonyal Aura: Küresel Kapitalizm Çağında Üçüncü Dünya Eleştirisi,* s.132-135.
[153] Drucker, s.254-256.
[154] Drucker, s.33, 63.
[155] Drucker, s.16-18.
[156] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.88-100.

içinde küresel ölçekte dolaşabilir hâle gelmiş; ekonomik faaliyet giderek fiziksel üretimden koparak finansal akışların yoğunlaştığı ağlarda merkezileşmiştir[157].

Ağ, yalnızca bir metafor değil; küresel kapitalizmin maddi örgütlenme biçimidir. Ulus-devletler egemenlik iddialarını sürdürse de ekonomik faaliyetin merkezi artık ulusal sınırlar değil, küresel ağların stratejik düğüm noktalarıdır. Bu yeni uluslararası iş bölümü devletler arasında değil; ağ içindeki enformasyonel ucuz emek ve ham madde üretimi gibi küresel konumlar arasında örgütlenir. Her ülke bu konumların hepsini barındırdığı için eşitsizlik ulusal değil, ağsal bir karakter taşır[158].

Bu bağlamda postmodern siyasal iktidar hem merkezsizleşmiş hem de yeni biçimlerde yeniden merkezileşmiş ağsal bir yapı olarak ortaya çıkmaktadır. Ağ temelli üretim modeli, ulus-aşırı şirketlerin gücünü devlet sınırlarının ötesine taşıyarak kapitalizm-devlet ilişkisinde yeni bir güç kayması yaratmıştır. Modern toplumun dönüştürücü aygıtı olarak devlet Pazar kıskacının eline düşmüş; varlığını sürdürse de egemenliği bulanıklaşmıştır. İktidar; ulus-üstü kurumlar, küresel şirketler ve dijital platformlar arasında parçalı biçimde dağılmıştır[159]. Şirketlerin küresel ölçekte serbest hareketi devletin geleneksel yetkilerini aşındırırken ortaya çıkan tablo, Polybios'un; siyasal iktidarın kaynağında kuvvetin olduğu "kuvvet-temelli ilk iktidar" tasvirini çağrıştırır: kendini koruyamayan insanların bir araya gelmesiyle oluşan toplulukta, en güçlü ve cesur kişi önder olup; insanların onun yönetimi ve koruması altına girmesiyle siyasal toplumun doğduğu[160]. Fakat yeni iktidar biçiminde belirleyici olan artık fiziksel zor değil, ekonomik ve teknolojik kapasitedir. Bu durum, siyasal iktidarın kaynağına ilişkin klasik varsayımları yeniden tartışmaya açmaktadır.

Akkaya'nın tespit ettiği üzere, küreselleşme, sermayeyi düşük maliyetli üretim ve vergi avantajı sunan bölgelere yöneltmiş; düşük ücretli emek arayışı yoğun bir dolaşım ve toplumsal dönüşüm yaratmıştır. Sınırsız ticaret ve para-emek hareketliliği, liberal

---

[157] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.120-133, 624.
[158] Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.37-42.
[159] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.73.
[160] Recai Okandan, "Devletin Tarihi Menşeini Kuvvet ve Mücadelede Bulan Muhtelif Görüşler", **İstanbul Hukuk Mecmuası,** Cilt.9, Sayı.3, ss. 495-515, (1944), s.497; Akad, Dinçkol ve Bulut, s.38; Şenel, s.193.

ekonominin yeniden güç kazanması anlamına gelirken, uluslararası rekabeti de neredeyse sınırsız hale getirmiştir. Bu yeni düzen, aslında tarihsel olarak tanıdık bir çatışma ve rekabet mantığının sivil alanda sürmesidir. Ulus-ötesi aktörler çoğalsa da değişmeyen temel kurum hukuktur; küresel düzen, ulus-üstü bir hukuka ihtiyaç duyar. Sınırları aşan sermaye bile güvenlik ve düzen için siyasal otoriteye muhtaçtır; aksi halde şiddet ve totaliter eğilimler yeniden güç kazanabilir[161].

Post-modern çağda, modernitedeki ulus-devlet-kapitalizm uyumu çözülmüş; yerini Hardt & Negri'nin "İmparatorluk" olarak tanımladığı çok-merkezli, dağınık ama birbirine bağlı iktidar odaklarından oluşan bir ağsal egemenlik almıştır. Küresel ağ ekonomisi, devlet-sermaye ilişkisini ulusal ölçekten ulus-aşırı düzeye taşıyarak egemenliği finans kurumları, küresel planlama organları ve dijital ağlara kaydırmıştır. Bu süreç politik otonomiyi zayıflatmış, devlet aygıtlarını ulus-aşırı komuta mekanizmalarına bağımlı hâle getirmiştir. Yetkiler, hükümetlerin birlikçi yapısından koparak ulus-aşırı kurullara, bankalara, finans merkezlerine ve küresel planlama organlarına dağılmaktadır. İktidarın denetim mekanizmaları yok olmamış, yalnızca ulus-devlet ölçeğinden küresel ölçeğe taşınmıştır. Bu yeni düzen, ulus-üstü egemenliğin kurumsal biçimi olarak adlandırılabilecek imparatorluk yapısının oluşumuna işaret eder[162].

Bu dönüşüm, toplumsal düzenin kontrol toplumuna evrilmesiyle tamamlanmıştır. Modernitenin merkezi ve kapalı disiplin kurumları (aile, okul, zorunlu askerlik, fabrika, hastane, hapishane, vb.) çözülmüş; iktidar, sürekli veri akışları ve dijital izler üzerinden işleyen bir denetim mantığına bürünmüştür. Gilles Deleuze'ün iktidarın sürekli veri akışlarında işlediği ve kimliğin sabit-kurumsal değil akışkan, melez ve sürekli yeniden üretildiği denetim toplumuna[163] ve Giorgio Agamben'in daimî yönetim tekniğine dönüşen sürekli istisna hâline geçilmiştir[164].

---

[161] Rukiye Akkaya, "Çözülen Sosyal Devlet ve Küreselleşme Olgusu", **Prof. Dr. Necip Kocayusufpaşaoğlu için Armağan,** Ankara: Seçkin Yayınları, (2004), s. 740, 742.
[162] Hardt ve Negri, *İmparatorluk,* s.315-320.
[163] Gilles Deleuze, "Postscript on the Societies of Control." **October**, Vol.59, (1992), ss. 3-7. s.3-4.
[164] Hardt ve Negri, *İmparatorluk,* s.338-340.

Sonuç olarak, Sanayi Devrimi gibi enformasyon ağı devrimi de kapitalizmin yeniden yapılanma süreçlerinin ürünüdür; bu nedenle postmodern toplum hem kapitalist hem enformasyoneldir[165]. Küreselleşme sürecinde ulus-devlet, otorite ve egemenlik; ulus-üstü kurumlar ve yerel yönetimlerle paylaşılır hâle gelmekte fakat yeni piyasa düzeni ona yeni işlevler de kazandırmaktadır[166]. Ulus-devlet artık kapitalist-ötesi küresel çok aktörlü düzenin unsurlarından yalnızca biridir[167].

B. KÜRESELLEŞME ÖTESİ YENİ ÜRETİM VE YÖNETİM TARZI: DİJİTAL KAPİTALİZM

Dijitalleşme, postmodern dönemin eğilimlerini yalnızca derinleştirmekle kalmamış, onları aşan yeni bir üretim ve iktidar düzeni yaratmıştır. Dijitalleşme bu dönüşümün hem motoru hem de ürünü olarak işlev görmektedir. Platform kapitalizmi, yapay zekâ ve küresel dijital şirketler devletlerin geleneksel yetki alanlarını aşındırırken; devletler de dijital araçları kullanarak iktidarlarını yeniden kurmaya yönelmektedir. Böylece egemenlik aynı anda hem çözülmekte hem de yeni biçimler altında yeniden inşa edilmektedir. Bu tekno-ekonomik dönüşüm beş temel boyutta ele alınabilir.

Birincisi, dijitalleşme postmodern üretim biçimlerini aşan yeni bir maddi zemin hâline gelmiştir. Üretim ilişkilerinin ulusötesi niteliği dijital bir boyut kazanmış; Fordist fabrika merkezli üretim modeli, esnek post-Fordist üretime[168] oradan da veri ekonomisi ve platform kapitalizmine evrilmiştir. Dijitalleşme, üretim ile tüketim arasındaki zamansal ve mekânsal bağımlılığı ve mesafeyi büyük ölçüde ortadan kaldırmış; otomasyon, yapay zekâ ve ağ temelli örgütlenmeler üretimin doğasını kökten dönüştürmüştür[169]. Platform ekosistemi ve pazarın sanallaşması, postmodern kapitalizmi

---

[165] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.15.
[166] Fulya Kıvılcım, "From 1980 on, the Impact of the Globalization on Democracy and Nation State Concept: Turkey Evaluation", **Journal of Social and Administrative Sciences**, Vol.4, No.2, (Haziran 2016), s.212.
[167] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.76-77.
[168] Muzaffer Dülger, "Homo Commoditus: 'Sahip Olmak, Genetik Metalar ve Fikri Mülkiyet'", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII Sayı.1, (2014), s.525.
[169] Hardt ve Negri, *İmparatorluk,* s.309.

daha yoğun bir evreye taşımış; küreselleşme ötesi bir yönüyle dijital imparatorluğa benzeyen yeni bir düzenin maddi temelini oluşturmuştur.

İkincisi, internet temelli bu yeni düzende merkezsizlik söylemi yaygın olmakla birlikte, fiilî iktidar yoğunlaşması giderek belirginleşmektedir. Küresel ölçekte işleyen dijital altyapılar; sosyal medya platformları, elektronik ödeme sistemleri ve bulut bilişim hizmetleri aracılığıyla veri, finans ve iletişim akışlarını sınırlı sayıdaki aktörün kontrolünde toplamaktadır. Facebook, Google, Amazon, Twitter gibi platformlar; Mastercard, Visa, PayPal gibi elektronik ödeme sistemleri ve AWS, Azure, Google Cloud gibi bulut hizmetleri, küresel veri ve finans altyapısını büyük ölçüde ABD merkezli bir çekirdeğe bağlamaktadır[170]. Ortaya çıkan bu yapı temel bir çelişkiyi açığa çıkarır: İnternet teknik olarak merkezsiz bir ağ olarak tasarlanmış olmasına rağmen, dijital çağın iktidar ilişkileri veri ve finansın belirli merkezlerde toplanmasına yönelmektedir. Tarihte benzeri görülmemiş bu denli yoğun merkezîleşme; dijital iktidarların küresel ölçekte denetim, yönlendirme ve müdahale kapasitesini artıran, oligopolistik ve tek yönlü bir mekanizma üretmektedir. Liberal ekonomik düzenin temel varsayımlarından biri olan rekabet, bu bağlamda altyapının farklı çıkar alanlarına bölünmesi ve yarı-tekelci yapıların oluşması üzerinden işlemektedir. Merkezsizlik söylemi ise, sorumluluğun belirsizleşmesine, hesap verebilirliğin zayıflamasına ve güçlü aktörler lehine işleyen bir düzenin meşrulaştırılmasına hizmet eden bir araç hâline gelmiştir[171].

Bu yapı, dijital sistemin tüm kullanıcıları açısından kırılgan, asimetrik ve bağımlılık üreten küresel bir iktidar ilişkisi doğurmaktadır. İktidar, bu anlamda, toplumsal internet ağının bütünlüğüne ve sürekliliğine bağımlı hâle gelmiştir[172]. Dijital kapitalizm, başlangıçta serbest etkileşimi mümkün kılan teknik altyapılar olarak tasarlanan platformların, zamanla veri toplama, davranışları yönlendirme ve ekonomik süreçleri algoritmalar aracılığıyla planlama kapasitesine sahip merkezî aktörlere dönüşmesiyle ortaya çıkmıştır. Bu dönüşüm sonucunda piyasa mekanizması, görünürde rekabete dayalı bir yapı sergilemekle birlikte, fiilen platformların belirlediği kurallar, merkezi planlama

[170] Aust ve Ammann, s.36.
[171] Hardt ve Negri, *İmparatorluk,* s.311-312.
[172] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.350.

pratikleri ve optimizasyon hedefleri doğrultusunda işleyen yeni bir üretim ve yönetim tarzına evrilmiştir[173].

Üçüncüsü, küreselleşmenin yeni evresi veri akışları üzerinden işlemektedir. Veri artık yalnızca üretimi kolaylaştıran bir araç değil, bizzat üretilen meta hâline gelmiştir[174]. İnternet ağları üretim, dağıtım ve tüketimin mekânına dönüşmüş; sınır ötesi veri akışları küresel ekonominin belirleyici unsuru olmuştur[175]. Google, Amazon ve Alibaba gibi büyük dijital platformlar, tedarikten tüketici etkileşimine kadar tüm süreçleri veri üzerinden yöneterek küresel ölçekte altyapılar kurmuş; algoritmalar aracılığıyla piyasa davranışlarını yönlendirme kapasitesi kazanmıştır[176]. Böylece veri akışları, sermaye ve mal akışlarını tamamlayan değil, onları yönlendiren merkezi bir unsur hâline gelmiştir.

Dördüncüsü, dijital kapitalizmin yükselişi ulus-devletin iktidar kapasitesini aşındırmıştır. Dijital mekânsızlık, toprak temelli egemenlik mantığını zorlamakta; çok uluslu teknoloji şirketleri emperyal devlet yapılarına ihtiyaç duymaksızın küresel pazarlara nüfuz edebilmektedir[177]. Ulus-devlet ortadan kalkmamış, ancak işlevsel olarak dönüşmüştür: bazı yetkilerini ulus-üstü yapılara devretmekte, bazı alanlarda ise küresel sermaye için daha elverişli bir düzenleyici aktöre indirgenmektedir[178]. İktidarın gerçek mekânsallığı artık ulusal sınırlar değil, küresel dijital ağların düğüm noktalarıdır[179].

Beşincisi, dijital kapitalizm toplumsal yaratıcılığın sömürülmesine dayalı yeni bir tahakküm biçimi üretmektedir. Davranışlar, kültürel üretimler ve düşünsel faaliyetler veri hâline getirilerek algoritmik manipülasyona tabi tutulmakta; toplumsal yaratıcılık

---

[173] Vili Lehdonvirta, **Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control,** London: The MIT Press, (2022), s.209-210.
[174] Banu Akdenizli, "İnternet, Egemenlik ve Devlet: İnternet'in Ulusal ve Uluslararası Yönetime Etkileri Üzerine Bir Değerlendirme", **Global Media Journal,** Cilt.Bahar, Sayı.2, (2011) s.34.
[175] Stephen Weymouth, **Digital Globalization Politics, Policy, and a Governance Paradox,** Cambridge: Cambridge University Press, 2023, s.1.
[176] McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx#:~:text= , (28 Ocak 2026), s.6.
[177] Hardt ve Negri, *İmparatorluk,* s.338-340.
[178] Akad ve Diğerleri, s.141.
[179] Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.41-42.

faydacılık ve verimlilik ölçütlerine indirgenmektedir. İyi olan, kendi başına iyi olduğu için değil, işe yaradığı için iyidir. Hakikat, kendi oluş süreci içinde değil; koşullara ve çıkarlara göre ele alınır. Bunun sonucunda insanın tüm faaliyetleri sahteleşir; çünkü insanı ve toplumsallığını ifade etmeyen her yapı, özü gereği insana karşıdır[180].

Bu dönüşüm, Yanis Varoufakis tarafından "teknofeodalizm" kavramsallaştırmasıyla açıklanmıştır. Varoufakis'e göre dijital kapitalizm, klasik kâr mantığını aşarak dijital "topraklar" üzerinde rant toplamaya dayalı yeni bir düzen yaratmaktadır[181]. Bulut bilişim altyapıları ve kapalı platform ekosistemleri, erişimi kontrol ederek kullanıcılar ve üreticilerden sürekli "dijital kira" tahsil etmektedir. Zenginlik faizden ya da üretim kârından değil, kapalı "bulut tımarlarına" yani dijital ekosistemlere (Amazon, Google Play Store, App Store vb.) giriş ve kullanım hakkından elde edilir; kullanıcılar ve satıcılar platforma erişebilmek için daimî bir dijital kira ödemek zorunda kalır[182].

Günümüz ekonomisinde çevrimiçi mal ve hizmet satan tüm üreticiler artık bulut tımarlarına erişmeden müşteriye ulaşamaz. Bu yapı, feodal düzenin ekonomik sistemi gibi kapalıdır. Buradaki bağımlılık fiziksel zorbalıkla değil, algoritmik görünmezleştirme ile işler. Çünkü arama sonuçlarından silinmek ya da platformdan çıkarılmak dijital varoluşun tamamen sona ermesidir. Uygulama geliştiriciler, dijital mağazanın-tımarın kullanım hakkı için gelirlerinin bir bölümünü "dijital kira" olarak ödeyerek modern "vasal" görevini icra ederler. Bu yapı, feodal kira ilişkilerinin dijital biçimidir: dikkat ekonomisi sayesinde dijital mülkün sahibi platformlar; reklamverenlerden, geliştiricilerden ve satıcılardan bulut rantı toplar; böylece tüketici özgürlüğü erir ve ekonomi üretimden çok erişim-kontrol mekanizmalarına dayanan teknofeodal bir yapıya dönüşür[183]. Bu yapıda pazarlar serbest değil; kurallar tek taraflıdır, veri kontrolü

[180] Kemal Çalgan, **Kapitalizmin Egemenlik Yapısı ve Dijital Tahakküm,** Ankara: Klaros Yayınları, 2023, s.133-135, 146-148.
[181] Uygun, s.160.
[182] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.2.
[183] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.114-118.

merkezîdir ve ekonomik faaliyet platform sahiplerine bağımlıdır. Böylece rekabetçi kapitalizm çözülür, yerine dijital beylikleri andıran hiyerarşik bir düzen geçer.

Varoufakis, dijital alandaki "kişiselleştirme" seçeneklerinin bu düzene hizmet eden yanılgı olduğunu ileri sürerek; ücretsiz hizmet karşılığında bireyin kimlik, dikkat ve davranış verilerinin şirkete devredildiği Faustvari bir takasa benzetir[184]. Benzer şekilde Uluk; kişiselleştirilmiş deneyim söyleminin, gerçekte gözetimi, manipülasyonu ve sınıflamayı perdeleyen bir maskeye dönüştüğünü öne sürer[185]. Kapitalizmin özgürlük anlayışı, ontolojik bir özgürlük değil, paraya ve tüketime bağlı yapay bir olanaklar özgürlüğüdür[186]. Bu düzenin yeni araçları olan dijital platformlar ise insanların ne isteyeceğini belirler, yapay zekâ destekli sistemler tercihleri yalnızca tahmin etmekle kalmaz, otomatik olarak şekillendirir; tüketimi tatmin değil, sürekli doyumsuzluk üreten bir döngüye dönüştürür[187]. Bu süreç, komuta sermayesinin otoritesinin yükselişine yol açar: ekonomi artık nesne üretmekten çok arzunun kaynağını kontrol etmek üzerine kuruludur. Algoritmaların karmaşık ve opak yapısı, kullanıcıları manipülasyona açık hâle getirir. Ücretsiz hizmet karşılığında kullanıcı verisini, dikkatini ve davranışlarını platformlara teslim eder; algoritmalar ise sadece ürün satmakla kalmaz, dikkati metalaştırarak üçüncü taraflara pazarlayan bir sömürü mekanizmasına dönüşür[188]. Bu yüzden, bir dönem önemli bir imkân ve kolaylık olarak görülen dijital platformların, beraberinde ciddi sorunlar da doğurduğu her geçen gün daha net biçimde fark edilmektedir.

Varoufakis'e göre asıl kırılma gözetimde değil, veri mülkiyetinin el değiştirmesindedir. Big Tech ortak dijital alanları çitleyerek özel mülke dönüştürmüş; en sıradan dijital faaliyet bile veri, dikkat veya kimlik bilgisi ödeyerek yapılır hâle gelmiştir.

---

[184] Faustvari takas kavramı, Goethe'nin Faust eserine dayanır. Eserde Faust; sınırsız bilgi, haz ve güç karşılığında ruhunu Mephistopheles'e yani şeytana satar. Bu nedenle "Faustvari" sıfatı, bedeli gizli ama yıkıcı olan bir anlaşmayı imler. Faustvari takas, insanın ilerleme ya da güç adına kendi geleceğini ipotek altına almasıdır.

[185] Murat Uluk, "Veri Odaklı Kapitalizmin Ardındakiler: Aktörler, Değişen İş Modelleri ve Algoritmaların Rolü", **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021, s.112.

[186] Çalgan, s.171-173.

[187] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.53.

[188] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.67-77.

Dijital toprağın sahibi platformdur; kullanıcılar ve üreticiler bu alanda var olabilmek için verilerini, emeklerini veya ücretlerini ödemek zorundadır[189].

Bu bağlamda dijital kapitalizm, toplumun sınıfsal yapısını dönüştürerek üretken iki yeni sınıf yaratmaktadır: platformlar için ücretli çalışan "bulut proleterleri" ve ücretsiz veri ve etkileşim üreten "bulut serfleri". Algoritmik sistemler, bu iki grubun emeğini ve verisini sürekli işleyerek sermayenin kendini yeniden üretmesini sağlamaktadır. Artı değer kullanıcıların ücretsiz ürettiği içerik ve verilerden oluşur; böylece milyarlarca kişi farkında olmadan bu sermayeyi sürekli olarak yeniden üretir[190]. Navigasyon uygulamalarından sosyal medya platformlarına kadar çeşitli uygulamalar, kullanıcıları gönüllü veri üreticilerine dönüştürür. Google, Facebook ve diğer şirketler; tahmin ve hedefleme için onlarca veri türünü sistematik biçimde toplayarak davranışları izler[191]. Bu nedenle bulut sermaye düzeni, gönüllü ama karşılıksız dijital emek üzerine kurulu, veri mülkiyetinin şirketlerde toplandığı ve erişimin rant üzerinden belirlendiği, klasik kapitalizmden çok yeni bir teknofeodal sömürü yapısını yaratır. Böylece ekonomik sömürü, üretim alanından dijital davranış alanına kaymakta; veri mülkiyetinin şirketlerde yoğunlaşması siyasal ve kültürel tahakkümü de beraberinde getirmektedir[192].

Ekonomi giderek daha az kâr, daha fazla bulut rantı üzerine kurulurken, üretim artışı doğrudan platform sahiplerini zenginleştirir. Böylece kapitalizm, kendi geliştirdiği dijital altyapılar tarafından aşındırılarak yerini erişimi kontrol eden platformların hâkim olduğu teknofeodal yeni bir rejime bırakır. Karl Marx ve Friedrich Engels'in "kapitalizmin kendi mezar kazıcısını yaratması" tezi[193] bu bağlamda yeniden anlam kazanır: mezar kazıcı artık işçi sınıfı değil, kapitalizmin içinden doğan bu devasa platformlardır. Fakat kapitalizmi ortadan kaldırmak yerine, onun da ötesinde daha sorunlu ve ağır sonuçlar doğurabilecek bir düzen inşa etmektedir.

---

[189] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.71-74.
[190] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.76-86.
[191] Aust ve Ammann, s.9.
[192] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.46-48.
[193] Marx ve Engels, s.34.

Sonuç olarak dijital kapitalizm, kâr merkezli kapitalist düzeni aşındırarak rant/kira ve erişim kontrolüne dayalı yeni bir ekonomik-siyasal rejim üretmektedir. Bu nedenle Varoufakis ortaya çıkan yapıyı "hiper-kapitalizm" veya "rantiyer kapitalizm" gibi kapitalizmin bir aşaması değil, rantın yeniden merkezileştiği teknofeodalizm olarak adlandırmak gerektiğini vurgulamıştır[194]. Kapitalizmin tekno-feodal bir yapıya evrilmesini yansıtan temel farklılıklar şu şekilde özetlenebilir:

- Bu yeni düzende artı değerin kaynağı fiziksel emek değil, kullanıcı davranışlarından elde edilen veridir.
- Üretim mekânı artık fabrika değil, dijital platformlardır.
- Kâr, klasik anlamda piyasada ürün satışından ziyade verinin işlenmesi ve davranışların öngörülüp yönlendirilmesi üzerinden gerçekleşmektedir.
- Sömürü biçimi ise ücretli emekten; çoğu zaman gönüllü ve görünmez şekilde üretilen veri emeğine doğru evrilmiştir.
- Nihai amaç da yalnızca sermaye birikimi değil; veri akışının sürekliliğini sağlamak ve davranış yönlendirme kapasitesini artırmaktır.

Teknofeodal bulut rantı, devletin dijital egemenliğini iki yönden aşındırmaktadır: Ekonomik bağımlılık yaratarak kamu ve özel sektörün sürekli yabancı sağlayıcılara ödeme yapmasına neden olur; veri egemenliğini zayıflatarak kritik verilerin kontrolünü platform sahiplerine geçirir. Devlet dijital/feodal bağımlılığı azaltmak için hem piyasa düzenlemeleriyle tekelleşmeyi ve rant toplamayı sınırlamalı hem de ulusal bulut altyapıları, veri yerelleştirme standartları gibi dijital stratejilerle kendi egemenlik alanını güçlendirmelidir.

[194] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.120-121.

IV. VERİ ODAKLI DİJİTAL TEKNOLOJİLERİN TEMEL BİLEŞENLERİ VE ETKİLERİ

A. Büyük Veri Analitiği ve Endüstrisi: Verinin Yapay Zekâ Algoritmalarıyla İşlenmesi

1. Verileşme (Datafication) ve Büyük Veri

Dijital dönüşümün merkezinde yer alan temel olgu verileşmedir. Verileşme, insan davranışlarının, toplumsal süreçlerin ve nesnelerin dijital teknolojiler aracılığıyla ölçülebilir, kodlanabilir ve algoritmik olarak işlenebilir hâle getirilmesi sürecini ifade eder[195]. Bu süreç sayesinde daha önce ölçülemeyen veya kayıt altına alınmayan unsurlar, veri biçiminde izlenebilir ve analiz edilebilir hâle gelmekte; insan faaliyetleri dijital ortamda daha hızlı, daha verimli ve daha hedeflenmiş biçimde işlenebilmektedir[196].

Endüstri 4.0'ın dayanağını oluşturan verileşme sürecinde veri hem temel girdi hem de ortaya çıkan nihai ürün niteliği kazanmıştır[197]. Büyük veri analitiği yoluyla işlenen veriler, ekonomik değere dönüştürülerek dijital ekonominin çekirdeğine yerleşmiştir[198]. Bu yönüyle verileşme, yalnızca teknik bir süreç değil; üretim, yönetim ve iktidar ilişkilerini yeniden yapılandıran kurucu bir dönüşümdür.

Veri, Türk hukukunda ve öğretide işlenebilir ve ekonomik değere sahip bir unsur olarak kabul edilmektedir. TDK[199] ve 5651 sayılı Kanun'daki[200] tanımlar, verinin bilgisayarlar tarafından işlenebilir niteliğine işaret eder. Veri, dijital ekonominin temel yapı taşıdır; dijital altyapıları, platformları ve işlemleri mümkün kılan sanal bir

---

[195] Jose van Dijck, "Datafiction, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Secular Belief". **Surveillance & Society,** Vol.12, No.2, ss. 197-208, (2014), s.198.
[196] Küzeci, s.43.
[197] Kaplanhan, *"Dijitalleşme, Vergi ve Egemenlik Sorunu",* s.174-175.
[198] Osman Gökhan Antalya, s.1209, 1211.
[199] Veri, TDK'ya göre ***"bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge; muta, data, done"*** demektir. Türk Dil Kurumu, Güncel Türkçe Sözlük, https://sozluk.gov.tr (13.12.2024); Data kelimesi, Latince datum kelime kökeninden gelmektedir. Datum (verilmiş) kelimesi Dare (vermek) kökünden gelmektedir. Han, s.14.
[200] 5651 sayılı İnternet Kanunu'nun 2/1(k) bendine göre veri, ***"bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"*** olarak tanımlanmıştır. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Resmî Gazete, 23.05.2007, Sayı: 26530, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5 .

birimdir[201]. Analog verinin dijital formata dönüştürülmesiyle ortaya çıkan dijital veri; makine tarafından okunabilir, kodlanabilir, saklanabilir ve işlenebilir hâle gelerek ekonomik değeri olan bir varlığa dönüşür. Bu dönüşüm, veriyi sözleşmelere konu olabilen, devredilebilen ve ticari dolaşıma girebilen bir mal (*res commercium*) niteliğine taşır[202].

Veri, kişisel veri[203] niteliği taşıyabilir: kişisel veri; bir kişiyi belirlenebilir kılan bilgidir ve dijital olmak zorunda değildir; ancak dijital verinin kişisel veriden farkı, her türlü bilginin yalnızca dijital formatta kodlanmış hâlini kapsamasıdır.

Özel hukuk bakımından dijital veri, ekonomik değeri olan dijital bir eşya (*res digitales*) olarak değerlendirilmekte[204] içeriğine göre fikrî veya sınaî mülkiyet korumasına konu olabilmektedir[205]. Fikrî mülkiyette koruma için verinin eser sahibinin hususiyetini taşıması[206] gerekir; sınaî mülkiyette ise hususiyet aranmaz, bunun yerine yenilik ve sanayide uygulanabilirlik koşulları değerlendirilir[207]. Bununla birlikte dijital veri, soyut niteliği nedeniyle klasik anlamda mülkiyet hakkına doğrudan konu

---

[201] Kristina Irion, "Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows", Mira Burri (Ed.), **Big Data and Global Trade Law** içinde (231-242). Cambridge: Cambridge University Press, 2021, s.233.

[202] Osman Gökhan Antalya, s.1208.

[203] Kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3/1(d) maddesine göre "***kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"*** ifade eder. Aynı maddenin devamında kişisel verilerin işlenmesi ise, ***"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"*** kapsayacak şekilde tanımlanmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 07.04.2016, Sayı: 29677, https://mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 (14.12.2024).

[204] Osman Gökhan Antalya, s.1220.

[205] Osman Gökhan Antalya, s.1214.

[206] 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 1/B(a) maddesine göre, ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri kapsamında değerlendirilen her türlü fikir ve sanat mahsulü, eser sahibinin hususiyetini taşıması kaydıyla eser olarak kabul edilmektedir. Bu çerçevede, dijital verinin fikrî veri olarak korunabilmesi için de eser sahibinin hususiyetini taşıması gerekir. 5846 sayılı Fikir ve Sanat Eserleri Kanunu, Resmî Gazete, 13.12.1951, Sayı: 7981, https://mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf (14.12.2024).

[207] 6769 sayılı Sınai Mülkiyet Kanunu'nun 82. maddesi gereğince, yeni buluş içeren dijital verinin patentle korunabilmesi için sanayide uygulanabilir olma kriterini taşıması gerekir. 6769 sayılı Sınai Mülkiyet Kanunu, Resmî Gazete, 10.01.2017, Sayı: 29944, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6769&MevzuatTur=1&MevzuatTertip=5 (14.12.2024).

edilmemektedir[208]. Fikrî mülkiyet hukukunda dijital içeriklerin korunması, kural olarak insan yaratıcılığına dayalı bir katkının varlığına bağlanmaktadır. Bu nedenle tamamen otonom yapay zekâ tarafından üretilen çıktılarının eser sayılıp sayılmayacağı hususu, karşılaştırmalı hukukta tartışmalı olmaya devam etmektedir[209]. Güncel karşılaştırmalı eğilim, eser statüsünün belirlenmesinde insan katkısının niteliği ve belirleyiciliğini esas alan somut olay değerlendirmesine yönelmektedir. Türk hukukunda da bu ölçütlerin içtihat ve idari kılavuzlarla netleştirilmesi, hukuki belirlilik açısından önem taşımaktadır[210].

Verileşme, somut dünyayı dijital ortama taşıyarak dijital enformasyon toplumunun altyapısını oluşturur. Kullanıcılarının ürettiği veri, gözetim kapitalizminin ham maddesi hâline gelmiştir[211]. Dijital platformlar, kullanıcıların içerik tüketiminden çok veri üretimine odaklanmakta; arama motorları ve sosyal medya ağları, insanların bilgilenmesinden ziyade algoritmaların beslenmesi için veri toplamaktadır[212]. Kullanıcılar, dijital hizmetlere erişim karşılığında verileriyle ödeme yapmakta; böylece veri açık biçimde metalaşmaktadır.

Verileşmenin depolanabilir ve işlenebilir niteliği, tarihsel olarak tarım devrimindeki artık ürünün depolanmasıyla doğan iktisadi dönüşümle bir korelasyon içerisindedir. Depolanabilirlik, ekonomik sistemlerin kırılma noktasıdır[213]. Dijital çağda verinin depolanabilirliği ve algoritmik işlenebilirliği, onu yeni bir emtiaya dönüştürmüş; insanlığın üretim ve iktidar ilişkilerinde yeni bir ivme yaratmıştır.

---

[208] Chris Reed, "Information 'Ownership' in the Cloud", *Queen Mary School of Law Legal Studies,* 2010, Research Paper No. 45/2010, https://ssrn.com/abstract=1562461 (1 Ocak 2026), s.1.

[209] Başak Karmutoğlu, "Telif Hakkında Orijinallik Ölçütü ve Bunun Yapay Zekâ Tarafından Meydana Getirilen Eserler Açısından Değerlendirilmesi", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.2025, Sayı.2, 2025, s.1690-1692.

[210] Zeynep Aslı Özkan, "Üretken Yapay Zeka Çıktılarının Fikrî Mülkiyet Hukuku Kapsamında Değerlendirilmesi: Güncel Kararlar Işığında Bir İnceleme", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.2025, Sayı.2, 2025, s.1751-1753.

[211] Shoshana Zuboff, **Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,** Tolga Uzunçelebi (çev.), İstanbul: Okuyan Us Yayınevi, 2021, s.89.

[212] Dyson, s.309, 313.

[213] Yanis Varoufakis, **Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,** Sinan Arslaner (çev.), İstanbul: Epsilon Yayınevi, 2019, s.18.

Verileşme, bilgi ve iletişim kapasitesini olağanüstü artırarak dijital ekonominin ölçeğini genişletmiştir. Kişisel veriler küresel kapitalist pazarın parçası hâline gelmiş[214] dijital veri çevrimiçi işletmeler için temel ekonomik girdiye dönüşmüştür[215]. Veri analitiği, yalnızca ekonomik değil, aynı zamanda toplumsal düzenleme ve davranış yönlendirme kapasitesi yaratmaktadır. Piyasa toplumunun üretkenliğinde bir sıçramayı tetiklerken, dijital ürün ve hizmetler için yeni pazarlar da açmaktadır[216]. Bu dönüşüm, üretimi, yaşam tarzını ve düşünme biçimlerini yeniden şekillendirmektedir[217]. Castells'in "enformasyonelizm" olarak adlandırdığı bu yeni kalkınma biçiminde üretkenliğin kaynağı, bilgi işlem teknolojisinin geliştirilmesi ve bilginin bilgiyle işlenmesi yeteneğidir[218].

Bu sürecin teknik omurgasını büyük veri oluşturmaktadır. Dijitalleştirilen verilerin toplandığı ve işlendiği büyük veri, "*interneti kullanan insanlar tarafından üretilen ve ancak özel araç ve yöntemler yardımıyla depolanabilen, anlaşılabilen ve kullanılabilen çok geniş veri kümeleri*" olarak tanımlanabilir[219]. Büyük verinin özünde, verileştirilen devasa veri kümelerinin; toplanması, depolanması ve işlenmesi yatar. Bu süreç; edinim-analiz-algoritmik uygulama zinciriyle işler: veriler ya bireylerden doğrudan toplanır ya veri satıcılarından satın alınır ya da mevcut veri setleri birleştirilir. Ardından alınan algoritmik kararlara ve sınıflandırılan bireylere göre analiz edilir ve

---

[214] Helena Ursic, "The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?", Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?,** içinde (55-83), Springer Nature, 2018, s.56.

[215] Lennart Chrobak, "Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law", Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?,** içinde (253-272), Springer Nature, 2018, s.254.

[216] Rogier J.E.H. Creemers, **The Ideology Behind China's AI Strategy,** London: Nesta, 2020, s.63-64.

[217] Bediha Şahin, "Ulusal Yapay Zekâ Stratejilerinin Eğitim Yönü: Çin ve Türkiye Örneği", **Scientific Journal of Finance and Financial Law Studies**, Vol.3, No.2, (2023), s.82; Semih Erdoğdu, "Yapay Zekâ Rekabeti Bağlamında Çin'in Ontolojik Güvenlik Algısı", **Uluslararası Hukuk ve Sosyal Bilim Araştırmaları Dergisi,** Cilt.3, Sayı.2, (2021), s.6.

[218] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.20-21.

[219] **Cambridge Dictionary,** "big data", https://dictionary.cambridge.org/dictionary/english/big-data (E.T.: 14.12.2024).

nihayetinde bu bilgi algoritmik kararlara dönüşür[220]. Böylece tek başına anlamsız olan parçalı bilgiler, ölçek ekonomisi içinde işlenerek değer kazanır[221].

Büyük veri; hacim, hız ve çeşitlilik özellikleriyle yapay zekâ sistemlerinin zorunlu girdisidir. Hacim, veri kümelerinin büyüklüğünü; hız, verilerin üretilme ve analiz edilme hızını; çeşitlilik, veri türlerinin metin, ses, video veya diğer biçimlerde olabilmesini ifade etmektedir[222]. Verinin büyük miktarda olması, algoritmanın doğru tahminlere ulaşmasını sağlar[223]. Büyük veri olmaksızın yapay zekâ, sıradan bir yazılımdan öteye geçemez. Biyometrik tanıma sistemlerinden öneri algoritmalarına, giyilebilir teknolojilerden üretken yapay zekâya kadar günümüz dijital ekosisteminin tamamı büyük veri analitiğine dayanmaktadır[224]. Büyük verinin algoritmik analizi, yalnızca ticaret ve sosyal medyada değil, günlük yaşamın hemen her alanında kullanıcıya en uygun çözümleri sunmanın temeli hâline gelmiştir. Online alışveriş, tatil rezervasyonu, arama motoru, yol bulma uygulamaları gibi sistemler kullanıcılara en uygun çözümleri algoritmalar üzerinden veri analizi yaparak sunar[225].

Büyük veri endüstrisi, hammaddesi insan yaşamı olan küresel bir ekonomik alan olarak işlemektedir. Mobil cihazlar, sensörler, IoT ve platformlar aracılığıyla toplanan veriler; şirket gelirlerinin temel kaynağına dönüşmüştür[226]. Veri tüccarları ve büyük teknoloji şirketleri arasında gerçekleşen veri alışverişleri, bu piyasanın hem ekonomik

---

[220] Manon Oostveen ve Kristina Irion, "The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?" Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?** içinde (7-26), Springer Nature, 2018, s.8-9.

[221] İbrahim Aydınlı, "Yönetici Özeti", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya,** içinde (3-4), Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, Vol.Ocak, Sayı.9, s.4.

[222] Britannica, "Big data", https://www.britannica.com/technology/big-data (E.T.: 14.12.2025).

[223] Ömer Faruk Erol, **Algoritmik Regülasyon: Yapay Zeka ve İdarenin Regülasyon Faaliyeti,** İstanbul: On İki Levha Yayıncılık, 2023, s.20.

[224] Üretken yapay zekâ algoritmaları; resim, müzik, şiir, öykü, video ve film gibi sanatsal ve edebi eserler üretebilmekte, matematik soruları çözebilmekte, çeviri yapabilmekte, şarkı besteleyebilmekte, yorumlayabilmekte, dijital oyun geliştirebilmekte, akademik makalelerde ortak yazar olmakta ve duruşma beyanlarının yazımını yönlendirebilmektedir. Sinem Özyiğit ve Bengi Baydan, "Telif Hukuku Ekseninde Deepfake", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (567-582), Ankara: Adalet Yayınevi, 2023, s.568.

[225] Alper Aytekin ve Diğerleri, s. 157, 159.

[226] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", **Journal of Information Technology**, Vol.30, No.1, (2015) s.76.

hem de siyasal bir güç alanına dönüşmesine yol açmıştır[227]. Böylece verileşme, yalnızca ekonomik değil; toplumsal güç ilişkilerini belirleyen bir endüstri hâline gelmiştir.

Verileşmenin nihai amacı açıktır: Daha fazla veri, daha güçlü algoritma, daha yüksek kâr. Frank Pasquale'nin vurguladığı üzere çağdaş ekonomide kararlar giderek algoritmaların işlediği verilere dayanmaktadır[228]. Bu nedenle verileşme, yalnızca teknolojik bir gelişme değil; dijital çağın ekonomik, siyasal ve toplumsal düzenini şekillendiren temel bir iktidar mekanizmasıdır. Büyük veri bu özelliğiyle ulusal güvenlik ve jeopolitik rekabetin stratejik unsuru hâline gelmiştir. Üstelik bu durum yeni değildir: 1970'lerde veri akışları üzerindeki denetimin ekonomik bir güç olduğu ve bir ülkeye stratejik üstünlük sağlayabileceği belirtilmişti[229]. Bugün veri petrolden değerli kabul edilmekte; birçok ülke veri işleme kapasitelerini artırmak ve veriye sahip olmak için rekabet etmektedir[230]. Dijital kutuplar ABD ve Çin arasındaki rekabet özellikle büyük veri ve yapay zekâ teknolojileri üzerinde yoğunlaşmakta; yapay zekânın askeri gücü "dijital çağın atom bombası" olarak nitelendirilmektedir[231].

2. Dijital Profilleme: Kişiselleştirme ve Hedefleme Pratikleri

Dijitalleşme, bireyi yalnızca çevrim içi değil, çevrim dışı davranışlarıyla da sürekli ölçülen, sayısallaştırılan ve analiz edilen bir özneye dönüştürmüştür. Bu dönüşümün merkezinde yer alan dijital profilleme, büyük veri ve yapay zekâ teknikleri aracılığıyla bireylerin ilgi alanlarını, eğilimlerini ve muhtemel davranışlarını öngörmeyi amaçlayan tahmine dayalı bir veri işleme rejimidir. Profilleme, kişisel verilerin otomatik

---

[227] Uluk, s.100-103; Aust ve Ammann, s.131.

[228] Frank Pasquale, **The Black Box Society: The Secret Algorithms That Control Money and Information**, Cambridge: Harvard University Press, 2016, s.21.

[229] John M. Eger, "Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?" **Law and Policy in International Business,** Vol.10, No.4, (1978), s.1065-66.

[230] Iclal Turan, "Dünyanın en değerli kaynağı artık petrol değil: veri", https://iclalturan.medium.com/dünyanın-en-değerli-kaynağı-artık-petrol-değil-veri-c948405dcb44 (E.T.: 14.12.2024); The Economist, "The world's most valuable resource is no longer oil but data", https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (E.T.: 14.12.2024); Forbes, "Data is the new oil and that's a good thing", https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/ (14.12.2024).

[231] "Çağın dijital atom bombası" ifadesi, MİT Başkanı İbrahim Kalın'ın yapay zekâyı sunduğu büyük imkânların yanında getirdiği büyük tehditlerle tanımladığı metaforik bir değerlendirmedir; bkz. yirmidort.tv, "Çağın dijital atom bombası", https://www.yirmidort.tv/gundem/cagin-dijital-atom-bombasi-210490 (14.12.2025).

yöntemlerle işlenmesi yoluyla bireylerin veya grupların özelliklerini analiz eden ve bu analizleri geleceğe dönük karar mekanizmalarına dönüştüren algoritmik bir süreçtir[232].

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) 4. maddesinde profilleme; bir gerçek kişinin davranışları, tercihleri, ekonomik durumu, konumu veya hareketleri gibi unsurların analiz edilmesi ya da tahmin edilmesi amacıyla kişisel verilerin otomatik olarak işlenmesi olarak tanımlanmıştır[233]. Bu tanım, profillemenin yalnızca teknik bir veri işleme faaliyeti değil, birey üzerinde değerlendirme ve yönlendirme etkisi doğuran bir süreç olduğunu açık biçimde ortaya koymaktadır.

Bilginin değeri artık tekil verilerin varlığından değil, bu veriler arasında kurulan ilişkilendirme, sınıflandırma ve öngörü modellerinden kaynaklanmaktadır[234]. Dijital profilleme, bu işlevi kişiselleştirme ve filtreleme teknikleri aracılığıyla yerine getirir. Kullanıcının her etkileşimi (tıklama, konum değişikliği, arama, temas) bir öngörü girdisine dönüştürülmekte; bu öngörüler ekonomik, siyasal ve güvenlik amaçlı kategoriler altında yeniden yapılandırılmaktadır[235]. Hollanda Veri Koruma Otoritesi'nin de belirttiği gibi, bu veriler kişilerin ilgi alanları, alışkanlıkları ve sosyal geçmişi hakkında kapsamlı bir tablo sunarak bireyleri etkileyebilecek şekilde kullanılabilmektedir[236]. Profilleme teknolojileri sayesinde sosyal medya platformları yüksek karlar elde etmekte ve içerik üreticilerine de hatırı sayılır ödemeler yapmaktadır[237]. Böylece profilleme,

---

[232] Akçaal, s.487, 490.

[233] GDPR'ın 4. maddesinde profilleme, ***"kişisel verilerin, bir gerçek kişiyle ilgili bazı kişisel özellikleri değerlendirmek, özellikle söz konusu gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususları analiz etmek veya tahmin etmek amacıyla kişisel verilerin kullanılmasını içeren her türlü otomatik işlenmesi biçimi"*** olarak tanımlanmıştır. Avrupa Parlamentosu ve Avrupa Konseyi, 2016/679 General Data Protection Regulation (GDPR), 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[234] Drucker, s.267-270.

[235] Serkan Bulut, "Çokluk Mekânı Olarak Dijital Medya ile Egemenlik Çerçevesinde Bilginin Kontrolü ve Yapısal Dönüşümü", (**Yayınlanmamış Doktora Tezi,** İstanbul Üniversitesi SBE, 2019), s.89.

[236] Kristina Irion ve Natalie Helberger, "Smart TV and the online media sector: User privacy in view of changing market realities", **Telecommunications Policy,** Vol.41, No.3, (2017), s.18.

[237] GZT, "Sosyal medya reklam yatırımlarında hedef 100 milyar dolar", https://www.gzt.com/z-raporu/sosyal-medya-reklam-yatirimlarinda-hedef-100-milyar-dolar-3615837 (E.T.: 14.12.2024); LinkedIn, "Markalar 2017'den bu yana sosyal medya reklamlarına 930 milyar dolar harcadı", https://www.linkedin.com/pulse/markalar-2017den-bu-yana-sosyal-medya-reklamlar%C4%B1na-930-milyar-y3ehf/ (E.T.: 14.12.2024); Özge Özdemir, "Sosyal medya: Türkiye'de dijital medyanın reklam büyüklüğü ne kadar?" *BBC Türkçe,* 29 Temmuz 2020, https://www.bbc.com/turkce/haberler-turkiye-53329655 (31 Ocak 2026).

görünürde hizmet sunan ancak fiilen davranış yönlendirme ve denetim kapasitesi üreten bir iktidar teknolojisi hâline gelmektedir.

a. Veri Temelli Profilleme Tekniği

Veri temelli profilleme, bireyin dijital izlerinin tekil bir profil altında toplanması, analiz edilmesi ve bu analizlerin geleceğe dönük karar süreçlerinde kullanılmasıyla işler. Süreç üç aşamada gerçekleşir: veri çıkarma, yorumlama/modelleme ve hedefleme.

Veri çıkarma aşamasında, ağa bağlı her cihaz potansiyel bir veri toplama noktasıdır. Akıllı telefonlar, uygulamalar, tarayıcılar, ödeme sistemleri ve sensörler; konum, hareketlilik, tüketim ve sosyal etkileşimlere ilişkin verileri sürekli biçimde kaydeder[238]. Akıllı telefon tam anlamıyla konum bildiren bir mobil böcektir. Uygulamalar; konumdan günlük alışkanlıklara, sosyal çevreden finansal bilgilere kadar kullanıcının neredeyse tüm kişisel verilerini toplayan kapsamlı bir gözetim aracına dönüşmüştür. Pantolon cebindeki casus metaforu, akıllı telefonun artık yalnızca iletişim aracı değil, sürekli çalışan bir psikometrik kayıt cihazı olduğunu gösterir[239]. Makineler neredeyse tüm verileri toplayarak bireylerin ve çevreleriyle etkileşimlerinin davranışsal, duygusal ve zihinsel yönlerini analiz eder[240]. Böylece sıradan dijital araçlar sadece geçmişteki değil el-ânda kritik alanlarda kullanılmaya hazır devasa büyüklükte sürekli veri çıkarma altyapısına dönüşür. Bu durum, dijital araçların yalnızca iletişim veya hizmet sunma işlevi görmediğini; aynı zamanda bireyin davranışsal ve duygusal örüntülerini kaydeden sürekli bir izleme altyapısına dönüştüğünü göstermektedir.

Yorumlama ve modelleme aşamasında, yapay zekâ algoritmaları bu ham verileri anlamlandırarak bireyleri belirli kategorilere yerleştirir. Risk skorları, tüketici segmentleri, siyasal eğilim kümeleri veya güvenilirlik profilleri bu aşamada üretilir. Büyük ölçekli davranış verileri, psikometrik profilleme yoluyla bireylerin tercih ve tepkilerini öngörülebilir hâle getirir. Facebook kim olduğumuzu, Amazon ne istediğimizi,

---

[238] Aust ve Ammann, s.154.
[239] Han, s.23.
[240] Akçaal, s.489.

Google ne düşündüğümüzü yansıtan dijital kimlikler üretmesi gibi[241] bu süreçte bireyin dijital temsili, gerçek kişiliğinden bağımsız olarak algoritmik bir kimliğe dönüşür.

MIT'deki bir araştırma, yalnızca dört hareketlilik verisiyle bir kişinin %95 doğrulukla teşhis edilebildiğini; anonim verilerin ise %80 oranında yeniden kimliklendirilebildiğini göstererek, konum verilerinin benzersiz bir elektronik parmak izi niteliği taşıdığını kanıtlamıştır[242]. Google'ın şefi Eric Schmidt, bu durumu şöyle ifade etmişti: "*Biz nerede olduğunuzu biliyoruz. Geçmişte nerede bulunduğunuzu biliyoruz. Şu an neler düşündüğünüzü aşağı yukarı biliyoruz*"[243]. Böylece arz-talep eşleşmesi hızlanırken, tüketim ve davranış kalıpları şirketler lehine ince ayarlı biçimde yönlendirilir. Yapay zekâ sistemleri, sürekli bağlantılı ve otonom yapıları sayesinde büyük ölçekli verileri birleştirip analiz ederek profillemeyi derinleştirmekte; bu süreç, bireylerin farkında olmadıkları ihtiyaç ve istekleri ortaya çıkararak, veri kullanımının bilinmediği durumlarda davranışların yönlendirilmesi ve manipüle edilmesini mümkün kılmaktadır[244].

Hedefleme aşamasında ise üretilen profil doğrudan müdahale aracına evrilir. Algoritmalar; arama sonuçlarını, içerik akışlarını, önerileri ve görünürlük düzeylerini kişiye özgü biçimde düzenler; hatta fiziksel ortamları bile kullanıcıya göre ayarlar[245]. Birey, seçenekler arasında özgürce tercih yaptığını düşünse de hangi seçeneklerin görünür olacağı ve hangilerinin dışlanacağı çoğu zaman önceden belirlenmiştir. Bu mekanizma, bireyin rasyonel karar alma süreçlerini zayıflatan ve kamusal bilgi akışını parçalayarak enformasyon balonları yaratan yapısal bir etki üretmektedir.

---

[241] Dyson, s.308.
[242] Aust ve Ammann, s.154-156, 164.
[243] Business Insider, "Eric Schmidt: 'We know where you are, we know where you've been, we can more or less know what you're thinking about'", https://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10 (31 Ocak 2026).
[244] Akçaal, s.490.
[245] Balázs Bodó ve Diğerleri, "Tackling the Algorithmic Control Crisis: the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents" **Yale Journal Of Law And Technology**, Vol.19, No.1, (2017), s.134.

b. Profillemenin Uygulama Alanları

Profilleme, toplumsal düzenin kurgusuna sirayet eden yaygın bir mekanizmadır: Davranışsal reklamcılık, siyasal mikro hedefleme (dar hedefleme), içerik sıralama algoritmaları, tüketici profillemesi, kredi ve risk puanlaması, kamu hizmetlerine erişim ve Çin'in Sosyal Kredi Sistemi gibi sosyal sıralama rejimleri aynı mantığın farklı görünümleridir. Ortak nokta şudur: Bireyin dijital izleri ya kâr maksimizasyonu ya da siyasal ve ideolojik davranış kontrolü amacıyla işlenir. Han'a göre dijital çağda yükselen gözetim kapitalizmi, bireylerin verilerini metalaştırarak ekonomi ve siyaseti kökten dönüştüren yeni bir enformasyon rejimi yaratmıştır. Devletler ve siyasi partiler dijital platformları kamuoyunu yönlendirmek için kullanır; şirketler ise kişisel verileri kâr amacıyla toplar, analiz eder ve metaya dönüştürür[246].

Ekonomik düzlemde profilleme; dikkat ekonomisi, platform kapitalizmi ve gözetim kapitalizmi gibi veri temelli birikim modellerinin merkezindedir. Kullanıcının her etkileşimi metalaşır[247]. İnsan artık emek ya da beden üzerinden değil, verisi üzerinden sömürülen bir varlığa indirgenir[248]. Bireyin yaşam deneyimi, tercihleri ve geleceği reklam ve öngörü piyasalarında alınıp satılabilen ticari ürüne dönüşür. Çerezler ve benzeri izleme teknolojileri dijital reklam sektörünün temelini oluşturur; algoritmalar, psikolojik özelliklere göre uyarlanmış reklamlarla insanların davranışlarını yönlendirir[249]. Davranışsal reklamcılık, yalnızca ürün tanıtmaz; kapitalist ideolojinin tüketim nesnesine indirgediği insanın duyularını, güdülerini ve bilinçaltını hedef alarak yapay ihtiyaçlar ve yetersizlik hissi de üretir[250]. Fiziksel dünyada suç sayılabilecek izinsiz veri toplama pratikleri; dijital alanda kişiselleştirilmiş reklam ve kullanıcı deneyimi gibi masumlaştıran etiketlerle normalleştirilir[251]. Dijital platformlar; kullanıcıların ilgi ve

---

[246] İpek Kaya, "Enfokrasi: Dijitalleşme ve Demokrasi Krizi" **Kocaeli Üniversitesi İletişim Fakültesi Araştırma Dergisi**, Cilt.23, Sayı.66, (2024), s.57.
[247] Sunstein, s.18.
[248] Abdulsemet Aydeniz, "Enfokrasi: Dijitalleşme ve Demokrasinin Krizi, **Medya Okuryazarlığı Araştırmaları Dergisi,** Cilt.2, Sayı.1, (2023), s.7.
[249] Uluk, s.99-106.
[250] Çalgan, s.160-166.
[251] Lori Andrews, **I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy**, New York: Free Press, 2012, s.21.

zaaflarını tespit ederek profillenmiş içeriklerle dikkati yönlendirir, çevrimiçi kalış süresini uzatır ve böylece gözetim kapitalizminin davranışsal tahakkümünü kurumsallaştırır[252]. Bu şirketlerin ekonomik gücü, topladıkları verilerin işlenip pazarlanmasına dayandığından dikkat ve davranış verisi çağın en değerli kaynağına dönüşmüştür. Ücretsiz sunulan hizmetler; davranış verilerinin takası ve özel hayatın feda edilmesidir[253].

Siyasal düzlemde profilleme; gözetim ve kontrol toplumunun işleyişiyle birleşerek bireyi sürekli izlenen ve değerlendirilen bir özneye dönüştürür. Dijital cihazlar sürekli ve fark edilmeden veri üretirken, NSA belgeleri bu cihazların kolayca hacklenebildiğini ve iletişim verilerinin ayrıntılı biçimde izlenip analiz edilebildiğini göstermiştir. Böylece modern gözetim kapasitesi tarihte eşi görülmemiş bir düzeye ulaşmış; devletlerin istihbarat birimleri bu imkânları rutin bir araç haline getirmiştir. George Orwell'in öngördüğünü aşan dijital gözetim, kullanıcıyı kendi denetiminin taşıyıcısı haline getirirken[254] puanlama ve sınıflandırma mekanizmaları makbul vatandaşı teknik olarak inşa eder[255].

Çin'in Sosyal Kredi Sistemi bu mantığın kurumsallaşmış örneğidir; teşvik-ceza temelli davranış mühendisliğiyle bireyleri uyumluluk üzerinden yeniden şekillendirir. Vatandaşlar yalnızca hukuka uyumla değil, siyasi sadakat ve toplumsal uyum ölçütleriyle de değerlendirilir. "*Bir alanda güvenilmez olanın her yerde kısıtlanması*" anlayışının esas alındığı[256] bu sistem, başlangıçta ekonomik güvenliği amaçlarken zamanla vergi, ulaşım, eğitim ve gündelik yaşama yayılan kapsamlı bir mekanizmaya dönüşmüştür. Kara listeye girenler, eğitimden ulaşıma, finansmandan kamusal hizmetlere kadar birçok temel haktan fiilen dışlanmaktadır[257]. 2016 tarihli Devlet Konseyi belgesi, biyometrik veriler ve gerçek

---

[252] Aust ve Ammann, s.9.
[253] Aust ve Ammann, s.167.
[254] Aust ve Ammann, s.10-12.
[255] Rogier J.E.H. Creemers, "Disrupting the Chinese State: New Actors and New Factors", **Asiascape: Digital Asia,** Vol.5, No.3, (2018), s.185.
[256] Straton Papagianneas ve Adam Knight, "The Stumbling Smart State Fragmented Policy Experimentatio and Dubious Consolidation" Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (35-52), Maryland: Rowman & Littlefield Publishers., 2023, s. 38, 39.
[257] Creemers, *"Disrupting the Chinese State: New Actors and New Factors",* s.181,184.

isim kayıtlarına dayalı kapsamlı bir dijital doğrulama ağı öngörerek sosyal kredi mekanizmasını güçlendirmiş; özellikle kamu görevlileri ve kritik meslek gruplarının puanlanmasına öncelik vermiştir[258]. Sermaye-devlet iş birliği ile Alibaba'nın Susam Kredisi gibi özel sistemler de davranışlar, finans geçmişi ve sosyal ilişkileri temel alarak kullanıcıları sınıflandırıp çeşitli ayrıcalıklar sunmuştur[259]. Benzer biçimde Baihe gibi uygulamalar eş adaylarını bu skorlarla değerlendirmiştir[260]. Bu düzen, temel haklara erişimi etkilemekte ve fiilen sınırlamaktadır. Gözetlendiğini bilen bireylerin davranışlarını değiştirmesi, dijital profillemenin yalnızca teknik değil, öz-denetim üreten bir iktidar biçimi olduğunu göstermektedir.

Dijital profilleme, bireyin çevrim içi etkinliklerini sürekli izleyerek onu yönlendirilebilir bir özneye dönüştüren gözetim toplumunun altyapısını oluşturur. Bu rejimde tasarruf edilen bireyin kendisi değil, verisidir; mahrem deneyimler dahi davranışsal veri ürünlerine indirgenir ve hatalı tahminler bile özgürlük ile refah üzerinde ciddi riskler doğurur[261]. Yapay zekâ destekli bu yönlendirme süreçleri büyük ölçüde görünmez biçimde işler. Bu bağlamda Meta, Google, X ve Amazon gibi platformlar, bilgi akışını filtreleyerek dikkat ve düşünceyi şekillendiren yeni güç merkezlerine dönüşmüştür[262]. Bilgi akışını tekelleştirerek hem bireyler hem de devletler üzerinde yönlendirici etkide bulunmaktadırlar[263]. Bu gelişmeler, algoritmik ajanların etkisinden tamamen korunabileceğimiz bir alanın olup olmadığını sorgulatmaktadır. Teknolojinin,

---

[258] Chinese State Council, "Guanyu jiaqiang geren chengxin tixi jianshe de zhidao yijian, (Guiding Opinions concerning Strengthening the Construction of a Personal Sincerity System)", Translated in China Copyright and Media, 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/23/guiding-opinions-concerning-strengthening-the-construction-of-a-personal-sincerity-system/ (31 Ocak 2026), s. III. Accelerating the construction of personal sincerity records Başlığı.

[259] Shazeda Ahmed, "Cashless Society, Cached Data: Security Considerations for a Chinese Social Credit System". *CitizenLab*, 2017, https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system (31 Ocak 2026).

[260] Küzeci, s.214-215. Japonya'da da flört uygulamalarında kullanıcıların gelir verileri eşleştirme amacıyla talep edilmiştir. Milliyet, "Japonya'da düşen doğum oranlarına karşı 'flört' uygulaması başlıyor", https://www.milliyet.com.tr/dunya/japonyada-dusen-dogum-oranlarina-karsi-flort-uygulamasi-basliyor-7138109 (14.12.2024).

[261] Michal Kosinski, David Stillwell ve Thore Graepel, "Private traits and attributes are predictable from digital records of human behavior", **Proceedings of the National Academy of Sciences of the United States of America,** Vol.110, No.15, 2013, s. 5802, 5805.

[262] Pasquale, **s.**59-60.

[263] Hatipoğlu Aydın, s.102.

topluma etkilerini kavrayamadan kullanıma sunulması, kontrol kaybı hissi ve endişeyle karşılanmaktadır[264]. Gözetim kapitalizminin veri odaklı yönlendirme mekanizmaları birey özgürlüğünü ve eleştirel yargıyı aşındırdığı ölçüde demokrasi içten zayıflar; yurttaşlık, eşitlik, hukuk devleti ve halk egemenliği aynı anda tehdit altına girer[265]. Demokrasi, yurttaşın özgürce ve bilgilenmiş şekilde karar verebildiği bir rejim olmaktan çıkar; veriyle güdümlenen, algoritmalarla dışarıdan ayarlanmış davranışların toplamına indirgenir.

Neticede, filtreleme insan doğasının ayrılmaz bir parçasıdır. Algımız seçicidir; dünyayı bütünüyle değil, görmek istediğimiz biçimiyle algılarız. Bu yüzden insanlar her zaman kendi ilgi ve çıkarlarına uygun içerikleri seçme eğilimindedir. İnsan her zaman seçerek görür; özgür toplumlarda birey ilgi ve çıkarlarına göre içerik seçer. Fakat sorun, dijital kişiselleştirmenin bu doğal seçiciliği radikalleştirmesi ve manipüle edilebilir hâle getirmesidir.

3. Bulut Bilişim: Küresel Veri Akışı ve Veri Egemenliği

Küresel veri akışı, Herakleitos'un panta rhei ilkesini[266] dijital bağlamda çağrıştıran sürekli bir hareket düzeni olarak okunabilir. Nasıl ki ırmakta sabit kalan bir an yoksa, dijital çağda veri de sürekli çoğaltılan, aktarılan ve yeniden işlenen akışkan bir varlık hâline gelmiştir. Depolama, bu akışın kalıcı bir durağı değil; yalnızca geçici bir düğümlenme noktasıdır. Bu akışkanlık, dijital çağda bilginin fiziksel sınırları aşan mekânsız niteliğini ortaya koymaktadır. Castells'in *akışlar toplumu*[267] ve Lupton'un

---

[264] Bodó ve Diğerleri, "Tackling the Algorithmic Control Crisis – the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents", s.136.

[265] Svetlana Yakovleva ve Kristina Irion, "Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade", **International Data Privacy Law,** Vol.10, No.3, (2020), s.208; Harvard Gazette, John Laidler, "High tech is watching you: In new book, Business School professor emerita says surveillance capitalism undermines autonomy - and democracy (Q&A with Shoshana Zuboff)", 4 Mart 2019, https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy (14.12.2024).

[266] Herakleitos'a göre evrenin temel niteliği sürekli akıştır. Hiçbir şey durağan değildir; her varlık oluş, değişim ve yok oluş döngüsü içindedir. Nevzat Çevik, "'Panta Rei - Her Şey Akar' Mı?," **Son Nokta Dergisi,** Sayı.30, (2007), s.49; Şenel, s.126.

[267] Castells'in belirttiği gibi modern toplum, sermaye, bilgi ve teknolojinin akışları üzerine kuruludur; bu akışlar ekonomik, siyasal ve toplumsal süreçlerin merkezine yerleşmiştir. Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.547.

verinin sıvılaşması[268] kavramları, bu hareketliliğin ulus-devletlerin geleneksel denetim kapasitesini zayıflattığını göstermektedir. Dijital akışı yöneten modern logos[269] ise algoritmalar, teknik standartlar ve devletler ile büyük platformların kurduğu normatif-teknik mimaridir[270].

Bu küresel dolaşımın temel altyapısını bulut bilişim oluşturur. Bulut bilişim; verilerin depolanması, işlenmesi ve kullanılmasının internet üzerinden, çoğu zaman ulus-aşırı sunucular aracılığıyla gerçekleştiği bir hizmet modelidir[271]. Bu model, veriyi yerel donanımlardan küresel altyapılara taşıyarak[272] dijital hizmetlere her yerden erişim[273] maliyet düşüşü[274] ve idari kolaylık gibi avantajlar sağlar[275]. E-ticaret, çevrim içi uygulamalar ve dijital platform ekonomisi, bütünüyle sınır ötesi veri akışlarına

[268] Lupton'un vurguladığı verinin sıvılaşması, onun ulus-devlet tarafından denetlenmesini güçleştirir ve bu durum hem devlet egemenliğini hem de bireyin özerkliğini tehdit eden bir potansiyel taşır. Deborah Lupton, **Digital Sociology,** New York: Routledge, 2015, s.106, 107.

[269] Irmaktaki akış, rastlantısal bir düzensizlik değil, arka planda hiç değişmeden işleyen logos (söz, akıl) adı verilen düzen kurucu bir ilke tarafından yönlendirilir. Berceste Gülçin Özdemir, "Yürümek Bir Devrimdir: Henry David Thoreau'nun Yürümeye Dair Felsefesi ile Heraklitos'un Ateşe Atfettikleri Bağlamında The Way Filmi", **SineFilozofi,** Cilt.7, Özel Sayı.4, s.6.

[270] Burada kullanılan "modern logos" kavramı, Antik Yunan düşüncesindeki evrensel ve kozmik düzeni ifade eden panteist logos anlayışından farklı olarak, dijital çağda verinin akışını yöneten teknik, algoritmik ve normatif düzeni ifade etmektedir. Bu bağlamda logos, çoğul ve dağınık değil; büyük ölçüde merkezî platformlar ve devletler tarafından kurulan tekil bir rasyonaliteye indirgenmiştir. Dijital mimarinin bu tek merkezli düzenleyici karakteri, panteist bir akış anlayışından ziyade; kontrol ve yönlendirme temelli modern bir iktidar mantığına işaret etmektedir.

[271] U.S. Department of Commerce National Institute of Standards and Technology, The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (1 Şubat 2026), s.2.

[272] Cambridge Dictionary, "cloud computing,", https://dictionary.cambridge.org/dictionary/english/cloud-computing (3 Şubat 2026).

[273] Nir Kshetri, "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution". **Telecommunications Policy,** Vol.37, No.4, (2013), s.3.

[274] "Kullandığın kadar öde" modeli hem kamu yönetimine hem işletmelere maliyet avantajı sağlar; uygun altyapıya sahip gelişmekte olan ülkeler için de güncel teknolojilere erişim fırsatı yaratır. Kristina Irion, "Government Cloud Computing and National Data Sovereignty", **Policy and Internet,** Vol.4, No.3-4, 2012, s.45. Veri akışları hem maliyetleri ve işlem sürelerini düşürür hem de yeni ticaret ve pazar imkânları yaratır; hatta artık fizikî mal ticaretinden daha fazla ekonomik değer üretmektedir. Hunter Dorwart, "China and Global Data Transfers Implications for Future Rulemaking", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (123-152), Maryland: Rowman & Littlefield Publishers., 2023, s.123; UNCTAD, Digital Economy Report, 2021, https://unctad.org/system/files/official-document/der2021_en.pdf (1 Şubat 2026), s.v.

[275] Victor Mayer-Schönberger ve David Lazer, "From Electronic Government to Information Government" Victor Mayer-Schönberger ve David Lazer (ed.), **Governance and Information Technology** içinde (1-14), Cambridge, MA: MIT Press, 2007, s.7.

bağımlıdır; bu akışlar kesildiğinde dijital hizmetlerin sürdürülebilirliği de ortadan kalkmaktadır[276].

Bununla birlikte bulut bilişim, veriyi yabancı şirketlerin ve devletlerin denetim alanına sokarak egemenlik, gizlilik ve güvenlik riskleri üretmektedir[277]. Hizmet sağlayıcıya bağımlılık; veri kaybı, erişim kesintisi ve siber saldırı risklerini artırırken, verilerin farklı yargı alanlarına dağılması hukuki korumayı karmaşıklaştırmaktadır[278]. Irion'un da belirttiği üzere, kullanıcı çoğu zaman verisi üzerinde fiilî bir tasarruf yetkisi kuramamakta; kullanıcı-BigTech arasındaki sözleşme hükümleri işlem gücünü bireylerden alarak merkezî ve çoğu zaman yabancı platformlara devretmektedir[279].

Küresel veri trafiğinin Hawaii, Miami, Frankfurt, Amsterdam ve Kopenhag gibi belirli coğrafi düğüm noktalarında yoğunlaşması ve NSA'nın meta-veri temelli gözetim kapasitesi, veri akışının jeopolitik boyutunu açıkça ortaya koymaktadır. NSA, dünya genelinde yüzlerce fiber hat birleşim noktasına doğrudan erişebilmektedir. Meta veriler, içerikten bağımsız olarak iletişim ağlarının tamamını çözümleme ve davranış kalıplarını analiz etme imkânı sunduğundan, çağdaş istihbarat açısından stratejik bir değer taşımaktadır[280]. Bu nedenle veri akışı, yalnızca ekonomik büyümenin değil, ulusal güvenliğin de temel unsurlarından biri hâline gelmiştir[281].

Bu gelişmelerle birlikte veri egemenliği kavramı gündeme taşınmıştır. Veri egemenliği, yerleşik bir hukuk terimi olmamakla birlikte; devletlerin ve bireylerin dijital veriler üzerindeki yetki ve kontrol iddialarını ifade etmektedir. Bulut bilişimin yaygınlaşması, verilerin ülke dışındaki sunucularda tutulması ve yabancı istihbarat

---

[276] OECD, "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, 2019, http://dx.doi.org/10.1787/b2023a47-en (1 Şubat 2026), s.31-32.
[277] Kshetri, s. 1; McKinsey Global Institute, s.1, 2.
[278] Irion, *"Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms The (Legal) Relationship Between Individuals And Their Personal Records"*, s.355-357; Irion, *"Government Cloud Computing and National Data Sovereignty",* s.49.
[279] Irion, *"Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms The (Legal) Relationship Between Individuals And Their Personal Records"*, s.349-351.
[280] Avrupa Konseyi, İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü, 2014, https://rm.coe.int/internet-ve-daha-genis-dijital-dunyada-hukukun-ustunlugu-avrupa-konsey/16806daa33 (1 Şubat 2026), s.5.
[281] Yakovleva ve Irion, s.201; Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.234.

erişimi gibi riskler bu kavramı kritik hâle getirmiştir[282]. Başlangıçta teknik bir güvenlik sorunu olarak ortaya çıkan bu kavram, zamanla hangi verilerin kimler tarafından, hangi yargı alanında ve hangi meşruiyetle işleneceği sorularını kapsayan geniş bir yönetişim meselesine dönüşmüştür[283].

Bir görüşe göre veri üzerindeki kontrol, mülkiyet ve hak iddiaları farklı aktörlere (bireylere, şirketlere, toplumlara ve devletlere) dağılmıştır. Bu çoklu aktörlük, birbiriyle çelişen egemenlik iddialarını doğurur. Veri egemenliği bir güç potansiyelidir; ancak bu güç otoriter denetimden ziyade müzakere, katılım ve temel haklar çerçevesinde düşünülmelidir. GDPR gibi Avrupa'nın hak temelli veri yönetişimiyle uyumlu olan bu yaklaşım; tekelleşmeye karşı veri üzerindeki kontrolün devlet egemenliği-şirket çıkarları-bireylerin hakları arasında dengelenmesini savunur. Bu nedenle, klasik "tek egemen" anlayışının verinin çok katmanlı doğası karşısında çözüldüğü iddia edilmiştir[284].

Bu tahrik edici önermeyi unutmadan; bulut hizmetlerinin ulus aşan ve dinamik yapısı, veri üzerindeki kontrolü hizmet sağlayıcı ile kullanıcı arasında bölerek devletlerin ulusal egemenlik kapasitesini zayıflattığı gerçeğini kabul etmek gerekir[285]. Dijital delillerin ve kamuya ilişkin verilerin artık başka ülkelerde depolanması, hakimiyetini aynı zamanda kamu kayıtları üzerinden işleten devletin geleneksel egemenlik anlayışının işlerliğini sorgulatmaktadır. Bu nedenle birçok ülke, verilerini yerel altyapılarda tutmaya yönelerek dijital egemenliğini yeniden tesis etmeye çalışmaktadır.

Bununla birlikte, kamu hukuku açısından "veri egemenliği" kavramsal olarak sorunludur. Çünkü egemenlik, modern devlete özgü, olgunlaşmış bir meşruiyet ve yetki biçimini ifade eder. Oysa dijital alanda söz konusu olan, devletler, şirketler ve bireyler arasında süregelen ve henüz normatif olarak istikrara kavuşmamış bir güç mücadelesidir. Bu nedenle burada, verinin üzerinde kurulan fiilî denetim ilişkilerini ifade eden "veri üzerinde iktidar" kavramı daha isabetlidir.

---

[282] Vivek Kundra, Federal Cloud Computing Strategy, **The White House,** Washington D.C., 2011. s. 30.
[283] Irion, *"Government Cloud Computing and National Data Sovereignty",* s.50.
[284] Patrik Hummel ve Diğerleri, "Data sovereignty: A review", **Big Data & Society,** Vol.8, No.1, 2021, s.15.
[285] U.S. Department of Commerce National Institute of Standards and Technology, s.2.

Sonuç olarak veri akışı küresel, hareketli ve sınırsızdır; ancak bu akışı yöneten altyapılar ve karar mekanizmaları belirli şirketlerin ve devletlerin elinde yoğunlaşmaktadır. Ulus-devletin coğrafi egemenliği, dijital akışın mekânsız doğasıyla giderek daha fazla çatışmaktadır. Bu nedenle Herakleitos'un akış metaforu, dijital çağda verinin yarattığı egemenlik krizini anlamak için güçlü bir analitik çerçeve sunmaktadır: Akış süreklidir, fakat bu akışın kim tarafından ve nasıl yönetildiği, dijital çağın temel siyasal sorusudur.

B. Küreselleşmiş Kitlesel Medya ve İletişimin Dönüşümü

İletişim, teknolojik gelişim ve kültürel ilerlemenin temel aracıdır; doğru, özgür ve güvenilir bilgi toplumsal refahı artırırken bireysel özgürleşmeye katkı sağlar[286]. Dijital iletişim devrimi, yazılı, sözlü ve görsel iletişim biçimlerini tek bir ağda bütünleştirerek kültürü ve gerçeklik algısını sanal zeminlerde köklü biçimde dönüştürmüştür[287]. Ağ temelli bu yapı, yüksek etkileşim yoğunluğunu taşıyabilen, esnek ve uyarlanabilir bir iletişim düzeni yaratmıştır[288].

Castells'e göre küresel ağlar, iletişimi eşzamanlı ve çok yönlü hâle getirerek yalnızca teknik değil, kültürel bir dönüşüm üretmiştir; zira medya biçimleri değiştikçe kültürün içeriği ve gerçeklik algısı da değişir[289]. Televizyonun tek yönlü ve homojenleştirici kitle kültürünün yerini, etkileşimli ve kişiselleştirilmiş küresel bir iletişim düzeni almıştır[290]. Buna karşılık Hardt ve Negri, çağdaş siyasetin "gösteri" alanında yürüdüğünü; medyanın artık yalnızca aktaran değil, doğrudan biçimlendiren bir manipülasyon aygıtına dönüştüğünü savunur. Bu ortamda politika içerikten çok imaj ve zamanlanmış görünürlükle yürür; kolektif siyasal özne parçalanırken bireyler seyircileşir. Korku, haz ve arzu üzerinden kurulan bu tahakküm, Hobbes'un korkunun düzen kurucu

---

[286] Serkan Bulut, s. V.

[287] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.42.

[288] Marie-Pierre Granger ve Kristina Irion, "The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection", ***European Law Review***, Vol.39, No.6, (2014), s.835.

[289] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.440-441, 499.

[290] Gürol Demirkan, "Blokzincir Teknolojisi ve Teknolojik Determinizm Çerçevesinde Toplumsal Değişime Etkileri" (**Yüksek Lisans Tezi,** İstanbul Medipol Üniversitesi SBE, 2021), s. 26; Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.450, 485-486.

rolüne ilişkin tespitlerini güncel bir bağlamda yeniden üretir. Gösteri hem tüketim hazzı hem de güvensizlik üretimi yoluyla bireyleri disipline eder[291].

Milton L. Mueller'e göre dijitalleşme iletişimi genişletmiş, biçimsel olarak merkezsizleştirmiş ve devleti; iletişim ve bilgi politikalarını yeniden düşünmeye zorlamıştır. İnternet içerikleri (sosyal medya paylaşımlarından videolara, reklamlardan mesajlaşmaya kadar) gündelik yaşamın her alanına yayılmış; bireyleri bilgi aktarımı, paylaşım, sosyalleşme, alışveriş, eğitim ve eğlence gibi çok çeşitli nedenlerle sürekli çevrim içi kalmaya yönelten geniş bir dijital ekosistem oluşturmuştur[292]. Dijitalleşme; bilgiye erişimi hızlandırmış, iletişimi kolaylaştırmış[293] ve katılımı artırmış olsa da mahremiyet ihlalleri, veri temelli gözetim, dezenformasyon, dijital bağımlılık ve manipülasyon gibi ağır riskler doğurmuştur. Bu nedenle iletişim verilerine ilişkin hukuk politikası, güvenlik ile temel haklar arasında hassas bir denge kurmak zorundadır.

Sonuç olarak dijitalleşme, iletişimi kısmen demokratikleştirirken aynı anda bilgi üzerindeki güç yoğunlaşmasını derinleştirmiş; manipülasyon kapasitesini artırarak kamusal alanı yeniden şekillendirmiştir. Byung-Chul Han'ın belirttiği üzere enformasyonun artışı, olgusallık bilincini zayıflatmakta ve bir güvensizlik toplumu üretmektedir[294]. Bu durum, Platon'un mağara alegorisini andıran yeni bir dijital tutsaklığa işaret eder: Hakikat geri çekilirken, enformasyonun gürültüsü gerçeğin üzerini örtmektedir[295].

---

[291] Hardt ve Negri, *İmparatorluk,* s.332-333.
[292] Milton L. Mueller, **Networks and States: The Global Politics of Internet Governance,** Massachusetts: MIT Press, 2010, s.307-308.
[293] İbrahim Demir ve Fatih Cemil Özbuğday, "Siber Güvenlik Bağlamında Sosyal Medya Platformları Ekonomisi ve Endüstriyel Organizasyonu", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya,** içinde (10-17), Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, Vol.Ocak, Sayı.9, s.11.
[294] Han, s.53-54.
[295] Han, s.60.

C. Blok Zincir (Blockchain) Teknolojileri: Kripto Para, NFT ve Akıllı Sözleşme

Blok zincir teknolojisi, bilgi ve işlemlerin merkezi bir otoriteye ihtiyaç duyulmadan dağıtık ağlarda kaydedilmesini sağlayarak dijital dünyada köklü bir dönüşüm yaratmıştır. Satoshi Nakamoto'nun 2008 tarihli çalışmasıyla gündeme gelen bu teknoloji; kripto paralar, NFT'ler, akıllı sözleşmeler ve DAO'lar aracılığıyla finans, hukuk, ekonomi ve yönetişim alanlarında hem yeni imkânlar hem de ciddi riskler üretmiştir.

Değiştirilemez ve şeffaf bir dijital defter olarak işleyen blok zincir[296] işlemleri merkezi denetime gerek olmaksızın eşzamanlı biçimde kaydederek güvene dayalı bir dijital özerklik alanı oluşturur. Bankacılık, kimlik doğrulama ve kamu hizmetleri gibi alanlarda merkezi yapılara bağımlılığı azaltma; e-devlet uygulamaları ve seçim sistemlerinde güvenilirliği artırma potansiyeline sahiptir[297]. Bununla birlikte denetimsizliğe elverişli yapısı, kripto varlıkların yasa dışı faaliyetlerde kullanılmasına ve devletlerin düzenleyici kapasitesinin aşınmasına yol açarak ulusal güvenlik bakımından yeni tehditler de doğurmaktadır.

Blok zincire dayalı kripto paralar, ulusal para politikalarını ve klasik finansal sistemleri dönüştürme potansiyeli taşır. Düşük maliyetli, hızlı ve görece anonim transfer imkânı sunmaları cazip olsa da[298] hukuki statüleri, vergilendirme rejimleri, kayıt yükümlülükleri, ceza ve miras hukuku bakımından ciddi belirsizlikler barındırmaktadır[299].

---

[296]. Merriam-Webster, "blockchain", https://www.merriam-webster.com/dictionary/blockchain (E.T.: 14.12.2024).

[297] Ekin Sökmen Güler, "Uluslararası Özel Hukuk Boyutuyla Sınır Aşan NFT (Non-Fungible Token) Uyuşmazlıklarının Çözümünde Karşılaşılan Sorunlar ve Uyuşmazlık Çözüm Yöntemlerine İlişkin Öneriler", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Katip Çelebi Üniversitesi, 15-16 Aralık 2022, s.196.

[298] Mehmet Bahadır Polat, "Blokzincir Üzerinde Bulunan 'Mixer' Protokollerinde Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Fiili Bağlamında Objektif İsnadiyet Değerlendirmesi", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.52.

[299] Emine Sevcan Artun, "Kripto Madenciliği Sonucunda Ortaya Çıkan Enerji Tüketiminin Azaltılmasına Yönelik Mali Düzenleme Önerileri", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Katip Çelebi Üniversitesi, 15-16 Aralık 2022, s.144.

NFT'ler yani nitelikli fikrî tapular, benzersiz dijital varlıkların mülkiyetini blok zincir üzerinde kayda bağlayarak fikrî mülkiyet alanında yeni olanaklar sunar. Dijital sertifikalar yoluyla mülkiyetin devri ve ispatı kolaylaşmakta; sanat eserlerinden dijital koleksiyonlara kadar geniş bir kullanım alanı ortaya çıkmaktadır. Ancak sınır ötesi nitelikleri, yetki ve uygulanacak hukuk sorunlarını da beraberinde getirmektedir[300].

Akıllı sözleşmeler, belirlenen koşullar gerçekleştiğinde otomatik olarak çalışan ve dış müdahaleye karşı dirençli dijital sözleşmelerdir. Aracıları ortadan kaldırarak maliyetleri düşürür, süreçleri hızlandırır ve şeffaflığı artırır[301]. DAO'lar ise akıllı sözleşmelerle yönetilen, merkeziyetsiz ve çevrimiçi otonom organizasyonlar olarak[302] katılımcılara doğrudan yönetime katılma imkânı sunar; şirketleşme, fonlama ve yönetişim modellerinde bürokrasi dışı yeni deneyler ortaya koyar[303].

Blok zincir teknolojisi yalnızca devlete karşı geliştirilen bir alternatif değildir; devletler tarafından da egemenliği güçlendiren bir araç olarak kullanılmaktadır. Özellikle Çin, bu teknolojiyi gözetimi artırmak, yerli sanayiyi desteklemek ve küresel rekabette stratejik avantaj sağlamak amacıyla devlet politikalarına entegre etmiştir[304].

Öte yandan kripto para madenciliğinin yüksek enerji tüketimi ve karbon salımı ciddi çevresel maliyetler doğurmaktadır. Bu nedenle madencilik faaliyetlerinin vergilendirilmesi, yenilenebilir enerjiye yönlendirilmesi ve mevzuat boşluklarının

---

[300] Aydıner Karaturp ve Nüket Evrim "Nitelikli Fikri Tapu (NFT) ve Telif Hakkı", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.412; Sökmen Güler, s.196.

[301] Remzi Demir, "Konut ve Çatılı İşyeri Kira Sözleşmelerinde, Akıllı Sözleşme Sisteminin Uygulanabilirliği", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.330-331.

[302] Hakan Dönmez, "Şirketin Doğasına İlişkin Teorilere Göre DOA'ların (Merkezsiz Özerk Kuruluş) Konumu", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.395.

[303] Mete Tevetoğlu, "DAO'nun Genel Olarak Hukuk Sistemine; Özel Olarak İse Ticaret Hukukuna Etkileri", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.405-406.

[304] Alice Ekman, "China's Blockchain and Cryptocurrency Ambitions: The First-Mover Advantage", *European Union Institute for Security Studies,* 13 Temmuz 2021, https://www.iss.europa.eu/content/chinas-blockchain-and-cryptocurrency-ambitions#_introduction/ (1 Şubat 2026); Mercy A. Kuo, "China in Blockchain, Web3, and the Metaverse: Insights from Winston Ma", *The Diplomat,* 5 Aralık 2022, https://thediplomat.com/2022/12/china-in-blockchain-web3-and-the-metaverse (1 Şubat 2026).

giderilmesi, blok zincir ekosisteminin sürdürülebilirliği açısından zorunlu görünmektedir[305].

D. Robotik ve Otonom Sistemler

Robotik ve otonom sistemlerin gelişimi; insan müdahalesi olmaksızın analiz yapabilen, karar alabilen ve ölümcül eylemler gerçekleştirebilen yapay zekâ destekli teknolojileri ortaya çıkarmıştır. Bu durum, savaş hukukunu kökten dönüştürmekte; sorumluluk, hesap verebilirlik ve suçun unsurları gibi temel hukukî kavramları belirsizleştirmektedir. Özellikle ölümcül otonom silah sistemleri, hedef seçme ve imha kararını insan denetimi olmadan alabilmeleri nedeniyle ciddi etik ve hukukî sorunlar doğurmaktadır. Sorumluluğun operatör, yazılımcı, üretici, askerî komutan veya devlete mi ait olduğu açık değildir[306].

Otonom sistemler kapsamında değerlendirilebilecek insansız hava araçları, istihbarat toplama işlevinden aktif saldırı kapasitesine evrilerek savaşın doğasını değiştirmiştir. Düşük maliyetli ve düşük riskli güç kullanımını mümkün kılan bu sistemler, askerî müdahaleyi teknik olarak kolaylaştırmakta; ancak savaş kararlarının eşiğini düşürerek asimetrik riskler ve derin etik ikilemler üretmektedir[307].

Tam otonom silahların geliştirilmesi, kamuoyunda "katil robotlar" tartışmasını gündeme taşımıştır. İnsan kontrolü olmaksızın ateş yetkisi taşıyan bu sistemler, uluslararası insancıl hukukun temel ilkeleriyle doğrudan çatışma riski barındırmaktadır. Bu bağlamda, Cenevre Sözleşmeleri'nin 1977 tarihli Ek Protokol I'de yer alan Martens Maddesi[308] açıkça düzenlenmemiş silah teknolojilerinin değerlendirilmesinde insanlık ilkeleri ve kamu vicdanı ölçütlerini esas alan tamamlayıcı bir norm işlevi görmektedir[309].

---

[305] Artun, s. 144-145.

[306] Berkant, Akkuş, "Yapay Zekâ Tarafından İşlenilen Savaş Suçlarında Yazılımcının Sorumluluğu", editörler Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (623-648), Ankara: Adalet, 2023, s.623.

[307] Cansu Ulu, "İnsansız Hava Sistemleri ve Hedef Gözeterek Öldürme", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.160-161.

[308] International Committee of the Red Cross (ICRC), Martens Clause (glossary), 2024, https://casebook.icrc.org/a_to_z/glossary/martens-clause (E.T.: 14.12.2024).

[309] Nazan Yeşilkaya, "Ölümcül Otonom Silah Sistemleri, Savaş Etiği ve Hukuk", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.175.

Tam otonom silahların hedef seçme ve saldırı kararlarını insandan bağımsız şekilde alması, ayırt etme, orantılılık ve askerî gereklilik ilkelerinin uygulanabilirliğini ciddi biçimde tartışmalı hâle getirmektedir.

Makine temelli karar süreçlerinin siviller ile savaşçılar arasındaki ayrımı her somut durumda doğru biçimde yapabileceği konusunda güçlü şüpheler bulunmaktadır. Bu nedenle robotik ve otonom sistemler, yalnızca savaş hukukunu değil; egemenlik anlayışını, savaşın meşruiyetini ve uluslararası düzenin normatif temellerini de sarsan bir dönüşüm yaratmaktadır. Bu teknolojilerin hukukî statüsü ve sınırları, 21. yüzyılın en kritik ve acil normatif tartışma alanlarından biri hâline gelmiştir.

V. DİJİTAL ALANIN AKTÖRLERİ: DEVLETLER VE DİĞERLERİ

A. Devletler: Egemenin Dijital Bir Aktör Olarak Ağ ve Bilgi Toplumunu Hakimiyet Altına Alma Çabası

1. Dijital Alanda Kontrol ve Hakimiyet: Zorunluluklar

Antik siyasal düşüncede devlet, rastlantısal bir güç ilişkisi değil; akıl yoluyla kavranabilir zorunlu bir düzen olarak ele alınmıştır. Platon, idealar dünyası ile duyular dünyası arasındaki ayrımı kurarken devleti adalet ideasının somutlaşmış biçimi olarak düşünmüş; siyasal düzeni matematiksel kesinliğe yaklaşan bir akıl yürütmenin ürünü saymıştır[310]. Benzer biçimde Aristoteles de devleti, erdemli yaşamın gerçekleşmesini sağlayan teleolojik bir ilkeye bağlamıştır. Her iki düşünürde de devlet, belirli bir temel düşüncenin kurumsal ifadesidir[311].

Hobbes da devleti seküler aklın ürünü olarak konumlandırmış; siyasal düzen ile matematiksel kesinlik arasında doğrudan bir ilişki kurmuştur. Bugün ise matematik, yalnızca devleti açıklayan bir araç olmaktan çıkmış; algoritmalar ve veri analitiği

[310] Uygun, s.117.
[311] Doehring, s.5.

aracılığıyla devletin işleyişini aşan yeni bir zamansal ve mekânsal evren yaratmıştır. Dijital dönüşüm, bir yandan devletin hukukuna tabi teknolojileri üretirken, diğer yandan devlet egemenliğini aşındıran siber ve platform temelli güç yapılarını ortaya çıkarmıştır. Bu durum, gündelik hayatın her yönünü kuşatan ve toplum üzerinde zor kullanma gücünü elinde tutan merkezileşmiş bir siyasal örgütlenme[312] olan devletin dijital alanda kontrol ve hâkimiyet kurma yönündeki çabalarının ekonomik, toplumsal, tarihsel, hukuki ve demokratik gerekçelerini ve devletin kullandığı araçların gerekliliği ve kaynakların yönetimini incelemeyi gerektirir.

Küreselleşme sonrası dijital teknolojiler, devlet egemenliğinin sınırlarını belirsizleştirmiştir. Algoritmalar, platform ekonomileri ve küresel teknoloji şirketleri dijital alanı çok aktörlü bir güç mekânına dönüştürmüştür. Büyük teknoloji şirketlerinin klasik diplomatik aktörler gibi muhatap alınması, dijital şirket yöneticilerinin/sahiplerinin devlet yönetiminde fiilî etki kazanması ve platformların uluslararası norm belirleyici hâle gelmesi bu dönüşümün sembolik göstergeleridir. Bu bağlamda temel soru, devletin dijitalleşme karşısında etkisizleşip etkisizleşmediği değil; egemenliğini hangi araçlarla ve hangi sınırlar içinde yeniden kurmaya çalıştığıdır.

Karl Doehring'e göre, iradi ve ahlaki değerlere dayanan somut bir devlet hedefi varsa o zaman devlet kuramıyla uğraşılan bilim dalında, bu amacın hangi örgütle nasıl gerçekleştirileceği konusu araştırılabilir. Bu çalışmayı yapabilmek için iki bilgi aracına gereksinim vardır: gözlem ve mantık. Devlet kuramının görevi, devletin hedefi doğrultusunda bundan doğacak bilimsel sonuçları göstermektir[313]. Bu çerçevede devletler, dijital aktörleri hangi ölçüde ve hangi gerekçelerle muhatap aldıklarını açıkça ortaya koymak zorunda kalmaktadır. Bu durum, egemenliğin sınırlarını bulanıklaştırırken devletin müdahale araçlarının, karşı karşıya kaldığı risklerin ve ortaya çıkan paradoksların ayrıntılı şekilde analiz edilmesini gerekli kılar.

Devlet, neden dijital alanda kontrol ve hakimiyet kurma ihtiyacı duymaktadır? Devletin dijital alana müdahalesini zorunlu kılan gerekçeler başlıca ekonomik, siyasal ve

[312] Uygun, s.1.
[313] Doehring, s.5.

güvenlik boyutlarında ortaya çıkmaktadır. Dijital çağda veri, yalnızca bilgi değil; stratejik bir üretim girdisi ve egemenlik aracıdır. Geçmişte artı ürünün siyasal yapıların oluşumundaki rolü neyse, bugün de veri dijital artı değer olarak toplumsal değer zincirinin merkezine yerleşmiştir. Özel platformlar eliyle metalaştırılan veri, halktan çekilen yeni bir artı-değere dönüşmüş; bu durum, devletin veriyi koruma ve düzenleme sorumluluğunu tarihsel bir zorunluluk hâline getirmiştir. Veri, ulusal nitelikte bir kamusal değer olarak görülmeli; tekelci platform birikimine ve yabancı denetime karşı devlet koruyucu güç rolünü üstlenmelidir.

Veri temelli düzenin yükselişi, siyasal iktidar açısından yeni bir güç alanı yaratmıştır. Dağınık ve çok merkezli görünen bu mimaride iktidar boşlukları kalıcı değildir. 21. yüzyılda siyasal yapılar, veriyi anlamlı bir yönetişim kapasitesine dönüştüremezlerse yerlerini daha etkin yapılara bırakmak zorundadır. Bu yapıların demokratik ya da otoriter olması ikincil; asıl belirleyici olan, önceki siyasal formlarla kıyaslanamayacak ölçüde yeni bir egemenlik biçimini temsil etmeleridir. Bu bağlamda temel soru, bu yapıları kimin inşa edeceği ve kimin denetleyeceğidir[314]. Bu bağlamda algoritmik regülasyon, hukukun metin merkezli yapısından veri ve algoritma merkezli bir yönetişim anlayışına geçişin zorunlu bir cephesidir[315].

Başlangıçta internetin özgürleştirici ve hiyerarşiyi ortadan kaldıran bir alan olacağı iddia edilmişti. Ancak ortaya çıkan yapı, demokratik meşruiyetten yoksun, oy hakkı bulunmayan fakat yönetsel güce sahip yeni iktidar odakları üretmiştir[316]. Büyük teknoloji şirketlerinin ekonomik güçleri, teknolojik kapasiteleri ve siyasal etkileri; devlet-şirket gerilimini niteliksel olarak yeni bir düzeye taşımıştır. Bu nedenle dijital alan, devlet açısından yalnızca ekonomik bir sektör değil; egemenliğin icrası ve hukukun üstünlüğünün korunması bakımından düzenlenmesi zorunlu bir kamusal alan hâline gelmiştir[317].

---

[314] Yuval Noah Harari, **Homo Deus: Yarının Kısa bir Tarihi,** Poyzan Nur Taneli (çev.), İstanbul: Kolektif Kitap, 2016, s.394.
[315] Erol, s.44.
[316] Lehdonvirta, s.4.
[317] Susana Coroado, "Leviathan vs Goliath or States vs Big Tech and What the Digital Services Act Can Do About It", **Forum Transregionale Studien,** No. 25/2023, https://doi.org/10.25360/01-2023-00038, 2023, s.5-6.

Dijital çağın çok merkezli (polycentric) ve sınır aşan doğası, devletlerin tek başına etkili düzenleme yapma kapasitesini sınırlandırmaktadır. Rekabet, vergilendirme, sınır aşan suçlar ve standartlar gibi alanlarda ulusal düzenlemeler yetersiz kalmakta; bağlayıcı uluslararası hukuk kurallarını gerekli kılmaktadır. Jeopolitik güç artık sadece devletin tekelinde değildir; teknoloji şirketleri, teknik topluluklar ve sivil toplum ağları gibi devlet dışı aktörler de etkili güç merkezleri hâline gelmiştir[318].

Timmers'e göre, liberal perspektif, uluslararası düzenin yalnızca devletlerden oluşmadığını; uluslararası örgütler, özel sektör, sivil toplum ve küresel teknoloji topluluğu gibi çok sayıda aktörün de küresel ilişkilerde belirleyici olduğunu savunur. Dijital düzende, uluslararası sistemin çok aktörlü ve ağsal bir yapıya evrilmesi, devlet dışı yapıları da egemenlik ilişkilerinde belirleyici aktör hâline getirmektedir. Bu yeni yapı, bazen fiilen (de facto), bazen hukuken (de jure) ekonomi, toplum ve demokrasi üzerinde belirleyici güce sahip yeni merkezler yaratmaktadır[319]. Fakat Big Tech şirketleri, veri üzerinde fiilî egemenlik kurmuş olsalar da meşru siyasal otorite iddiası hâlâ devlete aittir; şirketler dijital alanda egemen olarak henüz tanınmamıştır[320].

Veri ekonomisinin büyük ölçüde özel sektörün elinde olması, bilgi asimetrilerini derinleştirmekte; devletin şeffaf, güvenli ve hak temelli veri piyasaları oluşturma kapasitesini zorlaştırmaktadır. Veri ticareti ve paylaşımı alanında etkili bir düzen kurulamaması hem bireysel hakların korunmasını hem de kamu yararının gerçekleştirilmesini güçleştirmektedir[321]. Yapay zekâ gibi yükselen teknolojiler; ekonomik büyüme, rekabet gücü ve ulusal güvenlik açısından stratejik önem taşımaktadır[322]. Ancak teknolojik gelişmelerin hızı karşısında hukuki düzenlemeler geri kalmakta; bu da algoritmik ayrımcılık, kültürel tekdüzelik ve küçük işletmelerin rekabet gücünü kaybetmesi gibi ciddi riskler doğurmaktadır. Dijital teknolojilerin denetimi, veri güvenliği, mahremiyetin korunması, dezenformasyonla mücadele ve ulusal dijital

---

[318] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.129.
[319] Timmers, *"Sovereignty in the Digital Age",* s.573-575.
[320] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.15.
[321] Balázs Bodó ve Diğerleri, "Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks", **Internet Policy Review,** Vol.10, No.3, (2021), s.4.
[322] Gloria Özdemir, "Artificial Intelligence 'Arms Dynamics': The Case of the United States and China Rivalry", (**Doktora Tezi**, Ankara Yıldırım Beyazıt Üniversitesi SBE, 2024), s.53.

sınırların tesisi gibi başlıklar, devletleri daha sıkı bir egemenlik inşasına yöneltmektedir[323]. Machiavelli'ye göre bir devletin bekası ve sağlamlığı, dua ile değil hukuki düzeni temsil eden "iyi yasalar" ile fiziksel gücü ve güvenliği temsil eden "iyi ordular" arasındaki kopulmaz bütünlüğe dayanır[324]. Bu yüzden, ortaya çıkan çok aktörlü ve belirsiz dijital yapı, devlet için açık bir zorunluluk yaratır: Dijital alanın düzenlenmesi ve güç denetiminin yeniden tesisi. Devletlerin bu alanlardaki denetim ve yönlendirme kapasitesini artırması; ekonomik, demokratik ve toplumsal istikrar açısından zorunlu hâle gelmektedir[325].

Anayasa Mahkemesi'nin de vurguladığı üzere, internetin küresel ve dağınık yapısı klasik egemenlik araçlarını zorlamakta; ancak bu durum dijital alanın sınırsız bir özgürlük alanı olduğu anlamına gelmemektedir[326]. Kamu düzeninin korunması, dijital suçlarla mücadele, kişisel verilerin korunması ve ifade özgürlüğünün dengeli sınırlandırılması devletin anayasal sorumlulukları arasındadır. Dolayısıyla dijital egemenlik, teknik bir kontrol meselesi değil; hukuk devleti ilkesi ve temel haklarla dengelenmiş bir anayasal görev olarak ortaya çıkmaktadır.

Peki, devlet müdahalesinin meşruiyeti neye dayanmaktadır? Dijitalleşme, klasik egemenlik kuramında kırılmalar yaratmakla kalmamış, aynı zamanda devletin dijital alana yönelik müdahalesinin hukuki ve normatif meşruiyetini yeniden inşa etmesini zorunlu kılmıştır.

Egemenlik kuramı, modern devlete kendi sınırları içinde en yüksek ve bölünmez otoriteyi atfetmiştir. Modern devlet, yasama-yürütme-yargı tekelini, kamu düzenini sağlama görevini ve toplumu koruma yükümlülüğünü bu ilkeye dayanarak sürdürür; bu nedenle dijitalleşen dünyada devlet müdahalesi bir tercihten çok, egemenliğin yapısal gereğidir. Keza Akal'ın da belirttiği üzere, uluslararası hukukta genelde tüm insanlığa

---

[323] Eren, s.561.

[324] Rukiye Akkaya Kia, "Post Modern Zamanlarda Machiavelli Okumak," **Doç. Dr. Melike Batur Yamanerin Anısına Armağan** içinde (121-127), İstanbul: Galatasaray Üniversitesi Hukuk Fakültesi, 2014, s.123, 125.

[325] Altın Aslı Şimşek Öner, "Siber-Alanda Devlet Kudretine Bir Bakış: Dijital Egemenlik Kavramı", **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.155.

[326] AYM, 15/11/2017, E. 2015/76, K. 2017/153, Karşı Oy Gerekçesi, par. no. 12, https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/153

özgü olsa da her siyasi iktidar tipinin ya da devletin, onu kendi özel koşullarına uyarlama yetkisi bulunur[327]. Çünkü devlet, toplumu düzenleyen, bireyleri koruyan, kamu düzenini sağlayan ve uluslararası alanda ülkeyi temsil eden biricik siyasal güçtür. Dijitalleşen dünyada devletin düzenleyici kapasitesinin artması, bizzat bu egemenlik anlayışının doğal ve zorunlu bir uzantısıdır[328]. Bu zorunluluk, devlet müdahalesini tercihe değil, egemenliğin yapısal bir gereğine dönüştürür. Devletin dijital alana müdahalesi, yalnızca teknik bir kontrol arayışı değil, egemenliğin dijital araçlarla yeniden biçimlendirildiği daha derin bir siyasal evrimin parçası olduğunu gösterir. Egemenlik, devlet müdahalesinin normatif meşruiyetini doğrudan sağlarken; dijital alanın çok aktörlü ve sınır aşan niteliği, bu otoritenin pratikte nasıl kullanılacağına ilişkin yeni sorunlar ve gerilimler doğurmaktadır.

AYM; dijital düzenlemelerin meşruiyet sınırlarını çizerken internetle ilgili yasal müdahalelerin adalet, hakkaniyet ve kamu yararı ilkelerine dayanması gerektiğini vurgulamış ve böylece devletin bu alandaki düzenleyici gücünün sınırsız olamayacağını belirtmiştir[329]. Özellikle dijital suçlarla ve ulusal güvenliğe karşı içeriklerle mücadele, kişisel verilerin korunması ve ifade özgürlüğünün dengeli biçimde sınırlandırılması gibi başlıklarda devletin sorumluluğu açık biçimde belirmektedir. AYM'nin, internetin doğası gereği devletlerin klasik egemenlik araçlarını uyarlamak zorunda kaldığını kabul etmesi; hak ve özgürlüklerin korunmasının bu düzenlemelerin merkezinde olması gerektiği anlamına gelir. Bu yaklaşım, AYM'nin dijital egemenlik mücadelesinde devletin rolünü salt teknik bir kontrol meselesi olarak görmediğini; meşruiyet, hukuk devleti ve hak dengesi ekseninde değerlendirdiğini ortaya koyar. Doktrinde de algoritmik sistemlerin hem özel sektöre yönelik hem de idarece kullanımında ve regülasyon faaliyetlilerinde kamu düzeninin tesisi, kamu yararının gerçekleştirilmesi, şeffaflık ve hesap verilebilirlik ilkelerini sağlamada devletin temel zorunluluğu işaret edilmiştir[330]. Böylece dijital egemenlik hem kamu yararı ve düzenini koruma hem de bireysel özgürlükleri güvence

---

[327] Cemal Bali Akal, **Modern Düşüncenin Doğuşu: İspanyol Altın Çağı,** 7. Baskı, Ankara: Dost Kitabevi Yayınları, 2013, s.241.
[328] Andrew Linklater, **Critical Theory and World Politics**, London: Routledge, 2007, s.107.
[329] AYM, 8/12/2015, E.2014/87, K.2015/112, T., par. 133-135. https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/112?EsasNo=2014%2F87
[330] Erol, s.155.

altına alma yükümlülüklerinin birlikte yürütülmesini gerektiren çift yönlü bir anayasal sorumluluk olarak tanımlanır.

Uluslararası normlar ve çok taraflı yönetişim ilkeleri, dijital alanın yönetiminde insan haklarına dayalı, çoğulcu bir yapıyı öngörse de mevcut uygulamalar bu ideallerden büyük ölçüde sapmaktadır. Kritik dijital altyapıların hâlâ ABD merkezli şirketlerce kontrol ediliyor oluşu, küresel dijital yönetişimin adalet ve egemenlik ilkeleriyle çelişen bir biçimde işlediğini göstermektedir. Özellikle Snowden ifşaları bu kontrolün kitlesel gözetim amacıyla da kullanıldığını göstererek, devletlerin interneti millîleştirme veya bölgeselleştirme eğilimlerini tetiklemiş ve küresel ağın parçalanması riskini artırmıştır[331]. Çıkar amacıyla hareket eden özel şirketler, klasik anlamda kamu gücü kullanma yetkisi olmadığından uluslararası insan hakları hukukunun doğrudan muhatabı değildirler; bu alan esasen devletlere yükümlülükler yükler. Öte yandan, ulusal düzeyde getirilen düzenlemeler ise bazı durumlarda ifade özgürlüğü ve mahremiyet gibi temel hak ve özgürlük standartlarıyla gerilim yaratabilmektedir. Devletlerin suçla mücadele amacıyla bu şirketlerden iş birliği talep etmesi anlaşılır olsa da bu süreçte hem uluslararası insan hakları yükümlülüklerine uyulması hem de diğer devletlerin egemenliklerine saygı gösterilmesi zorunludur. Şirketlerin gönüllü kısıtlama yoluyla kendisini sınırlaması bir yol gibi görünse bile devletlerin sorumluluk almaktan kaçması kabul edilemez; şirketlerin bireylerin haklarına uygun davranma yükümlülüğü ihmal edilemez. Bu nedenle mevcut yönetişim; insan hakları ve egemenlik ilkeleriyle uyumlu değildir ve küresel internetin parçalanma riskini artırmaktadır[332].

Sonuç olarak devletin dijital alana müdahalesi, siyasal bir tercih değil; dijital çağda egemenliğin yapısal bir gereğidir. Bugün yaşanan süreç, şirket temelli fiilî iktidar ile devletin hukuki-siyasal üstünlüğü arasındaki bir ara evreyi temsil etmektedir. Devlet, dijital teknolojileri denetleyebildiği ve hukuki çerçeveye oturtabildiği ölçüde, dijitalleşmeyi kendi egemenlik kapasitesini pekiştiren bir araca dönüştürebilecektir[333].

---

[331] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.7.
[332] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.8.
[333] Sala, s.391-392.

2. Dijital Egemenliğe Devlet Yaklaşımları: ABD, Çin ve AB Perspektifleri

a. Farklılaşan Yaklaşımlar ve Ulusal Stratejiler

Devletlerin dijitalleşmeye yaklaşımları, siyasal rejimleri, ideolojik tercihleri ve ekonomi-devlet ilişkisine dair tarihsel kabulleri doğrultusunda belirgin biçimde farklılaşmaktadır. Dijital altyapının kurulması, veri rejimlerinin şekillendirilmesi ve dijital alanın düzenlenmesi; kimi ülkelerde rekabetçi ve piyasa odaklı, kimi ülkelerde devletçi ve denetim merkezli, kimi ülkelerde ise hak temelli ve düzenleyici modeller üzerinden yürütülmektedir. Bu farklılaşma, dijital uygulamaların demokrasi, bireysel özgürlükler ve kamusal denetim üzerindeki etkileri bakımından devlet tutumlarını karşılaştırmalı biçimde değerlendirmeyi gerekli kılmaktadır.

Castells'in de vurguladığı üzere, tarihsel deneyim açık ve rekabetçi sistemlerin teknolojik gelişmede daha başarılı olduğunu; kapalı ve aşırı merkeziyetçi yapıların ise uzun vadede geri kaldığını göstermektedir. ABD'nin teknoloji politikası, bireysel girişimi ve rekabeti teşvik eden bu açık sistem anlayışına dayanır. Rekabet, inovasyonun temel itici gücü olarak görülmekte; teknolojik ilerleme "bir sonrakini daha iyi icat etme" motivasyonuyla beslenmektedir. Buna karşılık, teknolojiyi sıkı devlet kontrolüne bağlayan ve rekabeti bastıran modeller tarihsel olarak sınırlı başarı göstermiştir[334].

Dijital egemenlik politikaları, devletlerin dijital alan üzerindeki kontrol ve yönlendirme kapasitesini artırmaya yönelik stratejilerinin bir yansımasıdır. Küresel dijital ekosistemin karşılıklı bağımlılık ilişkileri, devletleri farklı veri yönetimi ve düzenleme modelleri geliştirmeye yöneltmiş; veri, ekonomik olduğu kadar siyasal ve ideolojik rekabetin de merkezine yerleşmiştir. Bu bağlamda ulusal veri rejimleri, devletlerin stratejik önceliklerine, hukuki geleneklerine ve kapitalizmin farklı örgütlenme biçimlerine göre çeşitlenmiştir.

Literatürde yaygın kabul gören sınıflandırmaya göre, üç temel yaklaşım öne çıkmaktadır: AB, insan hakları ve veri koruma merkezli bir modeli GDPR, DMA ve DSA

---

[334] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.13.

gibi düzenlemelerle kurumsallaştırmıştır; ABD, sektör bazlı, parçalı ve görece iş dostu bir yaklaşımı benimsemekte; düzenleme yerine rekabet ve inovasyonu öncelemektedir; Çin ise kişisel verilerin ve dijital alanın yönetimini siber egemenlik anlayışı çerçevesinde ele almakta; Sosyal Kredi Sistemi gibi disiplin mekanizmalarıyla dijitalleşmeyi doğrudan siyasal kontrolle ilişkilendirmektedir[335].

Çin, siber egemenlik anlayışını[336] yalnızca ulusal hukukta değil, uluslararası platformlarda da normatif bir ilke olarak savunmakta[337] ICANN ve IANA gibi küresel internet yönetişimi kurumları üzerindeki ABD etkisini sınırlandırmaya çalışmaktadır. Rusya ve Hindistan gibi ülkeler ise kendi DNS altyapılarını geliştirerek internetin sınırlarını millîleştirme yönünde adımlar atmıştır. ABD, küresel internet altyapısını kuran ve büyük teknoloji şirketleri aracılığıyla fiilî kontrolü elinde bulunduran aktör konumundayken[338] AB, dijital egemenliği; insan hakları ve düzenleyici kapasite ekseninde tanımlamaktadır[339].

---

[335] Susan Ariel Aaronson ve Patrick Leblond, "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO", **Journal of International Economic Law,** Vol.21, No.2, (June 2018), s.245-247.

[336] 2004 BM İnternet Yönetimi Çalışma Grubu (WGIG) toplantısında, Çin internet yönetişimi ve ulusal internetin yönetiminin her ülkenin egemenlik alanına girdiğini; devletlerin ve halkların çıkarlarının en iyi şekilde özel sektör ya da sivil toplum aktörlerince değil hükümetler tarafından temsil edilebileceğini ileri sürmüştür. Gianluigi Negro, "China and Global Internet Governance ITU, ICANN, and the World Internet Conference", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (153-170), Maryland: Rowman & Littlefield Publishers., 2023, s.158. Çin'in siber uzayı fiziksel topraklar gibi devlet egemenliğinin parçası olarak tanımlayan Ulusal Güvenlik Yasası, klasik egemenlik anlayışı ile siber egemenliği birleştiren somut bir örnek oluşturur: ***"Madde 25: Devlet, ulusal bir ağ ve bilgi güvenliği koruma sistemi kurar; ağ ve bilgi güvenliğini sağlama kapasitesini geliştirir; ağ ve bilgi teknolojilerinin yenilikçi araştırma, geliştirme ve kullanımını teşvik eder; ağlar ve bilgi sistemleri ile önemli sektörlerdeki altyapılar ve verilerin güvenliğini temin edecek temel teknolojiler ve kritik altyapılar oluşturur; ağ yönetimini güçlendirir; ağ saldırıları, siber sızmalar, siber hırsızlık ve yasadışı ya da zararlı içeriklerin yayılması gibi eylemleri önler, durdurur ve hukuka uygun şekilde cezalandırır; siber uzaydaki egemenlik, güvenlik ve kalkınma çıkarlarını korur."*** China Law Translate, National Security Law of the People's Republic of China (2015), 2015, https://www.chinalawtranslate.com/en/2015nsl/ (E.T.: 14.12.2024).

[337] Konstantinos Komaitis ve Justin Sherman, "The ITU election pitted the United States and Russia against each other for the future of the internet", *Atlantic Council,* 29 Eylül 2022, https://www.atlanticcouncil.org/uncategorized/the-itu-election-and-the-future-of-the-internet/ (1 Şubat 2026).

[338] Stuart Biegel, **Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace,** London: MIT Press, 2001, s.355-356.

[339] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.130.

Günümüzde devletler, dijital egemenliği sağlamak amacıyla bütüncül ulusal stratejiler geliştirmektedir. Güney Kore[340] Estonya[341] Singapur[342] Hindistan[343] Birleşik

[340] Güney Kore Dijital Ekonomi Stratejisi: 1990'lardan itibaren Güney Kore, dijitalleşme sürecini hızlı internet altyapısı kurarak başlatmış; bilgi teknolojilerinin eğitim, iş ve kamu hizmetlerinde kullanımını hedefleyen projeler geliştirmiştir. 2000 yılında e-Korea Initiative ile e-ticaretin ve dijital kamu hizmetlerinin yaygınlaştırılması; 2009'da Green IT Policy ile çevre dostu teknolojik kullanım teşvik edilmiştir. 2020'de başlatılan Digital New Deal; yapay zekâ, büyük veri ve bulut bilişim gibi alanlarda dijital altyapının güçlendirilmesi, dijital eğitim ve istihdam olanaklarının artırılması gibi hedefler öngörmüştür. Ministry of Science and ICT, The Digital New Deal Is to Lead Digital Transition in the World After COVID-19, 2021, https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&mId=4&mPid=2&nttSeqNo=443 (14 Aralık 2024).

[341] Estonya Dijital Hükümet Stratejisi: Estonya, 2001'de kamu kurumları arasında veri paylaşımını sağlayan X-Road sistemiyle dijital dönüşümünü başlatmış; ardından 2002'de e-Oturum (E-Residency) programı, 2005'te elektronik oy kullanma (E-Voting) sistemi ve 2008'de tüm sağlık kayıtlarının dijitalleştirildiği Dijital Sağlık Sistemi uygulanmıştır. 2021'de açıklanan Estonian Digital Agenda 2030 ile ileri dijital çözümler ve sürdürülebilir dijital altyapılar öncelikli hedefler arasında yer almıştır. Andra Krasavina, "Estonia - Estonian Digital Agenda 2030", *European Commission (Digital Skills and Jobs)*, 27 Temmuz 2024, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/estonia-estonian-digital-agenda-2030 (14 Aralık 2025).

[342] Singapur Dijital Ekonomi Eylem Çerçevesi: Singapur'un dijitalleşme süreci, 1980'lerde kamu sektörünün dijitalleştirilmesini hedefleyen National Computerisation Plan ile başlamış; 1990'lardaki Akıllı Ada vizyonu ve IT2000 Planı ile ulusal bilgi teknolojisi altyapısı güçlendirilmiştir. 2014'te başlatılan Smart Nation Initiative ile nesnelerin internetine dayalı şehir altyapısı, dijital kamu hizmetleri ve veri analitiği öne çıkarken, 2020'deki Dijital Ekonomi Eylem Çerçevesi işletmelerin dijital dönüşümünü desteklemeyi, vatandaşların dijital becerilerini geliştirmeyi ve veri odaklı yönetimi benimsemeyi amaçlamıştır. Singapore Infocomm Media Development Authority (IMDA), Digital Economy Framework for Action Singapore, 2018, https://www.imda.gov.sg/-/media/imda/files/sg-digital/sgd-framework-for-action.pdf (27 Temmuz 2024).

[343] Hindistan Digital India: 2015'te başlatılan Dijital Hindistan projesi; dijital altyapının geliştirilmesi, e-devlet hizmetlerinin yaygınlaştırılması ve dijital okuryazarlığın artırılmasını hedeflemektedir. DigiLocker, UPI dijital ödeme sistemleri, Aadhaar biyometrik kimlik ve E-Hospital gibi uygulamalarla dijital hizmetler sunulurken; Start-Up Hindistan programıyla yerli inovasyon, kırsal internet altyapısı, kadın girişimciler ve düşük gelirli gruplar desteklenmektedir. Department of Industrial Policy and Promotion, Action Plan, 2016, https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/Action__Plan.pdf (27 Temmuz 2025).

Krallık[344] Türkiye[345] Almanya[346] ve AB[347] örnekleri incelendiğinde; dijital altyapının güçlendirilmesi, veri koruma rejimlerinin kurulması, dijital becerilerin artırılması, KOBİ'lerin dijital dönüşümünün desteklenmesi[348] kırsal alanlarda erişim eşitliğinin sağlanması[349] ve dijital okuryazarlığın geliştirilmesi gibi ortak hedefler öne

[344] Birleşik Krallık Digital Strategy: 2017'de başlayan Birleşik Krallık Dijital Stratejisi, büyük veri ve yapay zekâyı iş ve toplumda etkin kullanmaya, siber güvenliği güçlendirmeye odaklanır; dijital kamu hizmetlerini geliştirmeyi, dijital becerileri artırmayı ve teknoloji şirketleri ile start-up'ları destekleyerek dijital ekonomiyi büyütmeyi hedefler. Karen Bradley, "UK Digital Strategy 2017", *gov.uk*, 11 Eylül 2023, https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy (27 Temmuz 2025).

[345] Türkiye Dijital Devlet Stratejisi: 2018'de Türkiye, dijital ekonomide rekabeti artırmak, dijital altyapı ve güvenliği güçlendirmek, dijital okuryazarlığı yaygınlaştırmak ve kamu hizmetlerini dijitalleştirmek için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi öncülüğünde Dijital Devlet Stratejisi'ni oluşturmuştur. Türkiye Yüzyılı vizyonu çerçevesinde Dijital Türkiye ve Dijital Dönüşüm Hamlesi projeleriyle sürdürülebilir dijital dönüşüm ve rekabet gücü hedeflenmiştir. 11. Kalkınma Planı'nda e-devlet, büyük veri, yapay zekâ, yenilikçi teknolojiler ve siber güvenlik alanlarında politika ve tedbirler yer almaktadır. Kamu kurumları arasında veri standartlarını oluşturmak, ortak veri dilini geliştirmek ve kamu hizmeti alanında büyük verinin kullanımına yönelik Ulusal Veri Sözlüğü çalışmaları sürmekte; bu kapsamda veri standartları ve tanımları belirlenmesi, ulusal veri envanteri hazırlanması ve veri sahipliği ile sorumluluklar netleştirilmesi amaçlanmaktadır. T.C. Sanayi ve Teknoloji Bakanlığı: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ulusal Yapay Zekâ Stratejisi 2021-2025, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZekaStratejisi2021-2025.pdf, (10 Eylül 2025), s.48-49. Aynı çerçevede, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yürütülen Açık Devlet Verisi Portalı (veri.gov.tr) projesi, kamuda üretilen verilerin erişilebilir ve paylaşılabilir hâle getirilmesini amaçlamaktadır. 2021-2025 Ulusal Yapay Zekâ Stratejisi ile yerli yapay zekâ çözümleri geliştirilmekte; Türk Beyin Projesi kapsamında yapay zekâ, beyin tümörü tespiti ve hastalık sınıflandırmasında kullanılırken, Sayısal Göz Projesi ile sağlık alanında yerli yapay zekâ uygulamaları hayata geçirilmektedir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Türkiye'nin dijital dönüşüm hamlesi", https://cbddo.gov.tr/haberler/6588/turkiye-nin-dijital-donusum-hamlesi (14.12.2024).

[346] Almanya: Dijital Strateji 2025: Almanya, 2011'de High-Tech Strategy 2020 ile sanayi üretimini dijital teknolojilerle daha verimli ve entegre hale getirmeyi hedeflemiştir. 2016'da başlayan Dijital Strateji 2025 planıyla dijital altyapı, siber güvenlik, yenilikçi çözümler geliştirilmekte; KOBİ'lerin dijital dönüşümünü desteklemek için danışmanlık ve mali yardım sağlayan Go-Digital programı başlatılmıştır. Māra Jākobsone, "Germany-Digital Strategy 2025", *European Commission (Digital Skills and Jobs)*, 10 Haziran 2025, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/germany-digital-strategy-2025 (14 Aralık 2025).

[347] Avrupa Birliği 2021–2027 Dijital Avrupa Programı: Avrupa Birliği, 2021-2027 yılları arasında yapay zekâ, siber güvenlik, bulut bilişim, veri ve dijital beceriler gibi alanlarda dijital altyapıyı güçlendirmek, dijital dönüşümü hızlandırmak ve yerli teknolojileri geliştirmek için yaklaşık 7,5 milyar Euro bütçeli Dijital Avrupa Programı'nı başlatmıştır. European Commission, The Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme (14 Aralık 2025).

[348] Türkiye'deki dijital dönüşüm programları KOBİ'lerin dijital pazarlama ve veri analizi gibi alanlarda dönüşümünü desteklemektedir. KOSGEB, "KOBİ Dijital Dönüşüm Destek Programı", https://www.kosgeb.gov.tr/site/tr/genel/destekdetay/9144/kobi-dijital-donusum-destek-programi (E.T: 14.12.2024).

[349] Avustralya, Dijital Erişim Stratejisi'ni; Güney Afrika Cumhuriyeti, Ulusal Bağlantı Hedefleri'ni; ABD Tarım Bakanlığı (USDA) çeşitli girişimlerle kırsal internet altyapısını iyileştirerek dijitale erişimlerini artırmak için başlatmıştır. "ABD internet erişimini evrensel hale getirmek için 42 milyar dolar harcayacak", *Gazete Oksijen,* 26 Haziran 2023, https://gazeteoksijen.com/bilim-ve-teknoloji/abd-internet-erisimini-evrensel-hale-getirmek-icin-42-milyar-dolar-harcayacak-182067 (1 Şubat 2026).

çıkmaktadır[350]. Yüksek hızlı internet, siber güvenlik, veri koruma gibi alanlarda altyapıyı güçlendirmekte; dijital becerilerin gelişimini ve e-ticareti desteklemektedirler[351].

Bununla birlikte internetin küresel ve sınır aşan yapısı, devletlerin tek tek birbirinden bağımsız işleyen düzenleme kapasitelerini sınırlamakta; uluslararası iş birliğini zorunlu kılmaktadır. Dijital standartların belirlenmesi[352] etik kullanım ilkelerinin geliştirilmesi[353] ve sınır ötesi dijital hizmetlerin düzenlenmesi[354] ancak çok taraflı mekanizmalarla mümkün olabilmektedir. Bu stratejilerin başarısı hem uluslararası koordinasyonun niteliğine hem de ABD'deki "AI Czar" örneğinde olduğu gibi ulusal kaynakların etkin kullanımına bağlıdır.

Son olarak, devletlerin dijital egemenlik yaklaşımlarını tek bir modele indirgemek yanıltıcıdır. Aynı devlet, farklı politika alanlarında rekabetçi, düzenleyici, paternalist veya otoriter unsurları eşzamanlı olarak benimseyebilmektedir. Dijital politikalar çoğu zaman konjonktürel, pragmatik ve güç dengesi odaklıdır. Bu nedenle bir

---

[350] Avustralya (Dijital Güvenlik Eğitimi Programı) ve Kanada, çocuklar ve ebeveynlere internetin güvenli kullanımı, siber zorbalık ve veri güvenliği hakkında rehberlik sunan online platformlar oluşturmuştur: bkz. Canadian Centre for Child Protection, ProtectKidsOnline.ca https://protectkidsonline.ca/app/en/ (1 Şubat 2026). İngiltere'de Digital Skills Partnership, Avustralya'da Digital Literacy Strategy, Norveç'te Digi-læring, İsveç'te Digital Skills for All ve ABD'de National Digital Literacy Program toplumun her kesimine; Finlandiya Dijital Okuryazarlık Programı, dijital okuryazarlık ve siber güvenlik konularında farkındalık amacıyla öğrencilere ve öğretmenlere yönelik eğitim programları sunmaktadır. Finland Education Hub, Digital Literacy in Finnish Education: A Model for the World, 2023, https://finlandeducationhub.com/digital-literacy-in-finnish-education-a-model-for-the-world/ (1 Şubat 2026).

[351] 2018 AB Dijital Tek Pazar Stratejisi, dijital pazara erişimi ve dijital hizmetlerin uyumlu hale gelmesini sağlamak ve Avrupa dijital ekonomisini büyütmeyi hedeflemektedir. European Council, Digital single market for Europe, 2015, https://www.consilium.europa.eu/en/policies/digital-single-market/ (1 Şubat 2026).

[352] BM İnternet Yönetimi Forumu, Dijital Dünya Forumu, Dünya Ekonomik Forumu ve OECD Dijital Ekonomi Politikaları gibi uluslararası platformlarda, hükümetler, özel sektör ve sivil toplum farklı paydaşlarla internet yönetimi, dijital haklar, dijital ekonomi ve siber güvenlik konularını tartışmakta ve ortak stratejiler oluşturmaktadır. OECD, OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier, 2024, https://doi.org/10.1787/a1689dc5-en (1 Şubat 2026).

[353] 2018'de devletlerarası girişimlerle oluşturulan Toronto Bildirisi gibi belgeler, makine öğrenme sistemlerinde eşitlik ve ayrımcılıkla mücadele ederek teknolojinin etik kullanımı için rehberlik sağlamaktadır. Toronto Declaration, The Toronto Declaration, 2018, https://www.torontodeclaration.org (1 Şubat 2026).

[354] BM tarafından 2014'te yayımlanan Dijital Hükümet Kılavuzu (Digital Government Guidelines), ülkelerin dijital hizmet sunma yöntemlerini ve kullanıcılarla etkileşimleri nasıl geliştirebilecekleri konusunda uluslararası standartlar sunmaktadır. United Nations Department of Economic and Social Affairs, United Nations E-Government Survey 2014: E-Government for the Future We Want, 2014, https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf (1 Şubat 2026).

sonraki bölümde, ABD, Çin ve Avrupa Birliği'nin dijital egemenlik yaklaşımları ayrı ayrı ve karşılaştırmalı biçimde ele alınacaktır.

b. ABD: Askerî Kökenlerden Neoliberal Küresel Yönetişime

ABD'nin dijital egemenliğe yaklaşımı, başlangıçta tamamen askerî ihtiyaçlara dayanan bir teknolojik geliştirme modelinden doğmuştur. İnternet ve bilgisayar teknolojilerinin temelleri; II. Dünya Savaşı koşullarında istihbarat, gözetim, şifreleme ve nükleer silah programlarının gerektirdiği hesaplama kapasitesi ihtiyacıyla atılmıştır. Bu askerî köken, internetin çifte yüzlü doğasını da belirlemiştir: Bir yandan güvenlik ve denetim amaçlı geliştirilen kapalı bir teknoloji, diğer yandan küresel iletişim ağlarının altyapısını oluşturacak açık bir sistem[355]. Zamanla bu askerî miras; siber-romantik özgürlük idealleri, siber-istisnacılık ve siber özgürlükçü (liberteryan) düşünceyle birleşmiş, ardından neoliberal piyasa mantığına evrilerek küreselci bir dijital stratejiye dönüşmüştür.

İnternetin erken döneminde hâkim olan siber-romantik yaklaşım, teknolojinin kendiliğinden özgürlük üreteceği varsayımına dayanıyordu. Açık, katılımcı ve yatay mimari; gönüllü katkı kültürü ve aracısız iletişim idealiyle interneti dijital bir ortak alan olarak şekillendirdi[356]. Bu anlayışı izleyen siber-istisnacılık ise interneti devlet egemenliğine tabi tutulamayacak nitelikte, sınır tanımayan ve hukuken özerk bir alan olarak konumlandırdı[357]. Dijital alanın, uluslararası hukukta hiçbir devlete ait olmayan ve egemenlik altında bulunmayan toprak anlamına gelen *terra nullius*[358] kapsamında görülmesi, devlet müdahalesinin meşruiyetini reddeden bu yaklaşımın merkezindeydi[359]. John Perry Barlow'un Siberuzayın Bağımsızlık Bildirgesi, bu düşüncenin sembolik ifadesi oldu:

---

[355] Aust ve Ammann, s.215-216.
[356] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.6,65; Varoufakis, *Technofeudalism: What Killed Capitalism,* s.70.
[357] Shapiro, s.217.
[358] Merriam-Webster, "terra nullius", https://www.merriam-webster.com/dictionary/terra%20nullius (14.12.2024).
[359] Kripto para gibi bazı dijital alanların hâlâ devlet kontrolünden büyük ölçüde bağımsız kalabilmesi, bu yaklaşım için önemli bir kanıttır. Eren, s.559. Hatipoğlu Aydın, s.57. Her ne kadar yazar bu görüşünü siber özgürlükçüler için belirtmiş olsa da zikrettiği özellikler siber-istisnacılara daha uygun düşmektedir.

"*Endüstriyel Dünyanın Hükümetleri, ..., ben Zihnin yeni evi Siber uzaydan geliyorum… Toplandığımız yerde egemenliğiniz yoktur… Seçilmiş bir hükümetimiz yok ve olması da muhtemel değil… İnşa ettiğimiz küresel sosyal alanın, bize dayatmaya çalıştığınız tiranlıklardan doğal olarak bağımsız olacağını ilan ediyorum. Bizi yönetmek için hiçbir ahlaki hakkınız yok ….*"[360]

Bu deklarasyon, dijital alanların fizikî sınırların ötesinde, her yerde olan ama aynı zamanda hiçbir yerde olmayan, klasik devlet otoritesine ihtiyaç duymayan ve kullanıcıların kendi toplumsal sözleşmelerini oluşturduğu özerk bir yapı olması gerektiğini vurgular. İnternetin ilk dönemlerinde hâkim olan bu anlayış, dijital alanı kullanıcıların katılımıyla şekillenen küresel bir ortak alan olarak tanımlayan, oldukça ütopik bir vizyona dayanır[361]. Bu anlayış zamanla yaygınlaşarak bilgi teknolojilerini devlet güdümlü güvenlik araçları olmaktan çıkarıp liberal demokrasi ve serbest piyasa kapitalizminin sembolüne dönüştürmüştür[362].

Ne var ki, devletsiz ve tamamen özerk bir dijital alan tasavvuru; tarihsel ve pratik olarak sürdürülebilir değildir. İnternet bizzat devlet eliyle doğmuş; devletin çevrimiçi alandan bütünüyle çekilmesi ne mümkün ne de rasyonel olmuştur. ABD, söylemde müdahalesizliği savunurken uygulamada şifreleme, bilgi akışı ve güvenlik başlıklarında güçlü müdahalelerde bulunmuş; buna karşılık veri ekonomisi ve platform gücü gibi alanlarda ciddi düzenleme boşlukları yaratmıştır[363]. ABD'de telekomünikasyon ve internet alanında liberalizasyonu hedefleyen 1996 Telekomünikasyon Yasası ve Communications Decency Act'ın (CDA) bazı hükümlerinin Reno v. ACLU kararıyla iptali, internetin büyük ölçüde düzenleme dışı bırakıldığı liberal bir yaklaşımı pekiştirmiştir. İptal kararının gerekçesinde, demokratik toplumda internet de dâhil olmak üzere serbest fikir alışverişinin korunması, sansürle sağlanabilecek olası toplumsal

[360] John Perry Barlow, "A Declaration of the Independence of Cyberspace", **Duke Law & Technology Review**, Vol.18, No.1, (2019).
[361] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.235.
[362] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.112.
[363] Shapiro, s.217.

yarardan daha üstün olduğu savlanmıştır[364]. Bu süreçte özellikle CDA'nın Section 230'u, platformlara kullanıcı içerikleri bakımından geniş bir sorumsuzluk tanıyarak ABD internet hukukunun temel unsurlarından biri hâline gelmiştir. ABD'de mahkemeler, CDA 230'u sosyal medya platformlarına müstehcen içerikler dahil mutlak bir koruma sağlayacak şekilde yorumlamaktadırlar. Bu da platformların ihmalkâr bile olsalar sorumluluktan muaf tutulmalarını sağlamaktadır[365]. Bill Clinton'ın interneti vergiden ve sansürden büyük ölçüde arındırılmış bir alan olarak tanımlaması da devletin yalnızca asgari bir hukukî çerçeveyle yetinmesi gerektiği anlayışını güçlendirmiştir. Ancak bu yaklaşımın temel çelişkisi açıktır: Devlet eliyle yaratılmış bir teknolojinin neoliberal "bırakınız yapsınlar" mantığıyla yönetilmesi hem hukuki hem toplumsal boşluklar doğurmuştur[366].

Siber-istisnacıları takiben beliren siber özgürlükçü-liberteryen[367] yaklaşım, interneti mutlak bireysel özerklik alanı olarak gören ve devlet müdahalesini ilke düzeyinde reddeden en radikal ve ideolojik dijital düşünce akımıdır. Temeli radikal bireycilik, devlet karşıtlığı ve piyasa merkezliliğidir: Veri bireyin mülküdür; dijital alan devlet tarafından değil, dağıtık mimariler ve serbest piyasa tarafından düzenlenmelidir. Cypherpunklar (şifreleme ve anonimlik savunucuları) ve kripto-anarşistler bu çizginin en uç örnekleridir. Bu yaklaşımın felsefi arka planı klasik liberalizme, özellikle John Locke'un kapitalist toplumun ahlaki temeli olan mülkiyet eşitsizliğinin emek üzerinden haklılaştırıldığı[368] bireysel mülkiyet ve doğal hak öğretisine dayanır[369]. İnternetin erken

---

[364] Kayıhan İçel, "Cumhuriyetimizin 75. Yılında Türk Ceza Hukuku ve Globalleşme", **Cumhuriyetin 75. Yılı Armağanı** içinde, İstanbul: İstanbul Üniversitesi Yayınevi, 1999, s.74.

[365] Muharrem Çelik ve Muhammed Beheşti Aydoğan, "Sosyal Medyada Hukuku Yerleşik Kılma Çabaları", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (303-323), İstanbul: Adalet, 2021, s.305.

[366] Shapiro, s.19-20.

[367] Dijital çağ tartışmalarında liberal değil liberteryen kavramı daha yerindedir; çünkü dijital özgürlük arayışı klasik liberalizmin sınırlı devlet anlayışını aşarak radikal bireycilik, anti-devletçilik ve ademimerkeziyetçiliği merkeze alan bir çerçeveye dönüşmüştür. Türkçede liberal ve liberteryen kavramları sık sık karışır çünkü her ikisi de birey özgürlüğünü savunur. Ancak özellikle dijital çağda kişisel veri, anonimlik, gözetimden kaçış, ademimerkeziyetçilik gibi konular konuşulurken liberteryen demek çok daha doğru ve yerinde bir tercihtir. Bu yönüyle liberteryenizm, dijital çağın siyasi anarşizmidir.

[368] Uygun, s.236.

[369] John Locke, **Yönetim Üzerine İkinci İnceleme: Sivil Yönetimin Gerçek Kökeni Boyutu ve Amacı Üzerine Bir Deneme,** Fahri Bakırcı (çev.), Ankara: Ebabil Yayınları, s.64.

dönemlerinde ABD'de dijital alanın devletsiz özgürlük bölgesi olarak görülmesi, devlet müdahalesine duyulan güvensizlik ve siber özgürlükçü düşüncenin siyasal kültürde yer bulması bu teorik temel sayesinde meşrulaşmıştır. Teknoloji şirketleri de küresel büyüme için devlet denetimsizliğini avantaj gördüğünden bu zihniyeti desteklemiştir[370].

Ancak zaman içinde dijital alanların tamamen devletten bağımsız işlemesinin pratikte mümkün olmadığı ortaya çıkmıştır. İçerik denetimi, siber saldırılar, dijital suçlar ve kötü amaçlı içeriklerin topluluk tarafından kendiliğinden bertaraf edilememesi, devletin tamamen geri çekildiği bir düzenin sürdürülemez olduğunu göstermiştir. Bu nedenle güncel tartışmalar artık "devlet olsun mu olmasın mı" sorusundan ziyade, devlet müdahalesinin hangi sınırlar ve ilkeler doğrultusunda meşru olduğu sorusuna kaymıştır[371].

Dijital teknolojilerin ekonomik gücünün artmasıyla ABD'nin başlangıçtaki siber özgürlükçü çizgisi günümüzde iki yönlü simbiyotik bir modele evrilmiştir: Neoliberal piyasa modeli ve güvenlik-devlet modeli. Dijital tekeller (özellikle GAFAM) devlet desteğiyle küresel ölçekte büyütülürken ABD devleti, bu şirketlerin veri altyapılarına nüfuz edebilen, denetimsiz bir gözetim rejimi kurmuştur. Bu ikili yapı, dijital alanın hem piyasa kapitalizmi hem de devlet gözetimi tarafından ortaklaşa şekillendirildiği yeni bir düzene dönüşmüştür.

Bu süreç, devletsiz özgürlük söylemi altında ikili bir sonuç doğurmuştur: Bir yandan özel sektörün fiilî tahakkümü güçlenmiş, diğer yandan devlet dolaylı ve görünmez biçimde denetim kapasitesini artırmıştır[372]. Özellikle 11 Eylül sonrasında gizlilikten güvenliğe keskin kayış söz konusu olmuş; Clinton döneminde gizlilik ve veri koruma yönünde atılan adımlar tamamen tersine dönmüştür[373]. Patriot Act ve devamı niteliğindeki düzenlemeler, ABD'de güvenliği mutlaklaştıran bir olağanüstü hâl mantığı yaratarak devletin gözetim yetkilerini sınırsız biçimde genişletmiştir[374]. Patriot Act,

[370] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.113.
[371] Hatipoğlu Aydın, s.70, 73.
[372] Shapiro, s.219-220.
[373] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.115.
[374] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.147-148.

mahkeme kararı gerekliliğini fiilen ortadan kaldırarak kolluğun sınırsız gözetim yapabilmesini ve iletişim verilerine erişmesini sağlamış; böylece özel hayatın anayasal koruması çökmüştür. NSA, bu hukuki zeminle yalnızca ABD vatandaşlarını değil, zamanla küresel iletişimi de izleyebilecek yetkiye kavuşmuştur[375]. 2013 sızıntılarıyla ortaya çıkan; e-postalar, ekler, sohbetler, arama kayıtları, dosyalar, multimedya içeriklerini mahkeme izni olmadan toplayan ve şirketlerden kullanıcı verilerini doğrudan çeken PRISM[376] gibi mekanizmalar, fiber optik küresel iletişim hatlarının dinlenmesi, Google, Apple, Facebook, Microsoft gibi şirketlerle gizli veri paylaşım anlaşmaları, ABD'de kitlesel ve sürekli gözetimi kalıcılaştırdı ve NSA gözetim rejiminin kurumsallaşmasına yol açtı[377]. Edward Snowden'ın sözleri durumu özetler: "*NSA, Amerikan ağlarından geçen her şeyi istisnasız olarak toplamaktadır. Gözetim altında olmayan tek bir bağlantı noktası yoktur*."[378]. Özellikle teknoloji şirketleriyle yapılan gizli anlaşmalar sayesinde NSA, ulusal sınırları aşan, küresel iletişimi gerçek zamanlı izleyebilen tarihsel ölçekli bir gözetim aygıtı inşa etmiştir.

Bu yapı, güvenlik söylemiyle meşrulaştırılsa da fiilen modern çağın en kapsamlı gözetim devleti mimarisine dönüşmüş durumdadır. Oysa güvenlik mantığı mutlaklaştırıldığında, özel diye bir şeyin kalmadığı varsayılır; tüm toplumsal alan devletin kontrol edilebilir ortak bir yüzeyi hâline gelir[379]. Bu yalnızca teorik bir sonuç değil, devletin bilinçli tercihlerinin de ürünüdür. ABD'de federal ve yerel yönetimler vatandaş verilerini analiz etmek için yaygın biçimde algoritmik yazılımlar kullanmakta; bu kullanımın kapsamı ve yöntemleri kamuoyundan çoğu kez gizli tutulmaktadır.

---

[375] Aust ve Ammann, s.63-64.

[376] Glenn Greenwald ve Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian,* 7 Haziran 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (1 Şubat 2026).

[377] Bu ortamda NSA'nın kapasitesi patlayıcı biçimde büyüdü: küresel fiber hatlar dinlemeye uygun hâle getirildi, özel şirketlere izleme yazılımları ürettirildi, "Five Eyes" ittifakı sisteme entegre edildi ve kurum hiçbir gerçek denetime tabi olmadan bir veri toplama imparatorluğuna dönüştü. Nixon döneminde 300 kişi gözetlenirken bu sayı NSA döneminde 300 milyona çıktı; insan hakları hiçbir aşamada ölçüt olmadı. 1978 tarihli FISA, NSA ve CIA'in izleme faaliyetlerine yalnızca sembolik bir "yasal çerçeve" sağladı; mahkeme yılda bir kez bilgilendirilir, gerçek bir kontrol yapılmazdı. 2008 değişikliğiyle NSA, artık ABD vatandaşı olmayanların iletişim verilerini de doğrudan şirketlerden talep edebilir hale geldi. 2008 sonrası NSA, ABD Siber Kuvvetleri'nin komuta merkezi hâline gelerek dijital saldırı ve savunmayı yöneten ana yapı oldu. Aust ve Ammann, s.66-71.

[378] Aust ve Ammann, s.109.

[379] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.221.

Böylece hem özel alan daralmakta hem de ortak payda, devletin gözetim kapasitesini genişleten bir zemine dönüşmektedir[380].

Bu ortam, Google gibi şirketlerin yükselişine zemin hazırlayan bir gözetim istisnailiği üretip; devlet güvenlik gerekçeleriyle kendine veri akışını açarken, şirketlere de denetimsiz büyüme alanı tanımıştır. Devlet ile teknoloji şirketleri arasındaki simbiyoz, gözetim kapitalizminin doğuşunu hazırlamıştır. Devletin istihbarat kurumları ile Google başta olmak üzere teknoloji şirketleri arasında karşılıklı bağımlılık gelişmiş; devlet bu şirketlerin veri işleme gücünden yararlanırken şirketler de gizlilik düzenlemelerinden fiilen muaf bir genişleme rejimine kavuşmuştur[381]. Google'ın agresif lobi faaliyetleri, ABD ve AB'de gizlilik düzenlemelerini zayıflatmış; davranışsal veri çıkarımı adeta hukuki boşluk içinde kök salmıştır. Böylece gözetim kapitalizmi kurumsallaşmıştır. Kamu-özel sektör iş birliği görünümlü bu birleşme eğilimi, devlet gözetimi ile şirket gözetiminin iç içe geçtiği ve şirketlerin fiilî dokunulmazlık kazandığı yeni bir dijital güç rejimi yaratmıştır[382].

Radikal siber özgürlükçü yaklaşımın birey merkezli felsefi temeli (Locke'un mülkiyet doktrini), bu dönemde verinin şirket mülküne dönüşmesi üzerinden tersine işletilmiştir. Dijital mülkiyet kavramı üzerinden Locke'un emek üzerinden haklılaştırılan mülk anlayışı[383] veri üzerinden kendini yeniden göstermiştir. Bireylerin çevrimiçi davranışlarından elde edilen veriler, Locke'un emek üzerinden sahip olunan mülk anlayışı çerçevesinde özel şirketlerin ekonomik varlığına dönüştürülmüştür. Üstelik bir katılımcı olan kullanıcı tamamen hür (!) iradeyle bunu yapmaktadır. Kullanıcının davranış verisi, şirketlerin meta üretim kaynağına dönüşmüştür. Dijital alan, özgürlük değil veri metalaştırması ekseninde yapılandırılmıştır. Aynı zamanda dolar merkezli finansal sistem, bulut altyapısı, platform tekelleri ve veri ekonomisiyle bütünleşerek ABD'yi hem finansal hem dijital akışların merkezi yapmıştır. Bu durum klasik

---

[380] Erkan Saka, "Polislik Algoritmaları Bağlamında Öngörücü Algoritmalara (Predictive Algorithms) Eleştirel Bir Yaklaşım", Oğuz Kuş (Ed.), **Algoritmaların Gölgesinde Toplum ve İletişim,** içinde (81-98), Ankara: Alternatif Bilişim Derneği, 2021, s.69.

[381] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.149-155.

[382] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.160-161.

[383] Locke, s.23-37; John Locke, **Yönetim Üzerine İki İnceleme,** Ömer Saruhanlıoğlu (çev.), İstanbul: Litera Yayıncılık, 2020, par.26-40. s.188-197.

kapitalizmin dönüşüp tekno feodal bir yapıya evrildiğini gösteriyor: Güç birkaç teknoloji devinde yoğunlaşırken veri, algoritmalar ve platform hakimiyeti yeni sermaye türüne dönüşmektedir. Rekabet yerini, bağımlılık yaratan kapalı platform evrenlerine bırakmaktadır[384]. ABD'li teknoloji şirketlerinin oluşturduğu dijital yapının küresel bağımlılığı o kadar derinleşmiş durumdadır ki dolardan veya ABD merkezli sermaye ekosisteminden kaçış neredeyse imkânsız hale gelmiştir. Böylece ABD dijital egemenlik yaklaşımı, kapsamlı bir veri koruma rejimi yerine, neoliberal çizgiye kayarak şirketlerin faaliyet özgürlüğünü ve ticari çıkarlarını koruyan parçalı ve sektör-temelli düzenlemelerle yetinmiştir[385].

ABD, teknoloji şirketlerinin oluşturduğu dijital yapıyı korumak için dijital alanda rekabetten çekinmemektedir. Rekabetçi yaklaşım, dijitalleşmede yerlilik, stratejik özerklik ve ulusal güvenlik hedeflerini merkeze alır. Devlet, dijital altyapıların ve veri ekosistemlerinin yabancı bağımlılıklardan arındırılmasını, böylece hem güvenliği hem de ekonomik çıkarları korumayı amaçlar. ABD'nin 2020'de başlattığı Clean Network Programı, bu yaklaşımın en belirgin örneğidir[386]. Program, dijital altyapıdan uygulama mağazalarına, bulut hizmetlerinden denizaltı kablolarına kadar uzanan tüm zincirde güvenilirlik esasına dayalı bir ayrıştırma stratejisi kurar. Esas amaç yalnızca veri güvenliğini artırmak değil; Çin'in küresel dijital pazardaki etkisini sınırlamak ve ABD'nin dijital jeopolitik üstünlüğünü sürdürmektir. Bu kapsamda:

- Çinli donanım ve yazılım tedarikçilerinin telekom altyapısından dışlanması,
- Çin menşeili uygulamaların online mağazalardan ve platformlardan kaldırılması,
- Bulut hizmetlerinde yabancı (özellikle Çinli) erişimin sınırlandırılması,
- Denizaltı kabloları ve kritik iletişim hatlarının yalnızca güvenilir taraflarca kurulması,

---

[384] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.46-48.

[385] Paul M. Schwartz ve Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", **New York University Law Review,** Vol.86, (December 2011), s.1815-1819.

[386] Dijital hizmet sağlayıcılarında güvenilirlik kriterini esas alan bu program; operatör, uygulama mağazası, uygulamalar, bulut, iletişim kabloları, veri iletim yolu olmak üzere altı temel politikadan (clean carrier, clean store, clean apps, clean cloud ve clean path) oluşmaktadır. U.S. Department of State, "The Clean Network", https://2017-2021.state.gov/the-clean-network/ (14.12.2024).

- 5G gibi stratejik ağlarda Çin teknolojisinin tamamen dışlanması,

- TikTok ve WeChat gibi uygulamaların yasaklanması; Huawei, SMIC ve diğer teknoloji devlerine yaptırımlar uygulanması

gibi adımlar atılmıştır.

Bu politika, ABD'nin dijital ekonomideki küresel liderliğini koruma hedefiyle de doğrudan bağlantılıdır ve Washington, müttefiklerini benzer sınırlamalar getirmeye zorlayarak stratejiyi çok taraflılaştırmaya çalışmaktadır. Trump döneminde Huawei'ye yönelik yaptırımlar ve Avrupa'daki 5G'de Huawei'nin dışlanması, ABD'nin küresel dijital ağlarda teknoloji kontrolü ve egemenlik mücadelesinin bir parçasıdır. Çin ise bu yaklaşımı korumacı, tek taraflı ve uluslararası ticarete aykırı olarak nitelendirmekte; ABD'nin dijital egemenlik söylemini müdahaleci bir araç olarak kullandığını savunmaktadır[387]. Literatürde bu gerilim, ABD-Çin rekabetinin Cold War 2.0 olarak adlandırılan yeni bir dijital Soğuk Savaş mantığına dönüştüğünü gösterir[388]. Bu hattın daha da sertleştirmesi, dijital çağın stratejik kuşatma araçlarının silah ambargolarını aratmayacak düzeye geldiğini ortaya koymaktadır.

ABD'nin dijitalleşme yaklaşımı, teknolojik gelişmelerin yanı sıra refah devletinin krizleri sonrasında güç kazanan neoliberalizm, minimum devlet anlayışı ve yönetişim paradigmasıyla şekillenmiştir. Yönetişim, devletin tek merkezli ve hiyerarşik yapısının yerine; özel sektör, sivil toplum ve yerel aktörlerin karar alma süreçlerine dâhil edildiği çok aktörlü bir modeli ifade eder. Küreselleşmeyle birlikte bu geçiş, kamu gücünün kullanımını yeniden tanımlamış; modern merkeziyetçi devlet anlayışının sorgulanmasına ve neoliberal ideolojinin idari karşılığı olan yeni kamu işletmeciliği yaklaşımının kurumsallaşmasına zemin hazırlamıştır[389].

---

[387] Laurens Cerulus ve Jacopo Barigazzi, "Chinese foreign minister warns of US 'interference' on Europe tour", *Politico*, 25 Ağustos 2020, https://www.politico.eu/article/chinese-foreign-minister-warns-of-us-interference-on-europe-tour/ (1 Şubat 2026).

[388] Internet Society, Internet Society Statement on U.S. Clean Network Program, 2020, https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/ (1 Şubat 2026).

[389] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.137-143.

Çok paydaşlı internet yönetişimi; devlet merkezli ve hiyerarşik egemenlik anlayışı yerine; devletler, özel sektör, teknik topluluklar ve sivil toplumun eşit katılımına dayanan, iş birliği ve şeffaflığı esas alan bir modeli ifade eder. Bu yaklaşım, karar alma süreçlerinin tek bir merkezde toplanmasını azaltarak, küresel platformların ve farklı aktörlerin yönetime doğrudan dâhil olduğu, hesap verebilir bir düzen kurmayı amaçlar. Devlet egemenliğinin alternatifi olmaktan ziyade, onunla birlikte işleyen tamamlayıcı bir yönetişim biçimi olarak konumlanır[390].

ABD'nin dijital yönetişim anlayışı, Çin ve Rusya'nın devlet merkezli veri kontrol modelleri ile Avrupa Birliği'nin insan onuru temelli veri koruma yaklaşımından farklı olarak; ticareti ve veri akışının serbestliğini önceleyen bir perspektife dayanır[391]. Bu yaklaşım, OECD'nin 1980 tarihli Kılavuzu ile Avrupa Konseyi'nin 1981 tarihli 108 sayılı Sözleşmesi'nde de görüldüğü üzere, sınır ötesi veri akışını kolaylaştırmayı ve küresel veri piyasalarının işlerliğini sağlamayı hedefleyen neoliberal veri yönetişimi anlayışını yansıtmaktadır[392].

Veri rejimi bakımından ABD, devletin dijital veri altyapısı üzerindeki kurumsal denetimini güçlendirmek yerine özel sektöre geniş alan açan, neoliberal yönetişim anlayışının dijital yansıması niteliğinde bir yaklaşım benimsemiştir. Bu modelde veri, bireyin dijital özerkliğinin unsuru olarak değil; şirketlerin işleme ve ticarileştirme hakkının konusu olarak ele alınmakta; birey veri ekonomisinin öznesi olmaktan çok nesnesine indirgenmektedir. Federal düzeyde kapsamlı bir veri koruma yasasının bulunmaması ve gizliliğin sektörel ve parçalı düzenlemelerle sınırlı tutulması[393] ABD'li şirketlerin küresel ölçekte veri toplama ve işleme kapasitelerini onlara avantaj sağlamak

---

[390] Eren, s.560.

[391] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.5.

[392] OECD, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, 2011, http://dx.doi.org/10.1787/5kgf09z90c31-en (1 Şubat 2026), s.12; Irion, *"Government Cloud Computing and National Data Sovereignty",* s.62.

[393] COPPA (Children's Online Privacy Protection Act) çocukların; GLBA (Gramm-Leach-Bliley Act) finansal verilerin, FCRA (Fair Credit Reporting Act) kredi bilgilerinin ve HIPAA (Health Insurance Portability and Accountability Act) sağlık verilerinin korunmasına yöneliktir. ABD Ulusal Standartlar ve Teknoloji Enstitüsünce ilk kez 2014 yılında yayınlanan NIST (National Institute of Standards and Technology) Siber Güvenlik Çerçevesi, tüm sektörlerdeki kamu ve özel kuruluşlar için esnek, risk temelli bir rehber olarak kurumların siber güvenlik risklerini yönetmelerine ve azaltmalarına yardımcı olmak amacıyla oluşturulmuş bir referans yapıdır.

üzere[394] bilinçli biçimde serbest bırakmıştır[395]. Bu durum, AB'nin temel hak ve özgürlükler merkezli veri koruma rejimiyle yapısal bir uyumsuzluk yaratırken, az sayıda büyük şirketin elinde yoğunlaşan devasa bir veri ekonomisinin oluşmasına zemin hazırlamıştır[396].

Sonuç olarak ABD'nin güncel dijital egemenlik yaklaşımı, neoliberal küresel yönetişim çerçevesinde işlemekte; dijitalleşme, küreselleşmenin yeni bir tahakküm biçimi hâline gelmektedir. Başlangıçtaki devletsiz özgürlük ideallerinden uzaklaşan bu yapı; şirket güdümlü dijital piyasa, devlet güdümlü kitlesel gözetim ve platform tekellerinin birleştiği çok katmanlı bir dijital hegemonya üretmektedir[397]. Bu düzen, ulus-devletlerin ekonomik ve egemenlik kapasitelerini derinden aşındırmakta; dijital egemenliğini korumak isteyen devletleri bu modele karşı zorunlu olarak siyasal bir konum almaya itmektedir[398].

c. Çin: Otoriter Ulus-Devlet Merkezli Bilgi Güvenliği Modeli

Teknoloji ve dijitalleşme süreci başından beri siyasetten bağımsız değildir. Öncelikle ABD'nin öncülüğünde gelişen dijitalleşme, zamanla diğer devletlerin de ilgisini çekmiş ve bu devletler farklı stratejiler benimsemiştir. Bu kısımda, dijitalleşmede kurulu neoliberal/küresel rant düzenini korumaya yönelen ABD yaklaşımından ve insan hakları temelli kurallar koyucu bir çizgiyi izleyen AB yaklaşımından daha farklı olan; paternalist, rekabetçi, otoriter ve izolasyona yönelmiş Çin Halk Cumhuriyeti'nin yaklaşımı analiz edilmektedir.

---

[394] Anupam Chander, "How Law Made Silicon Valley", **Emory Law Journal,** Vol.63, No.3, (2014), s.642; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data (COM(2020)66), 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066 (1 Şubat 2026), s.3.

[395] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.8; Anupam Chander, Margot E. Kaminski ve William McGeveran, "Catalyzing Privacy Law", **Minnesota Law Review,** No.105, (2011), s.1767, 1768.

[396] Kai Spiekermann ve Diğerleri, "Big Data Justice: A Case for Regulating the Global Information Commons", **Journal of Politics,** Vol.83, No.2, (2019), s.12, 13.

[397] Doğan Özlem, "Ahlakta, Hukukta ve Siyasette Özgürlük Kavramı Üstüne", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII Sayı.1, (2014), s.94.

[398] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.60.

Paternalist yaklaşım, dijital alanların denetimsiz bırakılmasının bireyleri ve toplumu zarara açık hâle getirdiğini; bu nedenle devletin kamusal yararı korumak üzere müdahale ve yönlendirme sorumluluğu taşıdığını savunur[399]. Dijital ortamlar zaten *Lex Informatica* benzeri kurallarla işlediğinden, sınırsız özgürlük fikri yanıltıcıdır; doğru tasarlanmış devlet müdahalesi dijital özgürlükle çelişmez, hatta onu güvenceye alır[400]. Bu yaklaşım, Hugo Grotius'un açık deniz özgürlüğü *(Mare Liberum)* düşüncesine[401] ve uluslararası ticarette şekillenen *lex mercatoria* benzeri devletsiz ve kendi kendini organize eden norm alanlarına gönderme yapar; ancak çevrimiçi hakları koruyacak üst düzey bir otoritenin yokluğu devlet düzenlemesini gerekli kılar[402]. Çokuluslu şirketlerin kendi kendini örgütleyen fiilî hukuk alanları oluşsa da bunların yine de egemen devlet denetimine ihtiyaç duyarlar. Bu çerçevede paternalist model, devlete dijital süreçlere aktif müdahale görevi yükler. Çin'in 2015 Ulusal Güvenlik Yasası ile hükümete siber uzayda ulusal güvenliği ve kalkınma çıkarlarını koruma misyonu verilmesi buna örnek olup, erişim engeli, sansür ve içerik denetimi gibi araçların stratejik ve dikkatli kullanımını içeren esnek ama etkili bir yönetim tarzı geliştirilmiştir[403].

Çin'in dijitalleşmede rekabetçi yaklaşımı, Kuşak ve Yol Girişimi üzerinden gelişmekte olan ülkelere dijital altyapı desteği sunarak etki alanını genişletmesi, yabancı dijital platformları sıkı denetime tabi tutması[404] ve Renren, Tianya, Youku Tudou, Sina Weibo, WeChat gibi devlet destekli yerli alternatifleri teşvik etmesiyle belirginleşir[405]. Ancak dijitalleşmede paternalist ve rekabetçi yaklaşım, zamanla dijital altyapıyı tamamen yerli kaynaklara dayandırmaya yönelen izolasyoncu bir modele dönüşme riski taşır ve küresel teknolojik gelişmelerden kopmaya yol açabilir[406]. Rekabetçi dijital stratejiler aynı zamanda karşılıklılık etkisi yaratarak diğer devletleri de benzer kısıtlamalara

---

[399] Hatipoğlu Aydın, s.74.
[400] Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", **Texas Law Review,** 1997, Vol.76, (1997), s.555-556.
[401] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.236.
[402] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.111-113.
[403] Şimşek Öner, s.155.
[404] Creemers, "*China's Approach to Cyber Sovereignty"*, s.3.
[405] Schneider, *China's Digital Nationalism,* s.206-207. Benzer biçimde Türkiye'nin TROY'u, Rusya'nın MIR ödeme sistemi ve Rutube platformu, yerli dijital ekosistem oluşturma çabalarının örnekleridir.
[406] Tipper ve Krishnamurthy, s.2.

yöneltmekte; Huawei ve DeepSeek'in Batı'daki sınırlamaları ile TikTok'un ABD ve Hindistan'da yasaklanması bu gerilimin somut örneklerini oluşturmaktadır.

Çin'in yaklaşımı, bilgi akışının tamamını kapsayan güvenlik denetimi ve rekabet stratejilerinden oluşan katı bir Vestfalyan dijital egemenlik anlayışı şeklinde özetlenebilir ve üç temel boyuta indirgenebilir.

İlk olarak, Çin, dijitalleşme politikasını ulusal egemenlik, güvenlik ve iç işlerine müdahale edilmeme ilkesi üzerine kurarak her devletin kendi dijital alanını mutlak biçimde kontrol etmesini; internetin devletler arası yapılar eliyle yönetilmesini savunur[407]. Bu model, Batı'daki çok paydaşlı yönetişim yaklaşımını reddeder; devletin dijital alanda merkeziyetçi, hiyerarşik ve otoriter bir yapısını tesis etmesini esas alır[408]. "Tarihin sonu" liberal demokratik değerler, evrensel insan hakları ve dış müdahale fikri tehdit olarak görülür; Çin uluslararası düzeyde alternatif bir normatif çerçeve oluşturma arayışındadır[409]. Çin'in yaklaşımında dijital güvenlik yalnızca teknik altyapıya indirgenmez; bilgi otobanında akışın tümü üzerinde içerik ve iletişim kontrolünü de kapsar. 1990'lardan beri yürütülen enformasyonlaştırma programı, başlangıçta idari verimliliği artırmayı hedeflerken zamanla büyük veri ve yapay zekâ destekli daha kapalı ve kontrolcü bir sisteme dönüşmüştür. Amaçlar arasında karar alma ve yönetim süreçlerinin otomatikleşmesi, ekonomik büyümenin yeni yolları olarak bu teknolojilerde dünya lideri olmak yer alır. Bu anlayış, zamanla içerik denetimini ve bilgi kontrolünü önceliklendiren daha kapalı ve totaliter bir çizgiye evrilmiştir[410]. Bu süreçte, Çin Komünist Partisi egemenliğini teknolojik düzeyde sert, ideolojik ve kültürel sansür ile uygulamakta[411] Büyük Güvenlik Duvarı ile siyasi ve kültürel içerikleri filtrelemekte[412] ve

---

[407] Creemers, "*China's Approach to Cyber Sovereignty"*, s.9, 13.
[408] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.112.
[409] Creemers, "*China's Approach to Cyber Sovereignty"*, s.19;
[410] Rogier J.E.H. Creemers, "The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies", Nicholas Wright (Ed.), **Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives içinde** (129-135), Alabama: Air University Press, 2018, s.129.
[411] Schneider, *China's Digital Nationalism,* s.225-227.
[412] James Griffiths, **The Great Firewall of China: How to Build and Control an Alternative Version of the Internet,** London: Zed Books. 2019, s.8.

denetim sorumluluğunu merkezden çevreye[413] şirketlere[414] ve bireylere yayarak oto-sansür ile gözetimi içselleştiren bir dijital panoptikon yaratmaktadır[415]. Sosyal medya gruplarında paylaşımlardan grup yöneticileri sorumlu tutulmakta, böylece kullanıcılar sansür uygulayıcılarına dönüştürülmektedir[416]. Bu tutum, dijital güvenliği teknik bir mesele olmaktan çıkarıp siyasal, kültürel ve ideolojik bir mücadele alanına dönüştürmektedir[417]. Benzer biçimde Rusya da siber güvenlik yerine bilgi güvenliği kavramını öne çıkararak dijital alanı teknikten çok siyasal ve ideolojik bir mücadele zemini olarak tanımlar[418]. Çin'in güvenlik yaklaşımı zamanla içerik denetiminin ötesine geçerek veri güvenliği, tedarik zincirleri, kritik altyapılar ve küresel internet yönetişimi alanlarına yayılmıştır.

Çin'in dijital egemenlik anlayışının ikinci boyutu, dijital alanda kendi "sınırlarını" çizerek hem iç kontrolü güçlendirmeyi hem de dışa bağımlılığı azaltan kapalı ve özerk bir dijital düzen kurma hedefidir. Bu hedef doğrultusunda 2014'te siber güvenlik yapılarını (Siber Güvenlik ve Enformasyonlaştırma Merkez Komisyonu ve doğrudan düzenleyici yetkiye sahip Çin Siber Uzay İdaresi) oluşturmuş; ardından 2016'da ve 2017'de sırasıyla Ulusal Büyük Veri Stratejisi ve Ulusal Yapay Zekâ Stratejisi devreye alınmıştır. Bu çerçevede yerli teknolojiyi öne çıkarma kamu alımlarında yerli firmalara öncelik verme, standart belirleme süreçlerinden yabancıları dışlama ve "güvenilmez şirketler" listeleri oluşturma gibi adımlarla stratejik özerklik inşa edilmektedir[419]. Çin'in 13. Beş Yıllık Kalkınma Planı ve Internet Plus[420] girişimi bu dönüşümü

---

[413] Rogier Creemers, "The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Age", Jacques deLisle, Avery Goldstein ve Guobin Yang (ed.), **The Internet, Social Media, and a Changing China** içinde (86-105), Philadelphia: University of Pennsylvania Press, 2016, s.98-100.

[414] Creemers, "*China's Approach to Cyber Sovereignty"*, s.14.

[415] Schneider, *China's Digital Nationalism,* s.208; Florian A. Schneider, "The cultural governance of China's mass media events: how the PRC manages discourses in complex media environments", Chris Shei (Ed.), **The Routledge handbook of Chinese discourse analysis** içinde (458-469), London/New York: Routledge, 2019, s.460.

[416] Florian A. Schneider, "Communication and censorship", Chris Shei ve Qing Cao (Ed.), **Chinese studies: Chinese media, communication and technology,** içinde London: Routledge, 2023, s.5.

[417] Eric Siyi Zhang ve Rogier J.E.H. Creemers, **"Russian perspectives on China as an actor in cyberspace",** Leiden: Leiden Asia Centre., 2021, s.11.

[418] Zhang ve Creemers, s.3, 4.

[419] Creemers, "*China's Approach to Cyber Sovereignty"*, s.6, 16.

[420] Mobil internet, büyük veri, bulut bilişim ve nesnelerin internetini bütünleştirmeyi hedefleyen bu strateji, Çin'in dijital alanda küresel güç olma hedefinin son halkasıdır. İnternet yönetimindeki yeniden yapılanmanın ardından sosyal medya denetimi ve kötü amaçlı yazılımlara karşı düzenlemeler getirilmiş, üst düzey denetleyici kurumlar kurulmuştur.

kurumsallaştırmış; Alibaba, Tencent ve Baidu gibi devler yapay zekâdan dijital ödeme ve platform entegrasyonlarına kadar geniş bir ekosistem kurarak devlet stratejisiyle uyumlu biçimde büyümüştür[421]. Dış yaptırımlar ise Çin'in teknoloji geliştirme hızını artırmış; Huawei'nin 5G öncülüğü ve HarmonyOS gibi yerli işletim sistemleri bu yönelimin sonucudur. Bu egemenlik anlayışı küresel internet yönetişimine de taşınmış; ICANN'a alternatif olarak Çince alan adlarını destekleyen sistemler geliştirilmiş, kök DNS sunucularının ülke içinde tutulması ve alan adı otoritelerinin Çin hukukuna tabi olması zorunlu kılınmıştır[422]. İnternet trafiği büyük ölçüde ülke sınırları içinde yönlendirilmekte, acil müdahale mekanizmaları ve yerel veri merkezleri kurulmaktadır[423]. Snowden ifşaları sonrasında veri yerelleştirme stratejik bir güvenlik meselesine dönüşmüş; özellikle kritik altyapı verilerinin ve işlemlerinin ülke içinde tutulması[424] ve yerel temsilcilerce yürütülmesi şart hâline gelmiştir[425]. 2021 Veri Güvenliği Yasası, veri ihracında devlet onayı ve güvenlik değerlendirmesi zorunluluğu getirerek (m. 31-36) yabancı şirketlerin veri toplama yetkilerini sınırlandırmıştır (m. 36-37)[426]. Ayrıca yabancı yaptırımlara karşı hükümete misilleme yetkisi tanıyarak (m. 37) Çin'in veri egemenliği anlayışını uluslararası politikaya da yansıtmıştır.

Yoğun altyapı yatırımları toplumun büyük bölümünü hızla çevrim içi ortama taşımış; Baidu, Alibaba ve Tencent gibi şirketler Çin'in ulusal yenilik kapasitesinin sembolleri olarak küresel teknoloji sahnesinde yerini almıştır. Rogier J.E.H. Creemers, "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century", **Journal of Contemporary China,** Vol.26, No.103, 2017, s.85.

[421] Creemers, *"The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies",* s.130.

[422] Çin Sanayi ve Bilişim Teknolojileri Bakanlığı (MIIT) tarafından yayınlanan 2017 Internet Domain Name Management Rules (İnternet Alan Adı Yönetim Kuralları), m. 37: bkz. China Copyright and Media, Internet Domain Name Management Rules: Opinion Seeking Revision Draft, 25 Mart 2016, https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/ (E.T.: 14.12.2024).

[423] Çin 2021 Veri Güvenliği Yasası m. 22-24: bkz. Stanford University (DigiChina Project), Translation: Data Security Law of the People's Republic of China, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (14.12.2024).

[424] Çin 2017 Siber Güvenlik Yasası m. 37: bkz. Stanford University (DigiChina Project), Translation: Cybersecurity Law of the People's Republic of China, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (14.12.2024).

[425] 2021 Kişisel Bilgilerin Korunması Yasası (Personal Information Protection Law, PIPL), m. 38, 40: bkz. Stanford University (DigiChina Project), Translation: Personal Information Protection Law of the People's Republic of China (effective Nov. 1, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (14.12.2024).

[426] Ayrıca 2021 Kişisel Bilgilerin Korunması Yasası (Personal Information Protection Law, PIPL), m. 53'te yerel temsilci bulundurma zorunluluğu düzenlenmiştir.

Çin'in dijital egemenlik anlayışının üçüncü boyutu, siber uzayda hem vatandaşlar hem de yabancı aktörler üzerinde tam düzenleyici yetki talep eden ve devletlerin kendi dijital sınırları içinde mutlak otoriteye sahip olması gerektiğini uluslararası mecralarda savunan bir modeldir. Bu yaklaşım, Batı'nın çok paydaşlı internet yönetişimine karşı devlet-merkezli, egemenlik temelli bir alternatif sunar ve ABD'nin dijital alandaki baskın pozisyonuna tepki niteliği taşır. Bu tutum, Çin'in genel dış politika vizyonunun dijital alandaki yansımasıdır ve Beijing Konsensüsü olarak adlandırılan çerçevenin bir parçasıdır. Beijing Konsensüsü; ABD hegemonyasına doğrudan meydan okumadan, çok taraflılık ve kültürel-siyasal çeşitlilikleri tanıyan, homojenleştirici evrensel normlara karşı ortaklık-farklılık dengesine dayalı yeni bir küresel düzen tahayyülü sunar. Bu model, ulus-ötesi şirketlerin Çin kurallarına uyma eğilimi sayesinde küresel sermayeyi de etkisi altına alarak "küresel sermayenin Çin'e uyum konsensüsü" olarak da yorumlanmaktadır[427]. Çin ve Rusya, dijital egemenlik anlayışını uluslararası alanda meşrulaştırmak için BM'ye sundukları Davranış Kuralları Taslakları'nda dijital altyapı ve içerik üzerindeki devlet yetkisini vurgulamışlardır[428]. 2012 ITU Zirvesi[429] ve 2018 BM Açık Uçlu Çalışma Grubu[430] gibi platformlarda ABD'ye karşı devlet-temelli yönetim modelini savunmuşlardır[431]. Çin ayrıca ICANN'in yetkilerinin devletlere devredilmesini ve ITU çatısına taşınmasını önermiş, böylece çok paydaşlı yapıdan devlet merkezli bir internet yönetişimine geçişi kurumsallaştırmaya çalışmıştır[432]. Çin, 2012 Budapeşte Konferansı'ndan itibaren her devletin kendi tarihî ve kültürel değerlerine uygun dijital politika belirleme hakkını savunmuş; bu anlayış 2015 Wuzhen Bildirisi[433] ve 2017 Uluslararası Siber Uzay İş Birliği Stratejisi ile sistematik hâle gelmiştir. Strateji, BM Şartı'ndaki egemenlik ilkesinin siber uzayda da geçerli olduğunu ve hiçbir ülkenin bilgi teknolojilerini başka devletlerin iç işlerine müdahale amacıyla kullanmaması

---

[427] Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.161.
[428] Jack Margolin, "Russia, China, and the Push for 'Digital Sovereignty'", *Globalvioces*, 2 Aralık 2016, https://tr.globalvoices.org/2016/12/rusya-cin-ve-dijital-egemenlik-ihtiyaci/ (1 Şubat 2026); Zhang ve Creemers, s.8.
[429] Alexander Klimburg, **"The Internet Yalta."** Center for a New American Security, Washington D.C., 2013, s.3.
[430] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.115.
[431] Zhang ve Creemers, s.1, 2.
[432] Creemers, "*China's Approach to Cyber Sovereignty"*, s.11.
[433] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.153.

gerektiğini vurgular[434]. Çin'in bilgi akışını filtreleme politikası, rejim güvenliğini koruma amacına hizmet ettiği kadar, ülkenin küresel ekonomik ve teknolojik nüfuzunu artıran teorik bir dayanak işlevi görür. Kuşak ve Yol Girişimi kapsamındaki Dijital İpek Yolu, dijital alanın Çin dış politikasında stratejik bir güç projeksiyon aracına dönüştüğünü gösterir[435]. Tüm bu unsurlar, küresel ölçekte devlet-merkezli bir dijital yönetim modelinin meşrulaşmasında kritik bir kırılma noktası oluşturmaktadır[436].

Veri rejimi açısından, Çin'in veri politikaları merkeziyetçi ve denetim odaklıdır. Bunda dijital ekonominin ABD'li büyük küresel platformlarca yönlendirilmesi, kullanıcı verilerinin geniş çapta ticari amaçlarla toplanması, yasa dışı veri ticareti ve artan güvenlik tehditleri gibi gelişmeler etkilidir. Çin'in veri politikaları, veriyi ekonomik değerinin yanı sıra ekonomik istikrar ve siyasal bütünlüğü korumaya yönelik çok katmanlı ideolojik ve siyasi stratejiye dayanır[437]. Bireyin güçlendirilmesini veya temel hakların korunmasını öncelemekten ziyade veriler üzerindeki devlet kontrolünü pekiştirmeyi amaçlar. Özellikle otoriter devlet yapısıyla özel sektörün çıkarlarını birleştiren veri toplama ve izleme mekanizmaları, veri rejimini içe dönük ve güvenlik temelli bir forma sokmaktadır. Büyük veri, medya üretiminden ideolojik çalışmalara kadar birçok alanda bilgi üretimi ve işlenmesinin stratejik bir aracı olarak değerlendirilir[438]. Sosyal düzenin yanı sıra sansürden algoritma denetimine ve uluslararası dijital ilişkilerden ulusal siber güvenliğe kadar siyasi ve ideolojik bir araç olarak kullanılmaktadır. Bu yapının en belirgin örneği, bireylerin davranışlarını puanlayarak hizmetlere erişimi düzenleyen Sosyal Kredi Sistemi'dir[439].

---

[434] 2017 tarihli Uluslararası Siber Uzay İş birliği Stratejisi, Temel Prensipler, Xinhua News English, "(Başlık Belirtilmemiş)", http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm (14.12.2024), Egemenlik Prensibi kısmı.

[435] Dennis Broeders, Liisi Adamson ve Rogier Creemers, "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace", **The Hague Program For Cyber Norms Policy Brief,** Vol. November, 2019, s.2, 3.

[436] Negro, s.163.

[437] Rogier J.E.H. Creemers, "China's emerging data protection framework", **Journal of Cybersecurity,** Vol.8, No.1, 2022, s.3.

[438] Creemers, *"Disrupting the Chinese State: New Actors and New Factors",* s.178.

[439] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.9.

Çin veri hukuku; kişisel verilerin korunması ve veri güvenliği olmak üzere iki temel eksende şekillenmektedir. 2021'de yürürlüğe giren Kişisel Bilgilerin Korunması Yasası (PIPL) ve Veri Güvenliği Yasası (DSL) ile süreç daha sistematik bir yapıya kavuşmuştur. PIPL, birey-şirket ilişkisini düzenlerken; DSL, ulusal güvenlik ve kamu yararına odaklanır. Ancak her iki yasa da devletin veri toplama ve işleme yetkilerine kayda değer sınırlamalar getirmez. Kişisel Bilgilerin Korunması Yasası (PIPL), kamu kurumlarında veriyle ilgili suistimalin önlenmesi için yetki ve sorumlulukların belirlendiği disiplinli bir idari sistem kurulmasını öngörmüştür[440].

Bu düzenlemeler, GDPR etkisiyle şeffaflık, veri minimizasyonu, amaçla sınırlılık ve hesap verebilirlik gibi ilkeler barındırsa da AB'deki gibi gizliliği temel bir hak olarak görmez. Devlet, gerek duyduğunda kişisel veriler de dahil olmak üzere her türlü veriye erişme yetkisini veri koruma mevzuatının temel dayanaklarından biri olarak saklı tutmaktadır. Bununla birlikte, 2017 tarihli Siber Güvenlik Yasası, kritik bilgi altyapısı işletmecilerinin sunduğu hemen hemen tüm dijital hizmetlerde verilerin Çin sınırları içinde depolanması yükümlülüğünü yani veri yerelleştirmesini zorunlu hâle gelmiştir. Ayrıca Çinli şirketlerin yurt içinde ve dışında topladığı verilerin yurt dışına aktarımı devlet onayına tabi tutulması kapalı bir veri ekosistemi inşa edildiğini göstermektedir. Öte yandan DSL, verileri ekonomik ve toplumsal değerine ve kötüye kullanım riskine göre sınıflandırmakta; ulusal güvenlik, ekonomi ve temel kamu hizmetlerine ilişkin verileri 'çekirdek ulusal veri' kategorisi altında ayrı bir önceliklendirmeye tabi tutmaktadır. Çin, bu yolla dijital alanda stratejik özerkliğini tahkim ederken, küresel veri akışlarına sınırlı katılım göstermektedir. Creemers, DSL'in verinin kötüye kullanımından doğabilecek ekonomik, sosyal ve siyasi risklere odaklandığını ve bu yaklaşımın AB'nin kişisel veri odaklı gizlilik anlayışından ve ABD'nin güvenlik normlarına dayalı NIST çerçevesinden farklılaştığını[441] ve Çin'in veri

[440] Creemers, *"China's emerging data protection framework",* s.1, 8.
[441] Creemers, *"China's emerging data protection framework",* s.7, 9.

yaklaşımının dijital alanın küresel ölçekte siyasi ve normatif rekabetin konusu hâline gelmesine katkı yaptığını vurgulamaktadır[442].

Sonuçta Çin'in dijital egemenlik modeli, egemenliği hukuki, siyasal ve ideolojik boyutlarıyla dijital çağda yeniden tanımlayan, merkezi kontrolü güçlendiren ve dışa bağımlılığı azaltmayı hedefleyen kapalı bir düzendir. Modern egemenlik ilkelerini dijital çağın meydan okumalarına uyarlayan bu model, küreselleşme ve dijitalleşmenin ulus-devleti zayıflatan etkilerine karşı egemenliğin yeniden tesisi biçiminde yorumlanabilir. Ancak bu model, otoriter ve izolasyonist bir nitelik taşıdığı gibi, devletin güçlenmesini bireysel hakların geri plana itilmesi pahasına sağlamaktadır. Sistematik uygulandığında dijital totalitarizm riski barındırır[443]. Bu nedenle dijital egemenliğin yeniden inşası; güvenlik ve kontrol kadar özgürlük, katılım ve meşruiyet dengelerini gözeten daha kapsayıcı bir çerçevede ele alınmalıdır.

d. AB: Hak ve Değer Temelli Bir Dijitalleşme Modeli

Avrupa Birliği, bir devlet olmamakla birlikte üye ülkelerden bağımsız bir hukuk düzenine sahiptir ve temel amacı hukukun entegrasyonu değil pazar bütünleşmesidir[444]. Dijital dönüşümü teknik bir süreçten öte, insan hakları, etik değerler ve sürdürülebilirlik ekseninde değerlendirdiği iddiasındadır[445]. AB'nin dijital politika çerçevesi; gizlilik, veri koruma, rekabet, fikri mülkiyet, nefret söylemi ve yapay zekâ gibi geniş bir alana yayılarak dijital platformların gücünü sınırlamayı ve hakları korumayı amaçlar[446]. İnsan merkezli, değer temelli ve dengeli bir düzenleme modeli benimseyen AB, dijital ekonomiyi teşvik ederken hak ve özgürlüklerin güvence altına alınmasını hedefler[447]. Bununla birlikte düzenlemeleri, özel hukuk-kamu hukuku ayrımını esas almayan karma nitelikte ve sistematikliği zayıf bir yapı sergiler.

---

[442] Creemers, *"The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies",* s.133-134.
[443] Schneider, *China's Digital Nationalism,* s.207.
[444] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.96.
[445] European Commission, European Declaration on Digital Rights and Principles, 2022, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles, Başlangıç, par. 5.
[446] Christakis, s.16.
[447] Christakis, s.11.

Avrupa Birliği'nin dijital egemenlik yaklaşımı kontrol ve meşruiyet olmak üzere iki ayrı eksende şekillenmektedir.

AB açısından kontrol; hukuki ve teknik araçların tesisinde oluşur ve veri yönetimini dijital egemenliğin çekirdeğine yerleştirmekle başlar. Veri akışlarının denetimi, veri mahremiyetine dair yüksek standartlar ve veri üzerinde tasarruf hakkı, bu politikaların merkezindedir. Hukuki kontrol açısından, GDPR hem bireysel hakları koruyan hem de veri hakimiyeti temelli ekonomik-siyasal kapasiteyi artıran başlıca araçtır[448]. GDPR ve Schrems kararları, Brüksel Etkisi yani AB'nin veri egemenliğini sınırlarının ötesine taşıyarak küresel norm koyucu hâline geldiğini gösterir[449]. AB'nin önceliğinin dijital egemenlik yarışını kazanmak değil, kural koyucu olmak olduğu ileri sürülse[450] de bu yaklaşımın dijital egemenliğini pekiştirdiği görülmektedir. Nitekim 1995 tarihli Veri Koruma Direktifi'nden bu yana, özellikle GDPR ile şirketler; şeffaflık, veri minimizasyonu, amaçla sınırlılık gibi ilkelere uymaya zorlanmaktadır. Dijital platformlara yönelik Dijital Hizmetler Yasası (DSA) ve Dijital Pazarlar Yasası (DMA), teknoloji şirketlerinin özellikle Avrupa dijital pazarında daha sıkı bir denetime tabi olmasını öngörmektedir. DSA, sistemik risklere karşı platformlara yükümlülükler getirirken; DMA, piyasa gücünü tekelleştiren aktörlere karşı rekabeti teşvik etmeyi hedefler. Doktrinde DSA, içerik denetimi ve itiraz mekanizmaları gibi kamusal nitelik taşıyan düzenleyici ve yargısal yetkilerin büyük ölçüde yine platformlara bırakılması nedeniyle eleştirilmiştir. Bu yetkilerin fiilen platformlar tarafından kullanılması, Big Tech şirketlerinin gücünün ve meşruiyetinin daha da pekişmesi riskini doğurmaktadır. Bu sebeple, yalnızca platform temelli düzenlemelerle yetinilmeyip rekabet hukuku, adil

[448] Roberts ve Diğerleri, s.8.

[449] Anu Bradford'un tanımladığı bu etki, AB'nin hukuk normlarını tek taraflı olarak küreselleştirme gücüdür. AB'nin GDPR, Avrupa Adalet Divanı kararları, direktif ve tüzükler gibi sert hukuk araçlarının yanı sıra gönüllü standartlar ve rehber ilkeler gibi yumuşak hukuk araçları hem devletlerin iç hukuklarını hem de küresel teknoloji şirketlerinin stratejilerini etkileyerek dijital piyasalarda belirleyici rol oynamakta; kendi normlarını küresel ölçekte kabul ettirebilmektedir. Christakis, s.13, 14.

[450] Guntram Wolff, "Europe may be the world's AI referee, but referees don't win", *Politico,* 17 Şubat 2020, https://www.politico.eu/article/europe-may-be-the-worlds-ai-referee-but-referees-dont-win-margrethe-vestager/ (1 Şubat 2026)

vergilendirme rejimleri ve dijital anayasacılık gibi alternatif ve tamamlayıcı araçların geliştirilmesi zorunlu görünmektedir[451].

Dijital egemenliğin sürdürülebilirliği güçlü bir siber güvenlik mimarisine dayanır. NIS Direktifi, Siber Güvenlik Yasası ve 2020 Siber Güvenlik Stratejisi, AB'nin kritik altyapıları koruma ve ortak güvenlik standartları oluşturma çabasını temsil eder. Bu düzenlemeler, dijital kamu düzeninin yeniden inşası çabası olarak değerlendirilebilir[452]. Buna karşın araştırmacılar, veri koruma standartlarının sıkı olduğu rejimlerde, büyük veri ve yapay zekâ gibi yenilikçi alanlarda gelişimin yavaşlayabileceğini iddia etmekte[453] daha esnek düzenleme çerçevelerine sahip ülkelerin rekabet avantajı elde edebileceğini savlamaktadır[454]. Bu bağlamda AB'nin katı veri koruma rejimi, kimi zaman dijital inovasyonun önünde bir engel olarak algılanmaktadır[455].

Veri üzerinde AB egemenliğinin maddi temelini bağımsız dijital altyapılar yani teknik kontrolü sağlayan araçlar oluşturur. Covid-19 sürecinde Apple ve Google'ın teknik belirleyiciliği, dijital egemenliğin yalnızca hukuk yoluyla değil teknolojik özerklikle mümkün olabileceğini göstermiştir. Bu nedenle AB, bulut ve veri depolama alanında dışa bağımlılığı azaltmayı hedeflemekte; GAIA-X gibi projeler bu doğrultuda geliştirilmektedir. Ancak Google ve Amazon gibi küresel teknoloji devlerinin bu projelerde yer alması, stratejik özerklik iddiasını zayıflatmaktadır[456]. Yapay zekâ, yarı iletkenler ve süper bilgisayar yatırımları artmış olsa da özellikle mikroçip üretimi gibi alanlarda hedeflerin gerçekleştirilmiş olmaması ABD ve Çin karşısında hâlen sınırlı düzeyde olduğunu göstermektedir.

---

[451] Coroado, s.19.
[452] Roberts ve Diğerleri, s.10, 13.
[453] WTO, World Trade Report 2018 The future of world trade: How digital technologies are transforming global commerce, 2018, https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (1 Şubat 2026), s.140.
[454] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.5.
[455] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.237-238.
[456] Roberts ve Diğerleri, s.14-15.

AB, teknik kapasiteyle birlikte etik temelli küresel teknoloji politikaları geliştirmeye çalışmaktadır. Yapay zekâ kullanımında etik ve insan hakları kriterlerine bağlı kalmayı esas alan Global Partnership on Artificial Intelligence (GPAI) gibi oluşumlar bu yaklaşımı yansıtır[457]. Bununla birlikte etik merkezli bu modelin uzun vadede rekabet ve inovasyon açısından pragmatik, piyasa odaklı stratejilerine kıyasla dezavantaj yaratabileceği yönünde eleştiriler bulunmaktadır[458].

Dijital egemenlik yalnızca teknik ve hukuki kontrolle değil, aynı zamanda meşruiyetle de ilgilidir; bir meşruiyet meselesidir. Meşruiyet; yurttaş katılımı, karar alma süreçlerinin şeffaflığı ve politika sonuçlarının etkililiği olmak üzere üç düzeyde değerlendirilebilir. Ancak yurttaş katılımının sınırlı olması[459] ve teknoloji şirketlerinin yüksek düzeyli lobi faaliyetleri demokratik meşruiyeti zayıflatır. Bu koşullar altında AB, dijital egemenlik konusunda bütünlüklü ve sürdürülebilir bir model geliştirmekte zorlanmaktadır[460]. Zira büyük teknoloji şirketleri zamanla fiilî güçlerini meşru normlara dönüştürebilmektedir. Kullanıcı bağlılığı kimi zaman vatandaş-devlet ilişkisinin önüne geçmekte; bu da platform şirketlerini demokratik denetim dışı iktidar hâline getirmektedir[461].

AB, 23 Ocak 2023 tarihli Dijital Haklar ve İlkeler Deklarasyonu'yla dijitalleşme vizyonunu resmileştirmiştir. Deklarasyon, dijital dönüşümün fırsatlar kadar haklar ve demokrasi açısından riskler barındırdığını vurgular; çevrimdışı ortamdaki yasakların çevrimiçi için de geçerli olması gerektiğini belirtir[462]. Dijital egemenlik; temel haklar, hukukun üstünlüğü, demokrasi, eşitlik, erişilebilirlik ve sürdürülebilirlik ilkelerine dayandırılır[463].

---

[457] Christakis, s.35.
[458] Roberts ve Diğerleri, s.11-12.
[459] Roberts ve Diğerleri, s.16.
[460] Floridi, s.376-377.
[461] Pepper D. Culpepper ve Kathleen Thelen, "Are We All Amazon Primed? Consumers and the Politics of Platform Power". **Comparative Political Studies,** Vol.53, No.2, 2020, s.295.
[462] European Commission, *European Declaration on Digital Rights and Principles,* par.2, 3.
[463] European Commission, *European Declaration on Digital Rights and Principles,* par.6.

Deklarasyonun ilk ilkesi, dijital dönüşümün merkezine insanı yerleştirir. Dijitalleşmenin Avrupa değerleri doğrultusunda bireyleri güçlendirmesi; toplum ve ekonomi için ortak yarar üretmesi hedeflenir(par.3).

İkinci ilke, kapsayıcılık ve dayanışmadır. Herkesin uygun fiyatlı bağlantıya, dijital okuryazarlığa ve güvenli çalışma koşullarına erişimi temel hak sayılır(m.2-4.). Çalışanların mahremiyet, örgütlenme ve bağlantıyı kesme hakkı korunur; yapay zekâ uygulamalarında şeffaflık ve risk bazlı denetim öngörülür(par.6). Dijital kamu hizmetlerine erişim de temel hak olarak tanımlanır. Bu kapsamda, bireylerin çevrimiçi kamu hizmetlerine erişim sağlarken gereksiz veri paylaşımına zorlanmaması gerektiğinin üzerinde durulur(m.7).

Üçüncü ilke, dijital dönüşümde seçim özgürlüğünü vurgular. Yapay zekâ ve algoritmaların ayrımcılığa yol açmaması, insan denetimi altında olması ve bireylerin çevrimiçi hizmetleri objektif bilgilere dayanarak seçebilmesi hedeflenir. Özellikle sağlık, eğitim, istihdam ve özel yaşam gibi hassas alanlarda bu teknolojilerin bireylerin tercihlerini önceden tahmin etmeye yönelik araçlar olarak kullanılmaması gerekir (m.9). KOBİ'lerin yenilik yapabilmesi için adil rekabet ortamı talep edilir (m.10, 11).

Dördüncü ilke, dijital kamusal alana katılım hakkıdır. Güvenilir ve çoğulcu içeriklere erişim, ifade ve örgütlenme özgürlüğü, medya şeffaflığı ve zararlı içeriklere karşı korunma bu kapsamda yer alır. Hedefli reklamlarla bireylerin manipüle edilmesine karşı koruma vurgulanır (m.12-15).

Beşinci ilke, dijital güvenlik ve bireyin güçlendirilmesidir. Gizlilik ve siber güvenlik temel hak olarak görülür; bağlantılı ürünlere yönelik güvenlik standartları öngörülür (m.16). Bireylerin verileri üzerindeki kontrolü güçlendirilir; çocukların ve gençlerin dijital ortamda korunması öncelik hâline getirilir (m.17-20). Bu bağlamda AB için veri egemenliği meselesi, dijital çağda devletlerin hem kendi vatandaşlarını koruma hem de uluslararası dijital düzende söz sahibi olma çabalarının kesiştiği kritik bir alandır. AB'nin veri koruma konusundaki öncü rolü, sadece ekonomik çıkarların değil, aynı zamanda birey haklarını merkeze alan bir dijital egemenlik anlayışının göstergesidir. Bu

yaklaşım, devletin dijital alanı düzenleme yetkisinin yalnızca teknik bir müdahale değil, aynı zamanda normatif ve değer temelli bir müdahale olduğunu ortaya koymaktadır.

Altıncı ilke sürdürülebilirliktir. Dijital ürünlerin çevre dostu tasarımı, döngüsel ekonomiyle uyumluluğu ve enerji verimliliği hedeflenir. Kullanıcıların ürünlerin çevresel etkilerine ilişkin şeffaf bilgiye erişimi güvence altına alınır; AB, yeşil dijital teknolojilerin geliştirilmesini taahhüt eder (m.23, 24).

Veri rejimi açısından, Avrupa Birliği, veri yaklaşımını temel haklar ile ekonomik serbestlik arasında denge kurma hedefi doğrultusunda şekillendirerek ABD ve Çin'in veri politikalarından farklı bir rota izlemektedir. AB, veriyi dijital ekonominin asli kaynağı olarak görürken verinin serbest dolaşımını iç pazarın bütünlüğü açısından vazgeçilmez bir unsur olarak değerlendirir. Veriye ilişkin tüm düzenleyici süreci; bireysel mahremiyet ve veri özerkliğini tavizsiz biçimde önceleyen, güçlü, istikrarlı ve değer merkezli bir temel haklar rejimi etrafında inşa etmektedir. Bu bağlamda hem piyasa düzenleyicisi hem de hak koruyucu bir aktör konumundadır[464]. Bireyin veri özerkliği AB Temel Haklar Şartı'nın 8. maddesinde, temel hak olarak kabul edilmiştir. GDPR ve Avrupa Adalet Divanı'nın (CJEU) kararları[465] veri sahiplerine etkin kontrol hakkı tanıyan bu yaklaşımı kurumsallaştırmıştır[466]. Ancak, kişisel veri kavramının geniş yorumlanması ve tanımlanabilirlik ölçütlerindeki belirsizlik[467] AB'nin hem kamu hem özel sektör üzerindeki düzenleyici etkisini genişleterek veri alanındaki güç dengesini Brüksel

[464] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.6.

[465] ABAD, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzále, 13 Mayıs 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131; ABAD, Maximillian Schrems v Data Protection Commissioner, 6 Ekim 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362#c-ECR_62014CJ0362_EN_01-E0001; ABAD, Digital Rights Ireland and Seitlinger v Minister for Communications, Marine and Natural Resources, 8 Nisan 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293.

[466] Kristina Irion, "A special regard: The Court of Justice and the fundamental rights to privacy and data protection" U. Faber ve Diğerleri (Ed.), **Gesellschaftliche Bewegungen—Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte** içinde (873-890), Nomos, 2016, s.881-887.

[467] Josef Drexl, "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", Alberto Di Franceschi ve Reiner Schulze (Ed.), **Digital Revolution: New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies**, içinde (19–41), H. Beck; Nomos, 2019, s.20.

merkezli bir yapı lehine dönüştürdüğü eleştirisine neden olmuştur[468]. AB veri stratejisi, dijital hizmetlerin sınır ötesi yapısı nedeniyle üçüncü ülkelerin yargı talepleriyle yaşanabilecek çatışmalara karşı AB'nin küresel ölçekte yayılmacı norm belirleyici aktör olarak konumlanması çabası olarak görülmüştür[469]. Açık Veri Direktifi (EU 2019/1024) ve diğer sektörel düzenlemeler üzerinden özel sektörün açık veriye erişimi kolaylaştırılırken, kamu otoritelerinin denetim yetkileri de genişletilmektedir. Verinin kamu yararına yeniden kullanımı, yalnızca şeffaflık ve verimlilik açısından değil, bilgi üretimi ve kontrolü üzerindeki hakimiyetini kamusal alana taşınması olarak da eleştirilmiştir[470].

Sonuç olarak; veri yönetimi, platform düzenlemeleri, altyapı yatırımları ve stratejik teknoloji geliştirme, AB için dijital çağda ulusal güvenliği yeniden tanımlayan hukuki ve teknik boyuttan oluşan temel araçlardır. Birlik, dijitalleşmeye müdahalede birey haklarını, toplumsal değerleri ve etik ilkeleri merkeze alan bir yaklaşım benimser. Ancak bu modelin sürdürülebilirliği, yalnızca normatif düzenlemelerin küresel etki yaratmasına değil, aynı zamanda Avrupa merkezli teknoloji üretiminin güçlendirilmesine ve yurttaş katılımını artıracak demokratikleşme adımlarının atılmasına bağlıdır. AB, rekabet gücünü artırmaya yönelik proaktif sanayi politikaları geliştirmedikçe dijital egemenlik iddiasını uzun vadede korumakta zorlanacaktır[471].

AB'nin kişisel verilere ilişkin temel haklar eksenli yaklaşımı, küresel dijital düzenin çok kutuplu yapısı içinde izole bir şekilde işlememekte; ABD ve Çin gibi diğer büyük güçlerin veri yönetişimi rejimleriyle sürekli bir etkileşim ve gerilim içerisindedir. Bu bağlamda, iki kutup arasında konumlanan AB'nin veri modeli yalnızca bir normlar bütünü değil, aynı zamanda küresel dijital egemenlik mücadelesinde bir stratejik pozisyondur.

---

[468] Nadezhda Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", **Law, Innovation and Technology,** Vol.10, No.1, (2018), s.42.
[469] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.8.
[470] European Commission, *A European strategy for data*, s.3-5.
[471] Roberts ve Diğerleri, s.19.

Devletlerin veri rejimleri, dijital egemenlik mücadelesinin belirleyici alanı hâline gelmiştir. Veri akışının kontrolü, yerelleştirme politikaları, bağımsız denetim yapıları, platform regülasyonları ve uluslararası standart oluşturma çabaları; devletlerin hem dijital güvenliklerini hem ekonomik rekabet güçlerini hem de kamusal otoritelerini yeniden tanımladıkları stratejik araçlara dönüşmüştür. Bu farklı veri modelleri arasındaki gerilim, dijital dünyanın yeni küresel güç mücadelesinin de temel eksenini oluşturmaktadır.

3. Dijital Egemenlik Konuları: Devletin Dijital Alanı Düzenleme Araçları

a. Ulusal ve Uluslararası Hukuki Mekanizmalar

Dijitalleşmeyle birlikte artan veri işleme kapasitesi; özel hayat ve kurumsal mahremiyet açısından yeni riskler doğurmuş; bu durum devletleri dijital alanda hukuki düzenlemeleri güçlendirmeye zorlamıştır[472]. İnternetin yaygınlaşmasıyla ulusal ve uluslararası hukukun dijital alana uygulanacağı genel kabul görmüş[473] devletler egemenliklerini sibernetik[474] bir çerçevede: erişim kontrolü, içerik düzenlemesi, teknik müdahaleler ve algoritmik regülasyon yoluyla sürdürmeye yönelmiştir.

Devletlerin dijital alandaki egemenliğini sürdürmesi esas olarak hukuki düzenlemeler aracılığıyla gerçekleşir. Devlet iktidarının ayırt edici özelliği, yetkisini kullandığı kişilere iradesini bağlayıcı biçimde kabul ettirebilmesidir. Bu bağlayıcılık, bireylerin rızasından bağımsız olarak anayasa, kanun, kararname, yönetmelik ve idari kararlar gibi normatif işlemler yoluyla somutlaşır[475].

---

[472] Çağla Tansuğ, "Veriye Teknolojik ve Hukuki Yaklaşım Değişikliğinin Kamu Hizmeti Sunumu Alanındaki Etkileri", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (39-60), İstanbul: Adalet, 2021, s.52-53.

[473] Duncan B. Hollis, "A Brief Primer on International Law and Cyberspace", *Carnegie Endowment for International Peace,* 14 Haziran 2021, https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en (1 Şubat 2026).

[474] Sibernetik kelimesi etimolojik olarak Yunanca κυβερνήτης (kybernētēs) kelimesinden gelmektedir, bu kelime dümenci veya yönetici anlamına gelir. Vali anlamına gelen sözcük İngilizce governor kelimesi de şaşırtıcı biçimde Yunanca κυβερνήτης kelimesinin Latinceye değiştirilerek aktarılmasına dayanmaktadır. Norbert Wiener, **Cybernetics: or Control and Communication in the Animal and the Machine**, 2. Baskı, Massachusetts: The MIT Press, 1961, s.11.

[475] Uygun, s.11.

Dijitalleşmenin temeli verinin algoritmik işlenmesine dayandığından bu bağlamda öne çıkan algoritmik regülasyon kavramı da devletin algoritma ile regülasyon faaliyetlerini gerçekleştirmesi ve algoritmaları regüle etmesi anlamı taşır[476]. Bu bağlamda algoritmalar hem düzenleme aracı hem de düzenleme konusu hâline gelmiştir. Bu düzenleyici kapasite, teknolojik gelişmelere yetişmekte zorlanmasına ve düzenlemelerin yenilikleri engellediği eleştirisine[477] rağmen, devletin kullanıcı davranışlarını ve dijital alanın normatif yapısını belirleme gücünü koruduğunu göstermektedir.

Uluslararası düzeyde ise devletler, bağlayıcı olmayan soft law araçları, teknik standartlar, patentler ve ITU-ICANN gibi kurumsal yapılar üzerinden dijital yönetişimde etkilerini artırarak devlet otoritesini tahkim etmektedir[478]. Özellikle Çin'in bu kurumlarda görünürlüğünü artırarak alternatif yönetişim modelleri geliştirme çabaları bu sürecin somut örneklerindendir[479].

(1) Veri Akışının ve Platform Ekosisteminin Regülasyonu

Devletler, internet teknolojilerine yönelik mevzuat ve idari pratikler yoluyla, kendi ulusal sınırları içinde internetin gelişim seyrini ve kullanım biçimlerini yönlendirme gücüne sahiptir. Bu bağlamda bireylerin hangi içeriklere, hangi yollarla ve hangi nedenlerle erişebildiği ya da erişemediği; bulundukları hukuki düzen, ekonomik yapı, siyasal ortam ve toplumsal koşullara göre belirlenmekte ve bu unsurlar doğrultusunda değişkenlik arz etmektedir[480].

Devletler, dijital alan üzerindeki egemenliklerini tesis etmek için veri akışını, dijital platformları ve teknoloji ekosistemini giderek daha sıkı biçimde düzenlemektedir. Kişisel verilerin korunmasına ilişkin yasalar dünya genelinde yaygınlaşmış; Avrupa'dan Asya'ya, Latin Amerika'dan Afrika'ya kadar çok sayıda ülke kendi veri rejimini oluşturarak veri işleme süreçlerine haklar, yükümlülükler ve yaptırımlar getirmiştir:

[476] Erol, s.8-9.
[477] Floridi, s.371.
[478] Lina Benabdallah, **Shaping the Future of Power: Knowledge Production and Network-Building in China-Africa Relations.** Ann Arbor: University of Michigan Press. 2020, s. 42-43.
[479] Negro, s.153.
[480] Akdenizli, s.33.

Avustralya'da Gizlilik Yasası[481], Japonya'da Kişisel Bilgilerin Korunması Yasası[482] ve Bilgi Güvenliği Temel Yasası[483], Rusya'da Bilgi, Bilgisel Teknolojiler ve Bilginin Korunması Yasası[484], Brezilya'da Genel Veri Koruma Yasası[485], Türkiye'de 2016'da yürürlüğe giren Kişisel Verilerin Korunması Kanunu, İspanya'da Kişisel Verilerin Korunması Yasası[486] ve Dijital Haklar Bildirgesi[487], Çin'de Veri Güvenliği Yasası[488] ve Kişisel Bilgilerin Korunması Yasası[489], Afrika Birliği Veri Koruma İlkeleri[490] ve Asya-Pasifik Ekonomik İşbirliği Veri Koruma Çerçevesi[491] örnek verilebilir. Dijital platformların küresel hizmet veren oluşumlar olması nedeniyle düzenlemelerin tek tek her ülke tarafından yapılması etkinliğini azaltmakta küresel ya da kıtasal yapıldığında düzenlemelerin yaptırım gücünü artırmaktadır[492].

Bu düzenlemeler, bireylerin haklarını korurken dijital platformları daha denetimli hâle getirir ve devletin veri üzerindeki egemenliğini güçlendirir. Kişisel

---

[481] Federal Register of Legislation, legislation.gov.au, Privacy Act 1988, https://www.legislation.gov.au/C2004A03712/latest/text (14.12.2024).

[482] Japanese Law Translation, Act on the Protection of Personal Information, 2003, https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (14.12.2024).

[483] Japanese Law Translation, Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers, 2005, https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en (14.12.2024).

[484] World Trade Organization (WTO), WT/ACC/RUS58/LEG/369, 2006, https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf (14.12.2024).

[485] LGPD Brasil, Brazilian General Data Protection Law (LGPD) English Version, 2020, https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf (14.12.2024).

[486] Resmi adı: Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), GDPR'a ek düzenlemeler içeren bu yasa 2018'de yürürlüğe girdi. GDPRhub, Data Protection in Spain, https://gdprhub.eu/Data_Protection_in_Spain (14.12.2024).

[487] Resmi adı: Carta de Derechos Digitales, dijital kimlik hakkı da düzenleyen bu rehber metin 2021'de yayınlandı. Gobierno de España, Ministerio de Asuntos Económicos y Transformación Digital, Carta de Derechos Digitales, https://portal.mineco.gob.es/recursosarticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/sediacartaderechosdigitales.pdf (14.12.2024).

[488] İngilizce: Data Security Law, 2021'de yürürlüğe girdi. National People's Congress (NPC) of the People's Republic of China, Announcement on Adoption of the Personal Information Protection Law, http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (14.12.2024).

[489] İngilizce: Personal Information Protection Law (PIPL), 2021'de yürürlüğe girdi. National People's Congress of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (14.12.2024).

[490] İngilizce: African Union Convention on Cyber Security and Personal Data Protection, 2014'te kabul edildi. African Union, Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (14.12.2024).

[491] İngilizce: APEC Privacy Framework, 2005'te kabul edilmiş, 2015'te revize edilmiş ve 2017'de güncellenmiştir. Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework (2015), https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (14.12.2024).

[492] Işık, s.3.

verilerin işlenmesinde, bireyin verilerini öğrenme, sildirme ve paylaşımı engelleme gibi hakları; veri işleyenlerin şeffaflık ve sorumluluk yükümlülükleri, gizlilik ihlallerinde uygulanacak protokoller ve yaptırımlar yer almaktadır. Örneğin, California Tüketici Gizliliği Yasası, bireylere kişisel verileri üzerinde kontrol imkânı tanımış kişilerin, şirketlerin hangi kişisel verileri topladığını öğrenme hakkı (m. 1798.100), kişisel verilerinin silinmesini talep etme hakkı (m. 1798.105), ve verilerinin üçüncü taraflarla paylaşılmasını engelleme hakkı (m. 1798.120) düzenlenmiştir[493].

Devletler, yasalarla dijital alanı düzenleyerek kamu ve özel sektörde bilgi güvenliğini sağlar. Türkiye'de, 5809 sayılı Elektronik Haberleşme Kanunu ve Bilgi Teknolojileri ve İletişim Kurumu Yetkilendirme Yönetmeliği çerçevesinde, elektronik haberleşme alanında faaliyet gösterecek özel işletmeciler, sundukları hizmetin niteliğine göre Kurumdan yetkilendirme almak zorundadır. Bu yetkilendirme rejimi, veri akışının ve platform ekosisteminin kamusal denetime tabi kılınmasını sağlayarak, elektronik haberleşme altyapısının özel aktörler eliyle yürütülmesi hâlinde dahi devletin düzenleyici ve denetleyici otoritesinin tahkim edilmesine hizmet etmektedir. Böylece piyasa serbestisi korunurken; ulusal güvenlik, kamu düzeni ve temel hakların korunması bakımından kamusal çıkar odaklı bir regülasyon mekanizması tesis edilmektedir.

Devletler, kişisel verilerin güvenli, şeffaf işlenmesi için veri yerelleştirmesi uygulayarak kamu hizmetini dijitalleştirir ve dijital iletişimi kontrol altına alır. Örneğin, Rusya'da Federal Kişisel Verilerin Korunması Yasası m.18 gereği kişisel verilerin ülke içindeki sunucularda saklanması zorunludur[494]. ABAD da içtihadında, bağımsız denetim sağlanabilmesi adına özel sektörün hassas veriler içeren veri setlerinin AB sınırları içinde tutulması gerektiğine karar vererek veri yerelleşmesini onaylamıştır[495]. Bu yaklaşım, verilerin ülkede kalmasını, gizli bilgilerin sosyal medya ve mesajlaşmada paylaşılmamasını ve yerli çözümlerin kullanılmasını hedefler. Türkiye'de de kritik

[493] CCPA, 2020'de Kaliforniya'da yürürlüğe girdi. California Privacy Protection Agency (CPPA), California Consumer Privacy Act (CCPA), https://cppa.ca.gov/regulations/pdf/cppa_act.pdf (E.T.: 14.12.2024).
[494] No. 152-FZ, 2006'da yürürlüğe girdi. DataGuidance, Russian Personal Data Federal Law No. 152-FZ, https://www.dataguidance.com/sites/default/files/en_20190809_russian_personal_data_federal_law_2.pdf (14.12.2024).
[495] Yakovleva ve Irion, s.216.

verilerin güvenliği için Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi[496] çıkarılmıştır. Devlet, içerik kontrolü için coğrafi engeller koyar ve yurt dışındaki veri merkezlerine veri aktarımını kısıtlar. Aynı zamanda bireylerin internete özgürce erişimi ve ifade özgürlüğü gibi temel haklarını korur. Örneğin Brezilya'da İnternet için Medeni Haklar Çerçevesi[497] kullanıcı rızası olmadan kişisel veri işlenmesini engellemiş ve internet servis sağlayıcılarının içerik kısıtlamasını yasaklamıştır (m.7 ve 9). Ayrıca, internet servis sağlayıcıları, çevrimiçi platformlar ve veri işleyen kuruluşlara yükümlülükler ve yaptırımlar getirilerek devletin dijital alandaki hukuki müdahalesi güçlendirilmiştir. Sağlık gibi hassas bilgiler için özel düzenlemeler yapılarak dijital sağlık hizmetlerinde veri güvenliği, gizlilik ve yetkisiz erişime karşı koruma sağlanmaya çalışılmıştır[498]. Çocukların çevrimiçi güvenliği için dijital platformlara, çocuklara yönelik içeriklerin denetlenmesi ve verilerin korunması yükümlülüğü getirilmiştir[499].

Veri koruma yasalarının uygulanmasını denetlemek için bağımsız veri koruma otoriteleri[500] kurulmakta ve ihlallerde cezalar uygulanmaktadır. Bu otoriteler, veri işleme süreçlerini izler, tavsiyeler verir, kullanıcıları bilgilendirir, dijital platformların veri kullanımı hakkında şeffaflık raporları yayımlar ve veri ihlallerini kamuoyuna duyurur. Bağımsız veri koruma otoriteleri normların uygulanmasını denetleyerek dijital platformların şeffaflığını artırmakta; nefret söylemi ve dezenformasyonla mücadelede

---

[496] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2019 yılında yayımlamıştır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO), "Türkiye'nin dijital dönüşüm hamlesi", https://cbddo.gov.tr/haberler/6588/turkiye-nin-dijital-donusum-hamlesi (14.12.2024).

[497] Resmi adıyla Marco Civil da Internet-Lei N° 12.965, de 23 de Abril de 2014, 2014'te yürürlüğe girdi. CGI.br (Brazilian Internet Steering Committee), Marco Civil Law of the Internet in Brazil, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180 (14.12.2024).

[498] Dijital sağlık verilerinin korunmasına yönelik örnek düzenlemeler için bkz. Health Insurance Portability and Accountability Act (HIPAA), 1996, https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 (E.T.: 14.12.2024); Almanya E-Sağlık Yasası, 2015, https://www.eprivacy.eu/en/industries/e-health/ (14.12.2024); European Health Data Space (EHDS) Regulation Proposal, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197 (14.12.2024).

[499] Birleşik Krallık'ta yürürlüğe girmesi planlanan Online Safety Bill, ifade özgürlüğünü korumayı, sosyal medya dolandırıcılıklarını önlemeyi ve çocukların dijital ortamda istismarını engellemeyi amaçlamaktadır. The UK Rules, "Online Safety Bill", https://www.theukrules.co.uk/news/children-and-education/online-safety-bill/ (14.12.2024). AB'nin Dijital Hizmetler Yasası (DSA), sosyal medya platformları ve dijital hizmet sağlayıcıları için kapsamlı denetim kuralları getirmektedir.

[500] Devletlerin kurduğu bazı örnek otoriteler şunlardır: Avrupa Veri Koruma Otoritesi (EDPS), İngiltere Bilgi Komiserliği (ICO), Almanya Federal Veri Koruma Ofisi (BfDI), Fransa Veri Koruma Otoritesi (CNIL), İspanya Veri Koruma Ajansı (AEPD), Brezilya LGPD Otoritesi ve Türkiye Kişisel Verileri Koruma Kurumu (KVKK).

davranış kodu gibi yumuşak hukuk araçları da etkili olmaktadır. İhtiyari protokoller; bilişim şirketleri, sivil toplum ve devlet yetkililerinin karşılıklı öğrenip iş birliğini artırmasını sağlamaktadır[501].

Öte yandan, dijital dönüşümle birlikte devletler, kamusal düzeni ve temel hakları koruma sorumluluğu gereği dijital platformların içerik yönetimine doğrudan müdahale eden hukuki çerçeveler geliştirmektedir. Dezenformasyon, nefret söylemi, terör propagandası, çevrim içi dolandırıcılık ve siber zorbalık gibi tehditlerin artması hem toplumsal baskıyı artırmış hem de platformlara daha sıkı yükümlülükler getirilmesini zorunlu kılmıştır[502]. Bu kapsamda platformlara; zararlı içerikleri hızla tespit etme, kaldırma, sahte hesapları engelleme, kullanıcı bildirim ve şikâyet mekanizmalarını etkinleştirme, şeffaflık ve hesap verebilirlik sağlama gibi sorumluluklar yüklenmektedir. İçerik yönetim süreçleri hem insan denetimini hem de algoritmik araçları birleştiren hibrit bir modele dönüşmüştür.

İçerik yönetimi politikaları dezenformasyon arzını kontrol eden çeşitli aksiyonları içermektedir. Bunlar: hesap dondurma/kaldırma, içerik kaldırma veya geri ittirme, algoritmik filtreleme, otomatik tespit sistemi, teyit kuruluşlarıyla iş birliği, içerik etiketleme ve uyarı mekanizmaları ve kullanıcıya doğru bilgiye yönlendiren bilgi panelleri gibi. Facebook ve Instagram, uluslararası doğrulama ağlarıyla iş birliği yaparak içerik etiketleme kararları alırken; Twitter kendi teyit mekanizmasını işletmektedir. YouTube gibi platformlar ise kullanıcıları kritik konularda bilgilendirici panellere yönlendirerek yanlış bilgi riskini azaltmaya çalışmaktadır[503]. Sonuç olarak içerik yönetimi, dijital egemenlik araçlarının merkezinde yer almakta; devletlerin hukuki

---

[501] Örneğin, Avrupa Komisyonu 2016'da Facebook, Twitter ve YouTube ile nefret söylemini önlemek için Davranış Kuralları'nı imzalamış sonrasında Instagram, Snapchat, Google+, Dailymotion (2018), Jeuxvide (2019) ve TikTok (2020) da rızaen katılmış ve bunun sonucunda, 2020'de nefret söylemi içeren içeriklerin yaklaşık %90'ı platformlardan kaldırılmıştır. 2018'de yayımlanan bir başka Davranış Kuralları, sahte haber ve dezenformasyonla mücadele için Facebook, Google, Twitter, Microsoft, TikTok ve Mozilla gibi büyük platformların kendi standartlarını dezenformasyonla mücadeleye gönüllü olarak yönelttiğini göstermektedir. Christakis, s.19, 20.

[502] Schneider, *"Communication and censorship",* s.2.

[503] Simge Andı, "Sahte Haberler ve Sosyal Medya: Yanlış Bilgi Yayılımında Algoritmaların Rolü", **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021, s.8-10.

düzenlemeleri ile platformların teknik kapasitesi arasında giderek daha sıkı bir karşılıklı bağımlılık oluşmaktadır.

Devletler, egemenlik yetkisi kapsamında dijital güvenliği sağlamak, hassas grupları korumak ve dijital hizmetlere erişimi artırmak için sosyal medya ve dijital platformlara kapsamlı hukuki yükümlülükler getirmektedir. Türkiye'de 5651 Sayılı İnternet Kanunu[504] Almanya'da NetzDG[505] Avustralya'da Çevrimiçi Güvenlik Yasası[506] ve Yardım ve Erişim Yasası[507] Fransa'da İnternette Nefret İçerikleriyle Mücadeleye İlişkin Yasa [508] ve Bilgi Teknolojileri (Aracı Kurumlar) Kuralları[509] gibi düzenlemeler bu müdahalelerin örnekleridir. Bu çerçevede platformların: nefret söylemi, terör propagandası, dezenformasyon ve sahte hesaplarla mücadele etmesi; içerik kaldırma süreçlerini hızlı, şeffaf ve denetlenebilir şekilde yürütmesi; kullanıcı şikâyet mekanizmalarını işletmesi; yerel otoritelerle iş birliği yapması ve temsilci bulundurması zorunlu hâle gelmiştir[510]. Almanya'da içerik kaldırmayan platformlar ağır para cezası riski taşırken[511] Avustralya'da eSafety Komisyonu doğrudan müdahale yetkisine

[504] Tam adıyla İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007 yılında yürürlüğe girdi ve 2020 yılında kapsamlı değişikliğe uğradı.

[505] Ağ Yaptırım Yasası (NetzDG), kamuoyunda "Facebook Yasası" olarak bilinen düzenleme, 2018'de yürürlüğe girmiştir; bkz. https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf (14.12.2024).

[506] Çevrimiçi Güvenlik Yasası (Online Safety Act), 2021'de yürürlüğe girmiştir; bkz. https://www.legislation.gov.au/C2021A00076/latest/text (14.12.2024).

[507] Yardım ve Erişim Yasası (Assistance and Access Act), 2018'de yürürlüğe girmiştir; bkz. https://www.legislation.gov.au/C2018A00148/latest/text (14.12.2024).

[508] Loi Avia olarak da bilinen yasa, adını teklifi sunan milletvekili Laetitia Avia'dan alır ve 24 Haziran 2020 tarihinde yürürlüğe girmiştir.

[509] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021'de yürürlüğe girmiştir; bkz. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf (14.12.2024).

[510] Avustralya'da Yardım ve Erişim Yasası'nın başta m. 317G, 317L, 317T, 317E, 317ZF, 317C ve 317H olmak üzere 317B ile 317ZDA arasındaki maddeleri, telekomünikasyon şirketlerine, donanım üreticilerine, yazılım geliştiricilerine, internet servis sağlayıcılarına ve Whatsapp gibi şifreleme hizmeti sunan platformlara, suçla mücadelede güvenlik güçlerine teknik destek, içeriklere ve kullanıcı hesaplarına erişim sağlamak gibi yükümlülükler getirmiştir.

[511] Almanya'da NetzDG yasası, 24 saat içinde içerik kaldırmayan platformlara ağır para cezaları öngörür. Library of Congress, Global Legal Monitor, "Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech", https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/ (E.T.: 14.12.2024).

sahiptir[512]. Türkiye'de 5651 sayılı kanuna göre, kişilik hakları veya özel hayatın gizliliği ihlal edildiğinde, internet sağlayıcılarının oluşturduğu birlik içeriklerin engellenmesini hızlıca sağlar. Hindistan'da platformlar şikâyetlere 24 saat içinde yanıt vermek ve içeriği en geç 15 gün içinde değerlendirmek zorundadır[513]. Buna ek olarak, dijital hizmetlerin erişilebilirlik standardına sahip olması devlet yükümlülüğü hâline gelmiştir. AB Erişilebilirlik Direktifi[514] ve Kanada Erişilebilirlik Yasası[515] dezavantajlı grupların dijital hizmetlere eşit erişimini zorunlu kılarak dijital hakların sosyal bir boyut kazandığını göstermektedir.

2022 yılında AB'de yürürlüğe giren Dijital Hizmetler Yasası (Digital Services Act-DSA), dezenformasyonla mücadelede odağı tekil içerikten çok büyük çevrimiçi platformların algoritmik sistemlerine ve iş modellerine kaydırarak hesap verebilirliğe dayalı yeni bir yaklaşım benimsemektedir. Ancak bu durum öğretide; bilgi ve kaynak asimetrisi nedeniyle düzenleme tuzağı ve meşruiyet sorunları doğurması, kamu otoritelerinin bu sistemleri etkin biçimde denetleyememesi ve tek tip düzenleme anlayışı, bu mücadelenin platformların çıkarlarına bağımlı ve sınırlı bir yapıya dönüşmesi riskini barındırdığı gerekçesiyle eleştirilmiştir[516].

Ülkelerin başta sosyal medya olmak üzere platform ekosisteminin düzenlenmesine ilişkin bağlayıcı kanunlar kabul etmesi ve kapsamlı girişimler başlatması, platformlar açısından ABD yaklaşımını yansıtan self-regülasyon döneminin fiilen sona erdiğine işaret etmektedir. Bu gelişmeler, veri akışı ve platform ekosisteminin

---

[512] Avustralya'da Online Güvenlik Yasası'nın 4. Bölüm hükümlerine göre kullanıcılar şikâyetlerini eSafety Komisyonu'na iletebilir, Komisyon zararlı içeriklerin kaldırılmasını talep edip ceza verebilir.

[513] Hindistan'da da Bilgi Teknolojileri (Aracı Kurumlar) Kuralları'nın 3 vd. maddelerine göre, platformlar, kullanıcıların içerik raporlaması için mekanizmalar kurmak ve gelen şikâyetlere 24 saat içinde cevap vermek ve içeriği 24 saat ila 15 gün içinde inceleyip müdahale etmek zorundadır.

[514] AB Erişilebilirlik Direktifi, dezavantajlı kesimlerin dijital dünyada daha fazla yer almaları ve dijital hizmetlere erişimde eşit fırsatlara sahip olması için devletin dijital alanda erişilebilirlik standartlarını hukuki mekanizmalarla düzenlemesini teşvik etmektedir. 2019/882 numaralı Direktif Haziran 2025'te yürürlüğe girdi: Avrupa Birliği, Directive (EU) 2019/882, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0882 (14.12.2024).

[515] Kanada Erişilebilirlik Yasası'na göre, devletin tüm dijital hizmetlerinin dezavantajlı kesimlerce erişilebilir olması zorunludur. Kanada Erişilebilirlik Yasası: https://laws-lois.justice.gc.ca/eng/acts/a-0.6/FullText.html

[516] Sena. Kontoğlu Taştan, "Dijital Hizmetler Yasası'nda (DSA) Dezenformasyonla Mücadeleye Yönelik Davranış Kuralları." **Bilişim Hukuku Dergisi,** Cilt.7, Sayı.2, (2025), s.145-146.

giderek artan ölçüde ulusal hukuki mekanizmalar aracılığıyla düzenleneceğini ve platformların milli bazlı yasal rejimlerin doğrudan muhatabı hâline geleceğini göstermektedir[517].

Devletlerin dijital platformları düzenleme çabası yalnızca ulusal düzeyle sınırlı olmayıp, uluslararası iş birliği mekanizmaları üzerinden küresel bir hukuk ve standartlar rejimi oluşturmaya yönelmiştir. GDPR, DSA, Dijital Tek Pazar Stratejisi, AB-ABD Data Privacy Framework, BM İnsan Hakları Konseyi'nin 2018 İnternette İnsan Haklarının Kullanılması, Korunması ve Teşvik Edilmesi Kararı; engelli sağlık verilerini koruyan 2006 Engelli Hakları Sözleşmesi; yenilikçi teknolojileri öne çıkaran 2024 Dijital Hükümet Kılavuzu[518] 2023 UNESCO İnternet Evrensellik Göstergeleri[519] uluslararası dijital standartları belirleyen Uluslararası Telekomünikasyon Birliği'nin 1992 ve 2016 tarihli düzenlemeleri[520] 2014 İstanbul Sözleşmesi; 1964 Helsinki Deklarasyonu; 2016 Dünya Sağlık Örgütü Sağlık Verisi Yönetimi; ayrıca siber güvenlik, e-ticaret ve dijital hizmetlerde ortak politika içeren G20 Dijital Ekonomi 2021 Bildirgesi[521] ve diğer çok taraflı belgeler, dijital alanın sınır ötesi niteliği nedeniyle veri akışları ve platform ekosisteminin regülasyonu konusunda ortak norm üretiminin zorunluluğunu göstermektedir.

BM, OECD, WHO ve UNESCO gibi uluslararası örgütlerin belirlediği veri koruma, içerik güvenliği ve dijital hak standartları, ulusal düzenlemeleri uyumlaştırarak dijital ortamda insan haklarını, hukukun üstünlüğünü ve güvenli veri kullanımını güçlendirmeye yöneliktir[522]. GDPR, AB vatandaşlarının verilerini dünya çapında

---

[517] Çelik ve Aydoğan, *"Sosyal Medyada Hukuku Yerleşik Kılma Çabaları"*, s.319.

[518] United Nations Department of Economic and Social Affairs (UNDESA), UN E-Government Survey 2024, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024 (E.T.: 14.12.2024).

[519] UNESCO, UNESCO's internet universality indicators, https://unesdoc.unesco.org/ark:/48223/pf0000370288_eng (E.T.: 14.12.2024).

[520] United Nations Yearbook (UN), Global Telecommunications Connectivity, 1992, https://cdn.un.org/unyearbook/yun/chapter_pdf/1992YUN/1992_P7_CH12.pdf (E.T.: 14.12.2024); International Telecommunication Union (ITU), Digital Financial Services: Regulating for Financial Inclusion, 2016, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT02-2016-PDF-E.pdf (E.T.: 14.12.2024).

[521] G20 Dijital Ekonomi 2021 Bildirgesi, "The Declaration of G20 Digital Ministers", https://innovazione.gov.it/notizie/articoli/en/the-declaration-of-g20-digital-ministers/ (E.T.: 14.12.2024).

[522] Örneğin, OECD 1980 Kişisel Verilerin Korunması Prensipleri, dijital alanda ortak standartlar belirleyerek devletlerin hukuki düzenlemelerine rehberlik etmektedir. OECD'nin 2016 Dijital Ekonomi için Veri Koruma İlkeleri

koruyan bir dış etki yaratırken, DSA platformları yasa dışı içerikle mücadelede aktif sorumlu hâline getirir. DEPA, CPTPP, APEC Veri Çerçevesi gibi uluslararası anlaşmalar veri akışını kolaylaştırırken şirketler için öngörülebilir bir hukuki düzen yaratmayı amaçlar[523]. Aynı zamanda kadınlara, çocuklara ve hassas gruplara yönelik dijital şiddet ve istismar risklerine karşı platformlara özel yükümlülükler getirilmiştir; İstanbul Sözleşmesi[524] CEDAW[525] ve WHO[526] rehberleri bu koruma çerçevesini uluslararası ölçekte tanımlar.

---

ve 2021 Dijital Hükümet Yönetişimi El Kitabı, dijital içerikler konusunda ülkeler için uluslararası bir çerçeve sunmaktadır. OECD, The E-Leaders Handbook on the Governance of Digital Government, https://www.oecd.org/en/publications/the-e-leaders-handbook-on-the-governance-of-digital-government_ac7f2531-en.html (E.T.: 14.12.2024). BM İnsan Hakları Konseyi'nin 2018 Kararı, internetin bir araç olarak kullanılarak dijital ortamdaki içeriklere yönelik insan haklarını korunması ve geliştirilmesi çerçevesinde uluslararası standartlar belirlemeyi teşvik eder. United Nations Digital Library, [Belge Başlığı], https://digitallibrary.un.org/record/1639840/?v=pdf (E.T.: 14.12.2024).

[523] Asya-Pasifik Ekonomik İşbirliği (APEC) 2017 Veri Koruma Çerçevesi, bölgedeki dijital içerik standartlarını belirleyerek dijital ticareti desteklemektedir. Singapur, Yeni Zelanda ve Şili'nin imzaladığı 2021 Dijital Ekonomi Ortaklığı Anlaşması (DEPA), dijital ticaretin kolaylaştırılmasını ve dijital hizmetlerin düzenlenmesini amaçlamaktadır. Ministry of Trade and Industry (Singapore), Digital Economy Partnership Agreement (DEPA), https://www.mti.gov.sg/trade-international-economic-relations/agreements/digital-economy-agreements-dea/depa/ (E.T.: 14.12.2024). Ayrıca, 2018'de imzalanan Trans-Pasifik Ortaklığı Anlaşması (CPTPP), dijital içerik yönetiminin standardizasyonunu ve veri akışlarını teşvik ederek dijital hizmetler için engelleri kaldırmaktadır. Ministry of Foreign Affairs and Trade (New Zealand), Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Text and Resources, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources#bookmark0 (E.T.: 14.12.2024).

[524] 2014'te yürürlüğe giren İstanbul Sözleşmesi, devletlerin kadınları ve çocukları dijital ortamda korumak için gerekli hukuki düzenlemeleri yapmalarını zorunlu kılar. Council of Europe, Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210 (E.T.: 14.12.2024).

[525] BM Kadınlara Yönelik Ayrımcılığın Ortadan Kaldırılması Sözleşmesi (CEDAW) çerçevesinde 2021 tarihli BM Genel Kurulu Kadına Yönelik Şiddet Hakkında Kararı da dijital platformların kadınlara yönelik şiddetin önlenmesinde taşıdığı sorumluluğu vurgulamakta ve aile içi şiddet mağdurlarının verilerinin korunmasına yönelik hükümler içermektedir. United Nations Human Rights Council, Preventing and responding to all forms of violence against women and girls with disabilities: resolution, A/HRC/RES/47/15, 13 July 2021, United Nations Digital Library, https://digitallibrary.un.org/record/3936673?v=pdf (E.T.: 1 Şubat 2026).

[526] Sağlık alanında dijitalleşmenin artmasıyla birlikte, sağlık verilerinin etik ve güvenli kullanımı, denek haklarının korunması gibi konularda uluslararası ilke ve rehberler geliştirilmiştir. Örneğin, WHO'nun 2016 tarihli Health Data Governance ilkeleri, sağlık verilerinin güvenli yönetimi için temel çerçeveyi sunarken Dünya Tabipler Birliği'nin 1964 Helsinki Deklarasyonu, dijital sağlık uygulamalarında hasta haklarının ve verilerinin korunmasına yönelik etik standartları belirlemektedir. Bkz. Health Data Governance Initiative, Health Data Governance Principles, https://healthdataprinciples.org/images/English/[EN]%20Health%20Data%20Governance%20Principles.pdf (E.T.: 1 Şubat 2026); World Medical Association, WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, https://www.wma.net/policies-post/wma-declaration-of-helsinki (E.T.: 1 Şubat 2026).

Bu düzenlemeler, teknoloji şirketlerinin sınır ötesi veri işleme faaliyetlerini bağlayıcı kurallara tabi kılar; veri aktarımını güvenlik ve uyum şartlarına bağlar; platformların şeffaflık, hesap verebilirlik ve içerik yönetimi sorumlulukları açısından yol göstericidir. Sonuç olarak, devletler; uluslararası dijital düzenlemeler üzerinden veri koruması, içerik yönetimi, etik standartlar ve siber güvenlik gibi alanlarda devletler arası ortak norm üretimini güçlendirirken, platformlara küresel ölçekte sorumluluk yükleyen bir dijital yönetim mimarisi oluşturmuştur.

(2) Veri Akışından Para Akışına: Dijital Ekonominin ve Rekabetin Korunması Düzenlemeleri

Kripto varlıklar, dağıtık defter teknolojisine dayalı dijital ağlarda üretilen ve yatırım ya da bazı hâllerde ödeme aracı olarak kullanılan dijital değerlerdir. Kripto paralar, herhangi bir otoriteye bağlı olmayan ve değeri başka bir varlığa sabitlenmeyen dijital birimleri ifade ederken; kripto varlıklar, kripto paraların yanı sıra bir para birimine veya başka bir varlığın değerine sabitlenmiş stablecoin'leri de içermektedir[527].

Hukuki niteliği açısından kripto varlıklar, Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmeliğin m. 3'te tanımlanmıştır: "*kripto varlık, dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder*"[528]. Elektronik para ise, 6493 sayılı Kanun'un 3. maddesinin birinci fıkrasının (ç) bendine göre, *elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığında ihraç edilen, elektronik ortamda saklanan, Kanun'da tanımlanan ödeme işlemlerinin gerçekleştirilmesinde kullanılan ve ihraç eden kuruluş dışındaki*

[527] Ahmet Emrah Geçer, "Kripto Varlıkların Vergilendirilmesi Üzerine Düşünceler", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (553-572), İstanbul: Adalet, 2021, s.555.

[528] Türkiye Cumhuriyet Merkez Bankası, Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, 16 Nisan 2021 tarihli ve 31456 sayılı Resmî Gazete https://www.tcmb.gov.tr/wps/wcm/connect/6937855a-7c29-4d08-a26e-51ef3273c022/%C3%96demelerde%2BKripto%2BVarl%C4%B1klar%C4%B1n%2BKullan%C4%B1lmamas%C4%B1na%2BDair%2BY%C3%B6netmelik.pdf?MOD=AJPERES (1 Şubat 2026).

gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri ifade eder"[529].

Kripto paraların anonim yapısı yasa dışı faaliyetlerde kullanılma riskini artırmakta; yüksek fiyat oynaklığı ise ödeme aracı olarak kabulü ve hukuki niteliğinin belirlenmesini güçleştirmektedir. Ayrıca devlet veya merkez bankası tarafından ihraç edilmemeleri nedeniyle kripto paraların para politikası aracı olarak kullanılması mümkün değildir[530].

Devletler, dijitalleşmeyle birlikte finansal alan üzerindeki egemenliklerini yeniden kurmak için fintech ve dijital paraları stratejik bir araç olarak kullanmaktadır. Kripto varlıkların yaygınlaşması ve özel sektörün dijital ödeme altyapısını kontrol etmesi, devletlerin para politikası üzerindeki geleneksel hâkimiyetini zayıflatmış; bu nedenle birçok ülke hem kripto piyasasını düzenlemeye yönelmiş hem de Merkez Bankası Dijital Paraları (CBDC) geliştirmeye başlamıştır. Bu düzenlemeler yalnızca piyasa güvenliği için değil, aynı zamanda para arzı, sermaye hareketleri ve mali denetim üzerindeki kamusal otoritenin korunması amacıyla uygulanmaktadır. Çin örneğinde olduğu gibi bazı devletler, finansal teknolojileri yalnızca ekonomik bir araç değil, dijital çağda egemenlik inşasının ve ulusal kalkınma stratejilerinin bir bileşeni olarak görmektedir[531]. Bazı ülkeler, egemenlik anlayışını jeopolitik ve ekonomik koşullara göre esneterek ademimerkeziyetçi dijital varlıkları resmî para birimi olarak benimsemiştir. El Salvador[532] ve Orta Afrika Cumhuriyeti'nin[533] Bitcoin'i yasal ödeme aracı ilan etmesi,

---

[529] Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun (6493), RG 27.06.2013, Sayı 28690. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6493&MevzuatTur=1&MevzuatTertip=5 (E.T.: 1 Şubat 2026).

[530] Geçer, s.556-557.

[531] Fintek çözümlerinin yaygınlaştırılması, Çin'in küresel finansal sistemdeki merkezi kontrolünü güçlendirmesine ve dünyanın en büyük finansal teknoloji pazarına sahip olmasına imkân tanımıştır. Martin Chorzempa, "Fintech in China: Trading off Growth and Risk, Innovation, and Control", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (83-100), Maryland: Rowman & Littlefield Publishers., 2023, s.83.

[532] 2021'de El Salvador, Bitcoin'i resmi para birimi ilan eden ilk ülke olmuştur. "Bitcoin: El Salvador, kripto parayı resmi para birimi ilan eden ilk ülke oldu", *BBC News Türkçe*, 9 Haziran 2021, https://www.bbc.com/turkce/haberler-dunya-57415131 (E.T.: 1 Şubat 2026).

[533] 2022'de Orta Afrika Cumhuriyeti Bitcoin'i resmi para birimi olarak kabul eden ikinci ülke olmuştur. "Bitcoin, Orta Afrika Cumhuriyeti'nin resmi para birimi oldu", *BBC News Türkçe*, 28 Nisan 2022, https://www.bbc.com/turkce/haberler-dunya-

klasik parasal egemenlik anlayışının dönüşümüne işaret etse de bu tercih küresel düzeyde bir istisna olarak değerlendirilmektedir.

Kripto varlıklar ve fintech düzenlemeleri, egemenlik aracı hâline gelmiştir. Devletler, kripto paraların kayıt dışılığı artırması ve para politikası üzerinde kontrolü zayıflatması nedeniyle lisanslama, faaliyet kısıtlamaları ve yasaklama gibi mekanizmalarla kripto alanını denetlemektedir. Çin bu konuda en sert yaklaşımı benimseyerek kripto sektörünü tamamen yasaklayan ilk büyük ekonomi olmuştur.

Türkiye'de kripto varlıkların ödeme aracı olarak kullanılması, Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik ile yasaklanmıştır. Düzenleme; kripto varlıkların yüksek fiyat oynaklığı, anonimlikten kaynaklanan riskler, işlemlerin geri döndürülemezliği ve merkezî bir otorite tarafından denetlenememesi nedeniyle ödeme sistemlerinin güvenliği ve finansal istikrar açısından tehdit oluşturduğu gerekçesine dayanmaktadır. Bu kapsamda kripto varlıklar mal ve hizmet bedellerinin ödenmesinde kullanılamamakta ve ödeme kuruluşlarının bu varlıklara dayalı çözümler sunması engellenmektedir; buna karşılık kripto varlıkların yatırım aracı olarak alım-satımı yasak kapsamında değildir.

Merkez Bankası Dijital Paraları (CBDC), devletlerin dijital mali egemenliğini tahkim etmeye yönelik en stratejik araçlardan biri olarak öne çıkar. CBDC'ler dijital çağın yeni parasal egemenlik modeli olmuştur. CBDC'ler, aracısız bir ödeme sistemi yaratarak devletin para akışını, mali denetimi ve veri yönetimini doğrudan kontrol edebilmesini sağlar. Çin'in dijital yuanı (e-CNY) özel bankaları devreden çıkaran ilk örnek olup hem finansal gözetimi hem de ulusal kalkınma stratejisini güçlendiren bir egemenlik pratiği olarak değerlendirilir[534]. Benzer şekilde, Bahamalar'ın Sand Dollar projesi, Hindistan'ın kripto varlıklara karşı sıkı regülasyonları[535], ABD'nin dijital dolar

61252871#:~:text=Orta%20Afrika%20Cumhuriyeti%2C%20El%20Salvador,yoksul%20ülkeleri%20arasında%20yer%20alıyor (E.T.: 1 Şubat 2026).

[534] AFFRT, A New Digital Dawn: The Rise, Role and Relevance of the Digital Yuan, https://www.affrt.com/tr/a-new-digital-dawn-the-rise-role-and-relevance-of-the-digital-yuan.html (E.T.: 1 Şubat 2026).

[535] India's Cryptocurrency Legislation Framework in 2024, https://cryptocurrency.law/indias-cryptocurrency-legislation-framework-in-2024/ (E.T.: 1 Şubat 2026).

tartışmaları[536] ve Rusya'nın kripto paraların izlenmesi ve vergilendirilmesine ilişkin yasal adımları[537] da egemenliğin dijital çağın teknolojik parametrelerine uyarlanması süreci olarak okunmalıdır. CBDC modeli; para egemenliğini merkezîleştirir, sınır ötesi ödemeleri hızlandırır ve ucuzlatır, dolar/euro merkezli sistemlere alternatif oluşturur, Bankacılık sistemindeki rant zincirini kesintiye uğratır[538]. CBDC modeli, yalnızca teknolojik bir yenilik değil; devletlerin dijital aktör niteliğini güçlendiren, ekonomik bağımsızlığını, para üzerindeki denetimini ve küresel finansal güç dengelerini yeniden şekillendiren jeostratejik bir egemenlik aracıdır. Bu girişimler yalnızca kripto paraya alternatif oluşturmaz. Aynı zamanda vergi tahsilatı, sermaye hareketliliğinin denetimi ve kara para ile mücadele gibi kamu hukuku işlevlerinin dijital düzlemde sürdürülebilirliğini sağlamaktadır.

Kripto varlıkların düzenlenmesi ve vergilendirilmesi, dijital mali egemenliğin kurumsallaşması açısından temel bir araç hâline gelmiştir. Devletler, bu yeni ekonomik yapıyı kontrol altına almak amacıyla kripto varlıklara yönelik sıkı denetim ve entegrasyon politikaları geliştirmektedir. Söz konusu düzenlemeler yalnızca teknik-finansal altyapıyı değil, aynı zamanda devletin dijital alan üzerindeki egemenlik kapasitesini ve vatandaşla kurduğu ilişki biçimini yeniden tanımlamaktadır[539]. Brezilya Resolution 4,656[540] AB'nin 2026'da yürürlüğe girmesi beklenen Kripto Varlık Piyasaları Düzenlemesi (MiCA), Birleşik Krallık'ın aynı yıl uygulamaya koymayı planladığı kapsamlı yasal çerçeve ve

---

[536] Congressional Research Service, Cryptocurrency: Selected Policy Issues, CRS Report R47425, https://crsreports.congress.gov/product/pdf/R/R47425 (E.T.: 1 Şubat 2026).

[537] Russia Approves Cryptocurrency Framework: A New Era for Digital Assets Amid Sanctions and Tax Reform, https://university.heavnn.io/russia-approves-cryptocurrency-framework-a-new-era-for-digital-assets-amid-sanctions-and-tax-reform/ (E.T.: 1 Şubat 2026).

[538] Günlük dijital ödemeler, görünmez bir banka ve aracı zinciri üzerinden yürür; bu zincir süreci yavaşlatır, pahalılaştırır ve aracıların rant elde etmesine yol açar. Çin'in dijital yuanı ise bu aracı yapıyı devre dışı bırakmayı hedefleyerek mevcut ödeme düzenini kökten dönüştürme potansiyeline sahiptir. Varoufakis, *Technofeudalism: What Killed Capitalism,* s.145.

[539] CBDC (Merkez Bankası Dijital Parası): Devlet Destekli Dijital Para Birimi ile Finansal Sistemin Dönüşümü, Ninja News Akademi, Ender Ersoy, https://ninjanews.io/akademi/cbdc-merkez-bankasi-dijital-parasi/ (E.T.: 1 Şubat 2026). https://ninjanews.io/akademi/cbdc-merkez-bankasi-dijital-parasi/

[540] Brezilya'da çıkarılan Resolution 4,656 ile fintech şirketlerine ilişkin faaliyetlerin denetimi, hizmet kapsamı ve vergilendirmesi net çerçevelere bağlanmıştır. Banco Central do Brasil, Resolution CMN nº 4.656 of April 26, 2018, https://www.bcb.gov.br/content/financialstability/fintechs_docs/Resolution%204656.pdf (E.T.: 1 Şubat 2026).

Türkiye'nin 7518 sayılı yasası[541] devletlerin dijital mali alanı kontrol altına alma ve kamu gelirlerini güvenceye alma çabasının hukukî ifadeleridir. Bir görüşe göre, devletlerin kripto paraya yönelik düzenlemelerin, ağır ve piyasayı daraltıcı düzenlemeler yerine, anonimlik yapısına karşı kimlik tespiti ve ölçülülük esas alınmalıdır. Mevcut çerçevede kripto paraların menkul kıymet olarak nitelendirilmesi hâlinde değer artış veya ticari kazanç olarak vergilendirilmesi mümkündür[542].

Fintech ve CBDC düzenlemeleri, teknolojik bir yenilikten çok daha fazlasıdır: devletlerin parasal egemenliği dijital düzlemde yeniden kurma, ekonomik bağımsızlığı pekiştirme ve küresel finans mimarisinde güç kazanma stratejisidir. Bu süreç, dijital çağda egemenliğin yeni yüzünü ekonomik ve teknolojik araçlar üzerinden tanımlamaktadır. Fakat Fintech inovasyonu ile devlet egemenliği arasında gerilim vardır. Finansal teknolojiler rekabeti artırırken, devletin düzenleyici rolünü de zorlamaktadır[543]. Devletler piyasa dinamizmini baskılamadan egemenliğini koruma çabası içinde bir yandan dijital inovasyonu teşvik etmekte, diğer yandan veri erişimi, güvenlik ve mali istikrar adına piyasalara müdahale etmektedir[544].

---

[541] 2024 yılında kabul ettiği 7518 sayılı yasa ile kripto varlık hizmet sağlayıcılarını Sermaye Piyasası Kurulu'nun (SPK) denetimine tabi kılarak, dijital alanın kamusal denetimi doğrultusunda önemli bir adım atmıştır. Söz konusu yasa, faaliyet izni alınmadan sunulan hizmetleri cezai yaptırımlara bağlamış ve böylece devletin dijital mali alanda otorite kurma iradesini yasal zemine taşımıştır. Sermaye Piyasası Kurulu, Kripto Varlık Hizmet Sağlayıcılara İlişkin Duyuru, https://www.spk.gov.tr/duyurular/basin-duyurulari/2024/kripto-varlik-hizmet-saglayicilara-iliskin-duyuru_02072024 (E.T.: 1 Şubat 2026). Mevcut düzenlemeler dijital transferlerin vergilendirilmesini kapsamamaktadır; oysa yüksek tutarlı dijital işlemlerin kademeli vergilendirilmesi mümkündür. Böyle bir model, hem dijital alanda gelir eşitsizliğini sınırlayabilir hem de kayıt dışı yurtdışı servet transferlerini önleyerek devletin mali egemenliğini dijital düzeyde güçlendirebilir.

[542] Geçer, s.569-570.

[543] Finansal teknolojilerin hızlı ve denetimsiz gelişimi devletin ekonomik ve dijital egemenliğini zorlayabilmektedir. Bu nedenle devletler, finansal inovasyonu teşvik etmek için veri erişimini kolaylaştırırken, aynı zamanda şeffaflık, rekabet ve tüketici korumasını sağlayacak düzenleyici mekanizmalar geliştirmekte; sistemsel riskleri bu yolla sınırlandırmayı hedeflemektedir. Örneğin, Birleşik Krallık Financial Services Act, finansal hizmetler sektöründe şeffaflığa, tüketiciyi korumaya ve rekabeti sağlamaya yönelik şirketlere yükümlülükler getirmektedir: bkz. United Kingdom Parliament, Financial Services Act 2021, https://www.legislation.gov.uk/ukpga/2021/22 (E.T.: 1 Şubat 2026). AB Ödeme Hizmetleri Direktifi 2, dijital hizmetlerdeki yenilikleri destekleyip rekabeti teşvik etmeyi ve tüketicilerin korunmasını amaçlamaktadır. European Union, Directive (EU) 2015/2366 on payment services in the internal market (PSD2), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366 (E.T.: 1 Şubat 2026).

[544] Chorzempa, s.84.

Öte yandan e-ticaret platformları, yapay zekâ tabanlı algoritmalar kullanarak otomatik fiyatlama, pazar bölümlendirme ve arz yönetimi yapmaktadır. Bu dijital yöntemler, fizikî kartel anlaşmalarına gerek kalmadan fiyat sabitleme gibi rekabet bozucu pratiklerin dijital ortama taşınmasına imkân vermektedir. Dijital piyasalarda rekabet üstünlüğü; veri sahipliği, kullanıcı sayısı ve algoritmik kontrol gibi faktörlere dayanmakta; bu durum piyasa gücünün belirli aktörlerde yoğunlaşmasına neden olmaktadır.

Teknoloji devlerinin (örneğin Facebook'un Instagram ve WhatsApp'ı satın alması gibi) piyasa hakimiyetini pekiştiren stratejileri, devletleri dijital alanda rekabeti düzenleme ve güç yoğunlaşmasını engelleme yönünde harekete geçirmiştir. Devletler, bu kapsamda birleşme ve satın almaları denetlemekte, tekelleşmeye karşı cezai yaptırımlar uygulamakta ve küçük girişimlerin dışlanmasını önleyici politikalar geliştirmektedir. Bu yönelim, yalnızca klasik rekabet hukuku uygulamalarının değil, aynı zamanda dijital ekonomide egemenlik inşasının bir aracı olarak ortaya çıkan antitröst siyasetinin ifadesidir. Örneğin, ABD'deki Sherman Antitröst Yasası, dijital platformların rekabet dışı uygulamalarına da karşı aktif biçimde işletilmektedir[545]. Çin, 2008 tarihli Anti-Monopoly Yasası aracılığıyla, Alibaba ve Tencent gibi şirketlerin piyasadaki gücünü sınırlamaya yönelik müdahalelerde bulunmakta; veri kullanımı, fiyat politikaları ve inovasyon düzeylerini denetlemektedir[546]. Avrupa Komisyonu'nun Google'a 2017'de uyguladığı 2,42 milyar Euro'luk rekor ceza ve bu kararın 2024'te Avrupa Adalet Divanı tarafından onanması, AB'nin dijital piyasadaki hâkimiyet yapılarına karşı kamu gücünü yeniden tesis etme kararlılığını göstermektedir[547].

Avrupa Birliği'nin 2023'te yürürlüğe giren Dijital Pazar Yasası, büyük dijital platformların pazardaki ağırlığını sınırlamak, veri paylaşımını teşvik etmek ve kullanıcı

---

[545] United States Congress, Sherman Act, https://www.govinfo.gov/content/pkg/COMPS-3055/pdf/COMPS-3055.pdf (E.T.: 1 Şubat 2026).

[546] People's Republic of China, Anti-Monopoly Law, https://www.icao.int/sustainability/Compendium/Documents/China/download-antimonopoly-law-in-china-63824%20(3).pdf (E.T.: 1 Şubat 2026).

[547] Yusuf Özkan, "Avrupa Adalet Divanı, Google'a 2,4 milyar euroluk rekor cezayı onayladı", *BBC News Türkçe,* https://www.bbc.com/turkce/articles/c20rqkee2ldo (E.T.: 1 Şubat 2026).

haklarını güvence altına almak için önemli hükümler içermektedir[548]. Bu kapsamda Fransa Dijital İletişim Düzenleme Kurumu gibi ulusal düzenleyici kurumlar, dijital rekabeti izlemekte, piyasa dinamiklerini analiz etmekte ve teknoloji şirketlerinin hizmet kalitesi ile tüketici ilişkilerini gözeten politikalar üretmektedir. Dijital hizmetlerin güvenliğini ve kalitesini denetleyerek rekabetin kamusal çıkarlar doğrultusunda işlemesini sağlamaya çalışmaktadır.

Dijital anti tröst siyaseti, sadece piyasa düzenlemesi değil; aynı zamanda devletin dijital iktisadi egemenliğini koruma ve yeniden tesis etme stratejisidir. Bu bağlamda rekabet hukukunun dijital çağdaki dönüşümü, kamusal müdahale kapasitesinin sınırlarını ve araçlarını da yeniden tanımlamaktadır.

(3) Dijital Suç ve Siber Güvenlik Düzenlemeleri

Dijital tehditlerin ulus aşırı ve karmaşık hâle gelmesi, güvenlik alanlarının iç içe geçmesine yol açmaktadır. Bilişim suçları, siber tehditler ve millî güvenlik arasındaki sınırlar bulanıklaşmış; bu alanlarda görev yapan kurumlar giderek daha bütünleşik çalışır hâle gelmiştir. Devletler dijital tehditlere karşı daha yoğun koordinasyon kurmakta, güvenlik ve istihbarat faaliyetleri ise bireylerin çevrimiçi davranışlarının izlenmesine dayalı bir modele kaymaktadır[549].

Siber egemenlik yaklaşımı, devletin çevrimiçi alan üzerindeki denetimini meşrulaştıran ve dijital düzenin devlet eliyle korunmasını savunan bir perspektiftir[550]. Yapay zekâ, büyük veri, blok zincir, kuantum teknolojileri ve bulut bilişim gibi alanlarda artan tehditler nedeniyle kritik altyapıların ve kamu kurumlarının dijital varlıklarının korunması, devletler için stratejik bir zorunluluk hâline gelmiştir[551].

---

[548] European Union, Commission Delegated Regulation (EU) 2022/265, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC (E.T.: 1 Şubat 2026).

[549] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.6.

[550] Séverine Arsène, "Global Internet Governance in Chinese Academic Literature", [Electronic Version], *China Perspectives* 2017, Vol.2, http://journals.openedition.org/chinaperspectives/6973 (1 Şubat 2026), s.35.

[551] Siber Güvenlik Kanunu Gerekçesi, Genel Gerekçe, s.13.

Siber zorbalık, kasıtlı ve sürekli rahatsız edici davranışların dijital ortamda, özellikle sosyal ağlar üzerinden sürdürülmesidir. İnternetin anonimliği ve içeriklerin kalıcılığı bu fiillerin etkisini artırmakta; çocuklar ve gençler başta olmak üzere mağdurlar ağır biçimde etkilenmekte ve eylemler ceza hukukunda çeşitli suç tipleriyle (hakaret, tehdit, şantaj, özel hayatın gizliliğinin ihlali, kişisel verilerin kaydı vb.) ilişkilendirilmektedir[552].

Dijital çağda devletler, artan siber suçlar karşısında kamu düzeni ve dijital egemenliği korumak için ceza hukuku ile siber güvenlik politikalarını bütüncül biçimde ele almaktadır. Güvenliğin yalnızca teknik önlemlerle değil, güçlü ve etkin uygulanan bir hukuki altyapıyla sağlanabileceği vurgulanmakta[553] kurumların hukuki uyum, olay müdahalesi ve sorumlulukları kapsayan proaktif stratejiler geliştirmesi gerekmektedir[554]. Siber güvenlik; teknik, hukuki, kurumsal ve insan kaynağı unsurlarının uyumlu çalıştığı bir ekosistem olarak görülmekte[555] siber zorbalık, kişisel verilerin ihlali ve çevrim içi tehditler hem bireysel hakları hem de kamusal düzeni tehdit eden olgular olarak değerlendirilmektedir. Bu nedenle devletler, soruşturma, dijital delil toplama ve içeriklere erişim-kaldırma mekanizmalarını güçlendiren düzenlemelere yönelmektedir. Örneğin, Kanada'da 2014 yılında kabul edilen Protecting Canadians from Online Crime Act ile Ceza Kanunu'na eklenen m. 162.1 hükmüyle rızaya dayanmayan mahrem görüntülerin paylaşılması suç olarak düzenlenmiş; m. 164.1 ve m. 487 vd. hükümleriyle dijital delillere

---

[552] Kerim Çakır, "Sosyal Ağlarda Siber Zorbalık ve Ceza Hukuku", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (235-250), İstanbul: Adalet, 2021, s.235-236.

[553] Ergül, Ergin, **Siber Güvenlik Hukuku Temel Mevzuatı,** Ankara: Adalet Yayınları, 2025, s.29.

[554] Bu konuda şu düzenlemeler örnek verilebilir: ABD'de 1998'de yürürlüğe giren Çocukların Çevrimiçi Gizliliğinin Korunması Yasası (COPPA), United States Congress, Children's Online Privacy Protection Act (COPPA), 1998, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 (E.T.: 1 Şubat 2026); 2018'de yürürlüğe giren Bulut Yasası, United States Congress, Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (E.T.: 1 Şubat 2026); Bağlantı Güvenliği ve Bilgi Sistemleri Direktifi (NIS Directive), European Union, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union 2016, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf (E.T.: 1 Şubat 2026); ve Avustralya'da 2021 yılında yürürlüğe giren Çevrimiçi Güvenlik Yasası Commonwealth of Australia, Online Safety Act 2021, https://www.legislation.gov.au/Details/C2021A00076 (E.T.: 1 Şubat 2026).

[555] Ela Erturan, "Veri Sorumlusunun Siber Tehditleri ve İnternet Dolandırıcılığını Önlemek Amacıyla 'Başkalarının' Kişisel Verilerini İşlemesinin 'Meşru Menfaat' Kapsamında Değerlendirilmesi Meselesi", **Prof. Dr. Sabih Arkan'a Armağan,** İstanbul: On İki Levha Yayıncılık, 2019, s.425.

erişim ve içeriklerin kaldırılmasına ilişkin usuller güçlendirilmiştir[556]. Bu tür düzenlemeler, siber suçlarla mücadelede ceza hukuku araçlarının siber güvenlik stratejileriyle birlikte işletilmesinin, dijital kamusal alanın korunması açısından zorunlu hâle geldiğini ortaya koymaktadır.

Yine bu kapsamda dijital platformlara içerik kontrolü, veri güvenliği, kullanıcı haklarının korunması ve adli soruşturmalara destek gibi geniş bir yelpazede yükümlülükler getirilmektedir. Örneğin Türkiye'de 5651 sayılı Kanun; içerik, yer ve erişim sağlayıcılarının sorumluluklarını ve hukuka aykırı içeriklerin kaldırılmasına ilişkin düzenlemeleri belirlemiştir[557]. Uluslararası diğer örnekler, deepfake gibi dijital suçların tanımlanmasından içerik düzenlemelerine kadar geniş bir yelpazededir. 2021'de Avrupa Parlamentosu'na sunulan bir çalışmada, deepfake'in teknoloji, üretim, yayılma, hedef ve izleyici boyutları incelenmiş ve hukuki düzenleme önerileri sunulmuştur[558]. Avustralya Yardım ve Erişim Yasası[559] ile Birleşik Krallık Soruşturma Yetkileri Yasası[560] platformlara teknik yardım, veri takibi, iletişim kayıtlarına erişim ve dijital delil saklama gibi yükümlülükler yüklemektedir. Kritik altyapı güvenliği yasaları ise siber olay bildiriminden sektörel raporlamaya kadar ek sorumluluklar öngörmektedir[561]. Bu

---

[556] Canada, Protecting Canadians from Online Crime Act, S.C. 2014, c. 31, https://laws-lois.justice.gc.ca/PDF/2014_31.pdf (E.T.: 1 Şubat 2026).

[557] 5651 sayılı İnternet Kanunu, m. 3'te içerik sağlayıcıların bilgilendirme yükümlülüğünü, m. 4-6'de, içerik, yer ve erişim sağlayıcıların sorumluluklarını, m. 6/A'da, Erişim Sağlayıcıları Birliği'nin kurulmasını ve m. 8'de, hukuka aykırı içeriklerin kaldırılması ve erişimin engellenmesini düzenlenmektedir.

[558] European Parliamentary Research Service, Tackling deepfakes in European policy, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf (1 Şubat 2026), s.1.

[559] Avustralya Yardım ve Erişim Yasası dijital platformlara, siber suçların soruşturulması amacıyla m. 317G-317L arasında teknik yardım sağlama, veri takibi yapma ve cihazlara erişim gibi yükümlülükler; m. 317ZH'de kullanıcı verilerine erişim sağlama zorunluluğu getirmektedir.

[560] Birleşik Krallık Soruşturma Yetkileri Yasası (Investigatory Powers Act), m. 61, 62 ve 88'de dijital platformlara; güvenlik güçleriyle iş birliği içinde internet trafiğini izleme, iletişim kayıtlarına erişme, dijital cihazlarda veri arama yapma ve delil niteliğindeki verileri saklama gibi yükümlülükler yüklemektedir. United Kingdom Parliament, Investigatory Powers Act 2016 (c. 25), https://www.legislation.gov.uk/ukpga/2016/25/contents (E.T.: 1 Şubat 2026).

[561] Avustralya Kritik Altyapı Güvenliği Yasası, sektörel düzeyde siber güvenlik yükümlülükleri getirmekte; siber olayların bildirilmesi (Bölüm 2B), raporlama (Bölüm 2AA) ve ek yükümlülükler (Bölüm 2C) gibi hükümler içermektedir. Avustralya'da 2018'de yürürlüğe giren Kritik Altyapı Güvenliği Yasası, Commonwealth of Australia, Social Services Act 2018 (Cth), https://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/socia2018398/ (E.T.: 1 Şubat 2026).

yaklaşım, dijital platformların yalnızca ticari aktörler değil, kamusal sorumluluk taşıyan düzenlenebilir yapılar olarak konumlandırılmasını sağlamaktadır.

Çocuklar, dijital ortamda artan istismar, cinsel sömürü ve manipülasyon riskleriyle karşı karşıyadır. Bu durum, çevrimiçi suçlara karşı devletin ve ailelerin koruma ve önleme yükümlülüğünü daha da güçlendirmektedir[562]. Bu nedenle birçok ülke, platformları çocukların çevrimiçi güvenliğini sağlamakla yükümlendiren özel düzenlemeler geliştirmiştir. ABD'de Çocukların Çevrimiçi Gizliliğini Koruma Yasası (COPPA) çocuklara yönelik çevrimiçi hizmetlerde ebeveyn onayını zorunlu kılarken[563] Birleşik Krallık Dijital Ekonomi Yasası, yasa dışı içerik ve istismar materyallerine karşı filtreleme ve engelleme yükümlülükleri getirmektedir[564]. Avustralya Çevrimiçi Güvenlik Yasası ise platformları çocuk istismarına ilişkin içerikleri kaldırmakla sorumlu tutmaktadır[565]. Bu çabalar, devletlerin dijital alanda çocuk koruma politikasını güçlendirme iradesinin yasal karşılıklarıdır.

Fransa Danıştayı (*Conseil d'État*) bir başvuruda, devletlerin çocukları koruma ve kamu düzenini sağlama yükümlülüğü kapsamında dijital platformlar için sınırlayıcı tedbirler alabileceğini ortaya koymaktadır[566]. Bu tür müdahaleler, salt ekonomik

---

[562] Ebru Yavuz Yayla, "Anayasa'nın 41/4. maddesi Kapsamında Çocukların Dijital Ortamda Cinsel İstismara Karşı Korunması", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.35.

[563] Çocukların Çevrimiçi Gizliliğini Koruma Yasası (COPPA) m. 312.5, çocuklara yönelik çevrimiçi hizmet sağlayıcıların ebeveyn onayı almalarını zorunlu kılmıştır. United States Code of Federal Regulations, 16 C.F.R. (Children's Online Privacy Protection Rule), https://www.ecfr.gov/current/title-16/section-312.5 (E.T.: 1 Şubat 2026).

[564] Birleşik Krallık'ta 2017 tarihli Dijital Ekonomi Yasası'nın 3. ve 6. bölümünün 104. paragrafı, platformlara ve internet servis sağlayıcılarına, yasa dışı içeriklerin ve çocuk istismarı materyallerinin yayılmasını önlemeye yönelik içerik filtreleme gibi sorumluluklar yüklenmiştir. United Kingdom Parliament, Data Protection Act 2018 (c. 30), https://www.legislation.gov.uk/ukpga/2017/30/contents (E.T.: 1 Şubat 2026).

[565] Avustralya'nın 2021 tarihli Çevrimiçi Güvenlik Yasası m. 6 ve 12, platformlara çevrimiçi istismar içeriklerini kaldırma yükümlülüğü getirmiştir. Commonwealth of Australia, Online Safety Act 2021, https://www.legislation.gov.au/C2021A00076/latest/text (E.T.: 1 Şubat 2026).

[566] Fransa Danıştayı (Conseil d'État), Webgroup Czech Republic ve NKL Associates s.r.o. tarafından açılan davalar (dosya numaraları 461193 ve 461195) kapsamında 7 Mart 2024 tarihinde Avrupa Birliği Adalet Divanı'na (CJUE) önceki yorum için sorular (prejudicial questions) yöneltmiştir. Bu nedenle Danıştay'ın kendi kararında esaslı bir nihai hüküm vermektense süreci ABAD'a havale ettiği görülmektedir. ABAD'da bu dosya C-188/24 numarasıyla kayıtlı olup, Danıştay'ın ilettiği soruların yanıtlanması beklenmektedir. Bu, Fransa'daki ulusal uyuşmazlığın AB hukukuna uygunluk açısından yorumlanması içindir. Conseil d'État (France), Questions préjudicielles à la Cour de justice de l'Union européenne (CJUE), https://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/socia2018398/ (E.T.: 1 Şubat 2026).

düzenleme değil; ceza hukuku temelli ve tüm yayıncıları bağlayan genel koruma normlarının dijital alana uygulanması olarak değerlendirilmiştir. Fransa Danıştayı, Avrupa Birliği Adalet Divanı'nın da çocukların korunmasının ekonomik serbestiler karşısında öncelik taşıyabileceğini, müdahalelerin meşru amaç, orantılılık ve ölçülülük şartlarını sağlaması hâlinde Birlik hukukuna aykırı olmayacağını kabul ettiğini ifade etmiştir[567].

Devletler, dijitalleşmenin yarattığı ulusal güvenlik riskleri karşısında siber güvenliği kurumsal bir kapasiteye dönüştürmeye yönelmektedir. ABD'de 2018'de kurulan Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) federal iş birliğini güçlendirerek kritik altyapılar için standartlar geliştirmekte ve ulusal siber güvenlik koordinasyonunu sağlamaktadır[568]. Türkiye ise 2025'te yayımlanan Cumhurbaşkanı Kararnamesi ile Siber Güvenlik Başkanlığı'nı kurmuş ve kısa süre sonra Siber Güvenlik Kanunu Teklifi'ni hazırlayarak siber güvenliği milli güvenliğin ayrılmaz bir parçası olarak tanımlamıştır. Kanun gerekçesinde, dijitalleşmenin hızlanmasıyla birlikte siber güvenliğin stratejik bir öncelik haline geldiği ve bu alanın Milli Teknoloji Hamlesi kapsamında teknolojik gelişimin temel unsurlarından biri olarak görüldüğü belirtilmektedir[569]. Siber Güvenlik Başkanlığı, strateji geliştirme, kritik altyapıların korunması, denetim ve yaptırım görevleriyle siber güvenliği kurumsallaştırmakta; yerli-milli teknolojileri teşvik ederek kamu ve özel sektöre ortak sorumluluklar yüklemektedir. Düzenleme, siber güvenliğin temel haklara saygı, hesap verebilirlik ve sürdürülebilirlik ilkeleriyle yürütülmesini, nitelikli insan kaynağı ve toplumsal siber güvenlik kültürünün

---

[567] Conseil d'État (France), Décision n° 453763, 5ème-6ème chambres réunies, 6 mars 2024 (Coyote System), https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-03-06/453763 (E.T.: 1 Şubat 2026). Fransa, çocukların korunması ve kamu düzeni gerekçesiyle bazı dijital platformlara müdahale etmiş; şirketlerin E-Ticaret Direktifi'ndeki "köken ülke ilkesi"ne dayalı itirazları belirleyici olmamıştır. Çünkü söz konusu düzenlemeler, ticari faaliyetlerin sınırlandırılmasından ziyade, çocuklara müstehcen içerik sunulmasını yasaklayan cezai normların dijital alana uygulanmasına dayanmaktadır.

[568] CISA Yasası, United States Congress, Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. 115-278, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf (E.T.: 1 Şubat 2026).

[569] Siber Güvenlik Kanunu Gerekçesi, Genel Gerekçe, s. 13.

geliştirilmesini hedeflemekte; böylece dijital çağda devletin egemenlik kapasitesini güçlendirmektedir[570].

Siber Güvenlik Kanunu, kapsamının genişliği nedeniyle yalnızca "Orwellian" bir yaklaşımı çağrıştırmakla kalmayıp istihbari faaliyetleri denetim dışında bırakması ve muğlak kavramlara dayanarak yürütmeye geniş yetkiler tanıması nedeniyle ciddi hak ve özgürlük sorunları doğurma potansiyeli taşımaktadır. Kanun'un 2. maddesi, kamu kurumlarından özel sektöre kadar geniş bir muhatap kitlesi öngörürken; PVSK, Sahil Güvenlik Komutanlığı Kanunu, Jandarma Kanunu ve MİT Kanunu kapsamındaki faaliyetleri açıkça istisna tutmakta, böylece dijital ortamda istihbarat birimlerinin hukuki denetimden bağımsız hareket edebileceği bir alan yaratmaktadır. Bu durum, özel hayatın gizliliği, kişisel verilerin korunması ve ifade özgürlüğü üzerindeki anayasal güvenceleri zayıflatır; oto-sansür ve ifade özgürlüğünün fiilen baskılanması riskini artırır.

Kanunun 4. maddesinde hesap verebilirlik, hukukun üstünlüğü ve temel haklara saygı ilkelerini benimsediğini belirtmesine rağmen istihbarat faaliyetlerini kapsam dışı bırakması, normatif bir çelişki yaratmaktadır. Zira istihbari faaliyetlerin bu temel değerlere uygun yürütüldüğü iddia ediliyorsa, bu faaliyetlerin kanun denetimi dışında tutulmasının gerekçesi sorgulanmalıdır. Kanunun 6(2). maddesinde kişisel verilerin işlenmesine dair açık güvenceler yer alsa da istihbarat faaliyetlerinin bu hükümler dışında tutulması, bu kurumların söz konusu güvenceleri sağlayamadığı veya sağlamak istemediği izlenimini doğurmaktadır. Kişisel verilerin korunmasına ilişkin güvenceler bu istisna nedeniyle işlevsiz hâle gelmekte; bu durum Anayasa'nın 20. maddesi çerçevesinde hakların özüne müdahale niteliği taşımaktadır. Kanunun, sahte veri sızıntısı algısı oluşturmayı suç sayan 16(5). maddesi hükmü ise özellikle gazetecilik faaliyetleri bakımından caydırıcı bir etki yaratabileceği için ifade ve basın özgürlüğü yönünden tartışmalıdır[571]. Bunun yanında m. 6'da Siber Güvenlik Başkanlığı'na yargı kararı

[570] Siber Güvenlik Kanunu Teklifi m. 4 Türkiye Cumhuriyeti Resmî Gazete, 19 Mart 2025 tarihli ve 32846 sayılı Siber Güvenlik Kanunu yayımlanma sayfası, https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm (E.T.: 1 Şubat 2026);Siber Güvenlik Kanunu Gerekçesi, Genel Gerekçe, s. 14. Türkiye Büyük Millet Meclisi, https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf (E.T.: 1 Şubat 2026).

[571] "Siber Güvenlik Kanunu Teklifi Meclis'te kabul edildi", *Diken*, 15 Ocak 2025, https://www.diken.com.tr/siber-guvenlik-kanunu-teklifi-mecliste-kabul-edildi/. (E.T.: 1 Şubat 2026). Çin'de de sosyal medyadaki bilgi yayılımını

olmadan her türlü bilgi, belge ve log kaydına erişim yetkisi tanınması ise kişisel mahremiyet açısından ciddi bir müdahale riski doğurur ve hukuk devleti güvenceleriyle bağdaşmaz[572]. Genel olarak kanunun hem anayasal hak ve özgürlükler hem de hukuk devleti ilkesi açısından ciddi eksiklikler içerdiği ve ulusal siber güvenliğin sağlanması çabası açısından Türkiye'nin ABD ve AB'nin yaklaşımını değil devleti merkeze alarak güçlendiren Çin'in yaklaşımını benimsediği söylenebilir.

Çin'in siber güvenlik mimarisi, 1990'larda atılan hukuki temeller üzerine son on yılda hızla merkezîleşen ve devlet kontrolünü güçlendiren kapsamlı bir yapıya dönüşmüştür[573]. Xi Jinping döneminde kurulan üst düzey koordinasyon organları ve Çin Siber Uzay İdaresi (CAC), siber güvenliği teknik bir mesele olmaktan çıkarıp siyasi, ideolojik, ekonomik ve toplumsal boyutlarıyla birlikte ele alan bütüncül bir devlet projesine dönüştürmüştür[574]. Siber güvenlik artık yalnızca teknik bir mesele değil; hukuki, siyasi ve egemenlik boyutları olan çok katmanlı bir ulusal güvenlik unsurudur. Çin örneği, devletin dijital toplum, ekonomi ve yönetim yapısını korumak amacıyla siber güvenliği merkezî bir öncelik olarak ele aldığını ve güvenlik odaklı yönetim anlayışını dijital alana genişlettiğini göstermektedir. Bu doğrultuda yetkili kurumlar, kapsamlı tanımlar ve yeni düzenleyici mekanizmalarla siber güvenlik mimarisini yeniden

---

kontrol altına almak için yanlış bilgileri yaymak 500 retweet veya 5000 görüntülenme suç sayılmaktadır. Rogier Creemers, "The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy", **Journal of Contemporary China,** Vol.33, No.146, 2024, s.182.

572 "İFÖD'den 'Siber Güvenlik Kanunu' uyarısı: Tehlikenin farkında mısınız?", *Diken*, 16 Ocak 2025, https://www.diken.com.tr/ifodden-siber-guvenlik-kanunu-uyarisi-tehlikenin-farkinda-misiniz/ (E.T.: 1 Şubat 2026).

573 2010'da Google'ın ülkeden çekilmesi ve ABD'nin "Açık İnternet Gündemi", Çin tarafından rejim karşıtı bir meydan okuma olarak görülmüş; bunun sonucunda yayımlanan Beyaz Kitap'ta internetin ulusal sınırlarla belirlenen bir egemenlik alanı olduğu vurgulanmıştır. Creemers, *"The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy",* s.181; Çin'in siber güvenlik hukuku 1997'den itibaren şekillenmiş; bilgisayar suçları yasaklanmış, Büyük Güvenlik Duvarı kurulmuş ve 2000'de hizmet sağlayıcılara kullanıcı kaydı zorunluluğu getirilmiştir. Sistem; Devlet Konseyi, CAC, ilgili bakanlıklar ve sanayi standartlarına dayanmakta; teknik altyapının güçlendirilmesi, uzman insan kaynağı yetiştirilmesi ve toplumsal farkındalığın artırılması hedeflenmektedir. Rogier Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State", **China Law and Society Review,** Vol.6, (2023), s.111-115.

574 2014'te kurulan Siber Güvenlik ve Enformasyonlaştırma Merkez Liderlik Grubu ile dijitalleşme kalkınmanın stratejik aracı hâline getirilmiş; çevrimiçi içerik denetiminde merkezi otorite olarak CAC oluşturulmuştur. Aynı yıl yayımlanan Ulusal Siber Uzay Güvenliği Stratejisi, siber güvenliği teknik bir mesele olmaktan çıkarıp rejim istikrarı, toplumsal düzen ve dijital kalkınmayı önceleyen çok boyutlu bir ulusal güvenlik konusu olarak tanımlamıştır. Creemers, *"Cybersecurity Law and Regulation in China: Securing the Smart State",* s.117; Creemers, *"The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy",* s.174.

şekillendirmektedir[575]. 2016 Siber Güvenlik Yasası (CSL) dağınık düzenlemeleri tek çatı altında toplayarak bütüncül bir siber güvenlik sistemi kurmayı amaçlamış; kritik bilgi altyapısı kavramını hukuka sokmuş, içerik denetimini ve kimlik doğrulama zorunluluğunu kurumsallaştırmış; Büyük Güvenlik Duvarı'nın hukuki temelini tanımlamış ve CAC'ye yurtdışından gelen içeriklere müdahale yetkisi vermiştir[576].

2021 Veri Güvenliği Yasası (DSL) ise verileri; normal, önemli ve çekirdek olarak sınıflandırarak her düzey için farklı güvenlik yükümlülükleri öngörür; risk değerlendirmesi, raporlama, izleme ve acil müdahale gibi mekanizmaları zorunlu kılar. Ayrıca önemli verilerin ihracını sıkı denetime tabi tutar ve yabancı kurumlara veri aktarımına ciddi kısıtlamalar getirir. Yasa, veriyi ulusal bir stratejik kaynak olarak yeniden tanımlayarak güvenlik odaklı, hiyerarşik bir veri yönetimi sistemi kurmuştur. Bu süreçte önceden sıkça kullanılan bilgi güvenliği teriminden siber güvenlik kavramına geçiş yaşanmıştır. Çin'in yaklaşımı yalnızca iç tehditlere odaklanmamakta; siber suçlar, terörle mücadele ve uluslararası dijital yönetişimde daha etkili bir konum edinme hedefini de içermektedir[577]. Bu model, içerik üzerindeki sıkı kontrolü, kullanıcı kimlik doğrulaması ve platformlara geniş sorumluluk yüklenmesi gibi mekanizmalarla dijital alanın tüm aşamalarında devlet denetimini pekiştirmektedir. Çin'in, donanım lisanslamadan kullanıcı kimlik doğrulamaya, içerik kontrolünden hizmet denetimine kadar tüm dijital süreçlerde devletin kapsamlı denetimini hedeflerken sorumluluğu dijital platformlara yüklemesi dikkat çekicidir[578]. Çin'in siyasi ve ideolojik odaklı bu yaklaşımı, Çinli teknoloji firmalarının bazı Batı ülkelerinde güvenlik gerekçesiyle engellenmesinin arkasındaki nedenlerden biridir[579]. Ancak, Creemers'a göre, Batı'daki güvenlik tanımlarının da nesnel değil, siyasi ve toplumsal bağlamlara göre şekillenen öznel değerlendirmelerdir çünkü herhangi bir siber güvenlik tanımı doğası gereği politik bir söylemin ürünüdür[580].

---

[575] Creemers, *"Cybersecurity Law and Regulation in China: Securing the Smart State",* s.111.
[576] Creemers, *"The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy",* s.174.
[577] Creemers, *"Cybersecurity Law and Regulation in China: Securing the Smart State",* s.118-123.
[578] Creemers, *"Cybersecurity Law and Regulation in China: Securing the Smart State",* s.132.
[579] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.130.
[580] Creemers, *"Cybersecurity Law and Regulation in China: Securing the Smart State",* s.113.

Siber suçların sınır aşan niteliği, tek tek ulusal düzenlemelerle çözülemeyecek ölçüde karmaşık bir yapı oluşturduğundan, devletlerin ortak stratejiler geliştirmesini ve belirsizlikleri gideren uluslararası bir hukuki çerçeve kurulmasını zorunlu kılar. Bu amaçla hazırlanan uluslararası sözleşmeler, dijital suçların tanımlanması, önlenmesi, soruşturulması ve faillerin takibi için iş birliği ve bilgi paylaşımını kurumsallaştırır. Avrupa Konseyi'nin 2004 tarihli Budapeşte Sözleşmesi[581] bu alandaki ilk kapsamlı çok taraflı metindir. Sözleşme'nin 15. maddesi, siber suçlara ilişkin ulusal düzenlemelerin, uluslararası insan hakları belgeleriyle güvence altına alınan hakları ihlal etmeyecek şekilde yapılmasını zorunlu kılmaktadır.

AB'nin 2016 tarihli NIS Direktifi ve 2019'da yürürlüğe giren AB Siber Güvenlik Yasası ise olay bildirimi ve kurumsal kapasiteyi güçlendiren düzenlemelerdir[582]. ABD'nin 2018 tarihli CLOUD Act'i ve AB'nin E-Evidence Yönetmeliği (Regulation (EU) 2023/1543) hizmet sağlayıcılardan sınır ötesi elektronik delil talep edilmesini kolaylaştıran mekanizmalar öngörür[583]. İkisi de veriler sınırları içinde olsun ya da olmasın, hizmet sağlayıcılardan elektronik delil talep etme imkânı sağlamaktadır. Bununla birlikte ABD'nin, kendi şirketlerinin yabancı ülkelere doğrudan veri vermesini yasaklayan yaklaşımı ile ABD makamlarının AB vatandaşlarına ait verilere erişim talepleri, GDPR ile çelişmekte ve sınır ötesi veri paylaşımı konusunda önemli hukuki uyuşmazlıklara yol açmaktadır[584]. Bu nedenle uluslararası siber suçlarla mücadelede iş birliği zorunlu olmakla birlikte, veri koruma rejimleri arasındaki uyumsuzluklar hâlen temel bir gerilim alanı oluşturmaktadır.

---

[581] Resmî adı Siber Suçlar Sözleşmesi (Convention on Cybercrime) olup 2001'de Budapeşte'de kabul edilmiştir. Avrupa Konseyi, Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), 23 Kasım 2001, ETS No. 185, https://rm.coe.int/1680081561 (E.T.: 01.02.2026). Budapeşte Sözleşmesi, Avrupa ülkeleriyle birlikte ABD, Kanada ve Japonya tarafından da onaylanmıştır.

[582] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on ICT cybersecurity certification (Cybersecurity Act), Official Journal of the European Union L 151/15, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (E.T.: 01.02.2026).

[583] ABD'nin 2018 tarihli CLOUD Act'i, ikili anlaşmalar yoluyla devletlerin dijital verilere erişimini kolaylaştırmayı amaçlar. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), United States Department of Justice PDF, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (E.T.: 01.02.2026).

[584] Christakis, s.32.

Siber suçlarla mücadelede uluslararası kurumsal yapıların güçlendirilmesi, sınır aşan tehditlere karşı etkili bir yanıt oluşturmanın temel unsurudur. 2013'te kurulan Europol Siber Suç Merkezi[585] Interpol'ün küresel operasyonları, NATO'nun 2016'daki Siber Savunma Taahhüdü[586] ve BM'nin 2019'da kurduğu Siber Güvenlik ve Bilgi Güvenliği için Açık Uçlu Çalışma Grubu[587] gibi oluşumlar, devletlerin teknik kapasiteyi artırma, veri paylaşımı ve koordineli müdahaleyi kurumsallaştırma çabalarının örnekleridir. AB'nin 2020 Siber Güvenlik Stratejisi de bu doğrultuda ortak savunma kapasitesini güçlendirmeyi hedeflemiştir[588]. BM Güvenlik Konseyi'nin 2021 çağrısı ise dijital alanın ortak standartlarla düzenlenmesi ve devletler arası iş birliğinin artırılması gereğini vurgulamıştır[589]. Bu gelişmeler, siber tehditlere karşı uluslararası düzeyde bütüncül ve dayanıklı bir güvenlik mimarisi oluşturma yönünde atılan adımlardır.

Ceza hukuku, sosyal politikalarla tamamlayıcı bir ilişki içindedir ve son çare (ultima ratio) olarak uygulanmalıdır. Suçla mücadelede asıl hedef, cezalandırmadan önce önleme olmalı; sosyal politika güçlendikçe suç azalmalıdır[590]. Bu yaklaşım dijital toplum için de geçerlidir: siber zorbalık, nefret söylemi ve dolandırıcılık gibi dijital suçlar yalnızca ceza normlarıyla değil; eğitim, dijital okuryazarlık, bilinçlendirme, sorumlu platform tasarımı ve sosyal destek politikalarıyla önlenmelidir. Ceza hukuku dijital alanda da en son başvurulacak araç olmalıdır.

Sonuç olarak bu süreç, cezalandırma yerine önlemeyi esas alan bir güvenlik yaklaşımını öne çıkarmış; gizli servislere özgü tekniklerin sıradan emniyet birimleri

---

[585] Europol Crime Areas: Cybercrime, Europol resmi sitesi, https://www.europol.europa.eu/crime-areas/cybercrime (E.T.: 01.02.2026).

[586] NATO Cyber Defence Pledge, NATO resmi metni, https://www.nato.int/cps/en/natohq/official_texts_133177.htm (E.T.: 01.02.2026).

[587] UN Office for Disarmament Affairs Open-Ended Working Group on ICT Security, Birleşmiş Milletler Silahsızlanma İşleri Ofisi, https://meetings.unoda.org/open-ended-working-group/ (E.T.: 01.02.2026).

[588] Joint Communication – The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final), EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018 (E.T.: 01.02.2026).

[589] UN Security Council Open Debate on Cyber Security: Maintaining international peace and security in cyberspace – Concept Note, 29 June 2021, United Nations Security Council, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf (E.T.: 01.02.2026).

[590] Ali Nazım Sözer, "Ceza Hukuku ve Sosyal Devlet", **Prof. Dr. Kemal Oğuzman'a Armağan,** Ankara: İş Hukuku ve Sosyal Güvenlik Hukuku Türk Millî Komitesi Yayını, 1997, s.9-12.

tarafından kullanılmasını mümkün kılmıştır. Dijital çağın güvenlik paradigması, gözetim temelli, sürekli takip gerektiren ve ulusal ile uluslararası düzeyde iç içe geçmiş bir yapıya dönüşmüştür[591].

(4) Milli Teknoloji Kullanımını Zorunlu Kılan Düzenlemeler

Milli teknoloji kullanımını zorunlu kılan düzenlemeler, dijital çağda ekonomik egemenlik, ulusal güvenlik ve teknolojik bağımsızlık hedeflerinin birleştiği stratejik bir politika alanını ifade eder. Dijital altyapıların ve veri akışlarının küresel teknoloji şirketlerine bağımlılığı ve lisans maliyetleri devletleri yerli yazılım ve donanımı teşvik etmeye yöneltmiş; böylece milli ekonomi kavramı veri egemenliği, siber güvenlik ve ulusal dijital kapasite ile bütünleşmiştir.

Birçok ülke, özellikle kritik kamu hizmetlerinde yabancı teknolojiyi sınırlandırıp yerli çözümlere geçişi öngören düzenlemeler benimsemektedir. Örneğin Türkiye'de 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile kamu kurumlarına milli altyapı çözümleri kullanma yükümlülüğü getirilirken[592] Çin 2019'da kamu kurumlarında yabancı yazılım ve donanımların yerli alternatiflerle değiştirilmesini zorunlu kılmıştır[593]. AB ve ABD açık kaynak yazılımların kamu sektöründe teşviki[594] Fransa'da, ücretsiz olan LibreOffice

---

[591] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.6.

[592] Bu tür politikalar, anayasal güvenlik, ekonomik kalkınma ve eşitlik ilkeleriyle bağlantılıdır. 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi 2019'da yayınlanmıştır. 2019/12 Sayılı Bilgi Güvenliği Tedbirleri Cumhurbaşkanlığı Genelgesi, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/ (E.T.: 01.02.2026).

[593] Bu hususta Çin, Microsoft Office yerine WPS Office gibi yerli yazılımları desteklemiştir. China orders state offices to replace foreign computer equipment and software: report, TechNode, 9 Aralık 2019, https://technode.com/2019/12/09/china-orders-state-offices-to-remove-foreign-made-gear-and-software-report/ (E.T.: 01.02.2026).

[594] AB ve ABD kamu kurumlarında açık kaynak yazılım kullanımını, veri güvenliği ve inovasyon gerekçeleriyle teşvik etmektedir. Avrupa Birliği Komisyonu'nun 2021 tarihli kararı: Commission Decision of 8 December 2021 on the open source licensing and reuse of Commission software (2021/C 495 I/01), Official Journal of the European Union, CELEX: 32021D1209(01), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D1209(01) (E.T.: 01.02.2026). ABD'de kamu kurumlarına 2016'da gönderilen yazı: Office of Management and Budget (OMB) Memorandum M-16-21: Federal Information Security Modernization Act (FISMA) Reporting Requirements for Executive Agencies, The White House (Obama Administration archives), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf (E.T.: 01.02.2026).

programının kullanımının yaygınlaştırılması[595] ve Rusya'da yabancı yazılım ve veri merkezlerine getirilen kısıtlamalar[596] dijital korumacılığın diğer örnekleridir. Bu örnekler, dijital korumacılığın dijital egemenlik kapsamında nasıl kesiştiğini ve kamu politikalarının dijital alanı stratejik bir unsur olarak gördüğünü ortaya koymaktadır.

Bu politikalar sadece yerli sanayiyi koruma veya maliyet azaltma amacı taşımamakta; aynı zamanda teknolojik yaptırımlara karşı dayanıklılık, kritik veriler üzerinde tam kontrol ve yabancı şirketlere aşırı bağımlılığın azaltılması gibi egemenlik temelli hedeflere dayanmaktadır. 19 Temmuz 2024'teki Microsoft kaynaklı küresel kesinti[597] yabancı altyapıya bağımlılığın ulusal güvenlik boyutunu görünür kılan güncel bir örnek olmuştur[598]. Küresel firmalara aşırı bağımlılık ve yerli alternatiflerin yokluğu,

---

[595] Fransa'da kamu kuruluşlarında LibreOffice gibi açık kaynaklı yazılımlar kullanılmakta, Microsoft Office gibi yabancı ürünlerden uzaklaşılmaktadır. MIMO: a working group of French ministries to certify a LibreOffice release, Interoperable Europe Portal: Open Source Observatory, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/mimo-working-group-french-ministries-certify-libreoffice-release (E.T.: 01.02.2026).

[596] Rusya, 149-FZ ve 44-FZ ve sayılı yasalarla kamu kurumlarında yabancı yazılım kullanımı sınırlandırılmış; 425-FZ sayılı yasa ile Rusya'da satılmadan önce dijital cihazlara yerli yazılım yüklenmesi zorunlu tutulmuştur. Rusya'da Bilgi, Bilgi Teknolojisi ve Bilgi Koruması Hakkında Federal Yasa (No. 149-FZ) 2006'da yürürlüğe girmiştir. Federal Law No. 149-FZ of 27 July 2006 on Information, Information Technologies and the Protection of Information, accession document for the Russian Federation's WTO membership (WT/ACCR/RUS58/LEG/369), World Trade Organization, https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf (E.T.: 01.02.2026). Kamu İhale Sistemi Hakkında Federal Yasa, Federal Law No. 44-FZ "On the Contract System in the Sphere of Procurement of Goods, Works and Services for Ensuring State and Municipal Needs" (English translation), Federal Antimonopoly Service of the Russian Federation, https://en.fas.gov.ru/netcat_files/File/44-FZ%20eng.pdf (E.T.: 01.02.2026) ve Eleştirel Bilgi Altyapısı Güvenliği Hakkında Federal Yasa 2013'te yürürlüğe girmiştir: In a nutshell: data protection, privacy and cybersecurity in Russia, Lexology (Noerr), 22 October 2020, https://www.lexology.com/library/detail.aspx?g=4e25febc-cb62-422b-a5e2-c62e964e4a3d (E.T.: 1 Şubat 2026). Mobil Cihazlara Önceden Yüklenmiş Yazılım Zorunluluğu: Federal Law No. 425-FZ, On Amending the Article 4 of the Federal Law "On Consumer Rights Protection", December 2, 2019 (WILMap, Stanford University), https://wilmap.stanford.edu/entries/federal-law-no-425-fz-amending-article-4-federal-law-consumer-rights-protection-december-2 (E.T.: 1 Şubat 2026). Bu yasa doğrultusunda 2021 yılında Yerli Teknoloji ve Yazılım Kullanımına Yönelik Kararname çıkarılmıştır. Russia: mandatory pre-installation of Russian software on electronic devices from 01.01.2021, Schneider-Group, https://schneider-group.com/en/news/countries/russia-mandatory-pre-installation-of-russian-software-on-electronic-devices-from-01-01-2021/ (E.T.: 1 Şubat 2026).

[597] "Küresel 'restart': Dünya çapında işletmeleri etkileyen büyük bir yazılım sorunu yaşanıyor", *Anadolu Ajansı,* https://www.aa.com.tr/tr/dunya/kuresel-restart-dunya-capinda-isletmeleri-etkileyen-buyuk-bir-yazilim-sorunu-yasaniyor/3279453 (E.T.: 1 Şubat 2026).

[598] Türkiye'de BTK, kesintinin siber bir saldırıdan değil, Microsoft'un güncellemesinden kaynaklandığını açıklamıştır. Ziyahan Albeniz, "IT Sistemleri "Mavi Ekran" verdi, dünya sanal olarak çöktü", *Serbestiyet,* https://serbestiyet.com/featured/dunyaya-kuresel-siber-kesintinin-sokunda-174927/ (E.T.: 1 Şubat 2026). Bu tür olaylar, kamu hizmetlerinin kesintisiz devamı için milli teknolojilerin yalnızca bir tercih değil, zorunluluk olduğunu göstermektedir.

özellikle kritik anlarda ciddi zararlara yol açabileceğinden, bu durumun aynı zamanda bir ulusal güvenlik meselesi olduğu açıktır.

Milli teknoloji kullanımını zorunlu kılan hukuki düzenlemeler, salt teknik veya ekonomik tercihler olmaktan ziyade, dijital egemenliğin yeniden yapılandırılması sürecinin temel bileşenleri olarak değerlendirilmelidir. Bu düzenlemeler, aynı zamanda veri yerelleştirme politikaları ile sıkı bir ilişki içindedir. Devletler, küresel dijital ekonominin içine dahil olmayı sürdürürken; kritik veri setleri ve teknolojik altyapılar üzerindeki tam yetkiyi koruma amacıyla veri yerelleştirmeye yönelmektedir. Bu durum, dijital egemenliğin yeni ve çok katmanlı bir biçimde şekillendiğinin göstergesidir. Örneğin, Rusya'da 2017'de kabul edilen Federal Yasa No. 187-FZ ile enerji, ulaşım, finans ve sağlık gibi stratejik sektörlerde yabancı yazılım kullanımı sınırlandırılmış; veri merkezlerinin ülke sınırları içinde olması zorunlu kılınmıştır[599].

Milli teknolojinin kapasitesinin önemi, şifreleme teknolojilerinin tarihsel gelişiminde de gözlemlenir. ABD, güçlü şifreleme ihracatına sınırlamalar getirerek kendi güvenlik kurumlarının erişimine açık, arka kapı bırakan eski standartları (DES gibi) tercih etmiş; benzer şekilde Rusya ve Çin de veri erişiminde devlet çıkarlarını önceliklendirmiştir[600].

b. Teknik Mekanizmalar

Devletler tarihsel olarak teknolojik ilerlemenin itici gücü olmuş ve dijital çağda kontrol kapasitesini sofistike araçlarla en ücra noktalara kadar genişletmiştir. Teknoloji devrimini başlatan da bireysel girişimciler değil, devletin sağladığı finansman ve yönlendirmedir[601]. Devletler, veri yerelleştirme sistemleri ve yapay zekâ yazılımları gibi atılımlar ile dijital altyapılarını geliştirerek dijital egemenliklerini pekiştirmekte ve dijital alandaki aktör niteliklerini göstermektedir[602]. Büyük veri, 5G, yapay zekâ ve kuantum

[599] "In a nutshell: data protection, privacy and cybersecurity in Russia," *Lexology (Noerr*), 22 October 2020, https://www.lexology.com/library/detail.aspx?g=4e25febc-cb62-422b-a5e2-c62e964e4a3d (E.T.: 1 Şubat 2026).
[600] Aust ve Ammann, s.17.
[601] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.88.
[602] Floridi, s.370-371.

teknolojileri, artık sadece gelişmişlik göstergesi değil; jeopolitik rekabetin yeni belirleyici alanları olarak dijital egemenlik mücadelesini artırmaktadır[603]. Devletler, dijital alandaki hızlı teknolojik gelişmelere yanıt verebilmek için yüksek kapasiteli bilgisayar altyapısı[604] yerli mikroçip üretimi[605] bağımsız bulut hizmetleri[606] güçlü internet altyapısı[607] internet servis sağlayıcılarının kontrol altına alınması[608] gibi araçlar geliştirmektedir.

(1) Gözetim Teknolojisi ve İçerik Denetim Araçları

Devletler dijital alandaki iktidarlarını pekiştirmek için gözetim teknolojileri, içerik denetim mekanizmaları ve iletişim kısıtlama araçlarından oluşan geniş bir teknik araç seti kullanmaktadır. Bu araçlar hem bireylerin çevrimiçi davranışlarını izlemeye hem de toplumsal eğilimlerin analizini mümkün kılarak dijital kamusal alanı kontrol etmeye

---

[603] Gloria Özdemir, s.vii.

[604] Almanya, 2021'de Avrupa'nın ilk kuantum bilgisayarı IBM Quantum System One'ı açmış; Şansölye Merkel, bunun teknolojik egemenlik ve ekonomik büyüme için önemli olduğunu vurgulamıştır. Yasir Ölmez, "Almanya, İlk Kuantum Bilgisayarını Tanıttı", *Kuantum Türkiye*, https://kuantumturkiye.org/almanya-ilk-kuantum-bilgisayarini-tanitti/ E.T.: 1 Şubat 2026). AB, EuroHPC projesi kapsamında 9 süper bilgisayara sahiptir. "Our Supercomputers", *EuroHPC Joint Undertaking*, https://eurohpc-ju.europa.eu/supercomputers/our-supercomputers_en (E.T.: 1 Şubat 2026).

[605] Çin'e bağımlılığı azaltmak için ABD, mikroçip ve işlemci ekosistemini güçlendiren CHIPS Act'i çıkarmıştır. 2021'de Avrupa Komisyonu Başkanı Ursula von der Leyen de bu alanın teknolojik egemenlik için önemli olduğunu vurgulayarak AB'nin düzenleme yapacağını açıklamıştır. Report: CHIPS Act is Just First Step to Addressing Threats to U.S. Leadership in Advanced Computing, MIT News, 28 February 2023, https://news.mit.edu/2023/report-chips-act-just-first-step-addressing-threats-us-leadership-advanced-computing-0228 (E.T.: 01.02.2026); European Chips Act: A Vital Step in the Right Direction, Wilson Center, https://www.wilsoncenter.org/article/european-chips-act-vital-step-right-direction (E.T.: 01.02.2026).

[606] 2011'de ABD, bulut teknolojilerinin güvenli kullanımı için FedRAMP adlı bulut hizmet standartlarını belirleyen programı başlatmıştır. FedRAMP Program Basics, Federal Risk and Authorization Management Program (FedRAMP), https://www.fedramp.gov/program-basics (E.T.: 01.02.2026). 2020'de AB, 2030 Dijital Pusula programı kapsamında European Alliance for Industrial Data, Edge and Cloud'u kurmuş ve Data Governance Act ile verinin güvenli paylaşım ve depolanmasını sağlayacak bulut altyapıları oluşturmayı hedeflemiştir. Cloud Computing Services: European Alliance for Industrial Data, Edge and Cloud | Digital Compass Library (video), Futurium (European Commission platform), https://futurium.ec.europa.eu/en/digital-compass/digital-businesses/library-video/cloud-computing-services-european-alliance-industrial-data-edge-and-cloud (E.T.: 01.02.2026).

[607] Sağlık, iş ve eğitime uzaktan erişim sağlamak için dijital dönüşümde hızlı internet önemli olması nedeniyle fiber optik ve 5G altyapısına yatırım yaparak, dijital eşitsizlikleri azaltmak için ülke genelinde internet erişimini ve hızını artıran erişim noktaları kurulmaktadır. "5G in rural areas: spotlight", Ericsson Blog, 5 Temmuz 2020, https://www.ericsson.com/en/blog/2020/7/5g-in-rural-areas-spotlight (E.T.: 01.02.2026).

[608] Rusya'nın Runet, İran'ın Ulusal Bilgi Ağı ve Kuzey Kore'nin Kwangmyong ağı, devletlerin interneti küresel ağdan bağımsız, yerel bir ağ olarak kontrol etmesini sağlar. Yurtdışındaki içeriklere erişimin kısıtlanabilmesi ile devlet kendi propaganda ve bilgi akışını yönetebilir. Jane Wakefield, "Russia 'successfully tests' its unplugged internet", *BBC*, 24 December 2019, https://www.bbc.com/news/technology-50902496 (E.T.: 01.02.2026); Elizabeth Schulze, "Tech Russia just brought in a law to try to disconnect its internet from the rest of the world", *CNBC*, 1 Ekim 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html (E.T.: 01.02.2026).

yöneliktir. Devletler, yalnızca dijital alanı teknik olarak denetlemekle kalmayıp, kamuoyu oluşturma süreçlerine etki edebilmek, muhalif sesleri bastırmak ve dış aktörlerin etkisini zayıflatmak amacıyla dijital araçları etkin biçimde kullanmaktadır.

Gözetim teknolojileri; internet trafiği takibi, yüz tanıma sistemleri, yapay zekâ destekli analiz araçları ve casus yazılımlar gibi yöntemlerle devletlere kapsamlı izleme kapasitesi sağlar. ABD'de NSA'nın küresel izleme programları[609] Çin'in Golden Shield ve Great Firewall projeleri[610] Hindistan[611] ve Suudi Arabistan'ın[612] çevrimiçi davranış izleme yetkileri bu eğilimin belirgin örnekleridir. Dahası, dijital gözetim kapasitelerini artırmak amacıyla, bireylerin dijital cihazlarına veya iletişim ağlarına sızarak veri toplama yöntemlerine başvurulmaktadır. Bu durum, devlet açısından, özellikle ulusal güvenlik gerekçeleriyle meşrulaştırılmaya çalışılsa da bireysel mahremiyetin ve temel hakların ihlali riskini beraberinde getirmektedir. Örneğin, İsrailli NSO Group tarafından geliştirilen Pegasus adlı casus yazılım, hedef alınan mobil cihazlara uzaktan sızarak mesajlar, aramalar, konum verileri ve cihazın mikrofonu ile kamerasına erişim sağlayabilmektedir[613]. Bu tür teknolojilerin kullanımı, yalnızca özel yaşamın gizliliği açısından değil, aynı zamanda uluslararası insan hakları hukuku bağlamında da ciddi

[609] NSA, 1952'de kurulan ve varlığı uzun süre gizli tutulan bir istihbarat kurumu olarak küresel iletişim ağlarını izleme, şifreleme faaliyetlerini yürütme ve stratejik enformasyonu analiz etme görevini üstlenmiştir. Edward Snowden'ın 2013'teki ifşaları, NSA'nın dünya genelinde yürüttüğü kitlesel gözetim programlarını ortaya çıkararak bireysel mahremiyetin ihlali ve demokratik denetimin zayıflığı konusunda yoğun tartışma başlatmıştır. "Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress", *American Civil Liberties Union* (ACLU), https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress (E.T.: 01.02.2026).

[610] Çin'de 1998 yılında başlatılan Golden Shield Projesi ve Great Firewall uygulamaları, dijital içeriklerin filtrelenmesi ve kullanıcı faaliyetlerinin izlenmesi amacıyla geliştirilmiştir. "Great Firewall", Encyclopædia Britannica, https://www.britannica.com/topic/Great-Firewall (E.T.: 01.02.2026).

[611] Hindistan bu yetkileri 2018 yılında çeşitli güvenlik kurumlarına vermiştir. "Surveillance Laws in India & Pegasus Project", *Boom Live*, https://www.boomlive.in/law/surveillance-laws-in-india-pegasus-project-13962 (E.T.: 01.02.2026).

[612] Suudi Arabistan çevrimiçi davranışları takip eden yazılımlar kullanmaktadır. Saudi Arabia: Freedom on the Net 2021 Country Report, Freedom House, https://www.freedomhouse.org/country/saudi-arabia/freedom-net/2021 (E.T.: 01.02.2026).

[613] "The Pegasus Project: Unmasking the NSO Group's Spyware", *Amnesty International*, 18 Temmuz 2021, https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/ (E.T.: 01.02.2026); "NSO: Who are the spyware makers at the centre of the Pegasus scandal?", *The Independent*, https://www.independent.co.uk/news/world/nso-who-spyware-pegasus-b1886786.html (E.T.: 01.02.2026).

tartışmalara yol açmaktadır. Söz konusu uygulamalar, gözetim faaliyetlerinin sınırlarını ve devletin birey üzerindeki denetim gücünü yeniden düşünmeyi zorunlu kılmaktadır.

Gözetim teknolojileri; devletlerin yalnızca bireyleri değil, yüksek çözünürlüklü uydu sistemleri ve küresel konumlama ağları aracılığıyla diğer devletlerin fizikî varlıklarını ve hareketlerini anlık izleme kapasitesi kazandırarak egemenliğin dijital boyutunu tartışmaya açmıştır. Copernicus örneğinde görüldüğü gibi, insani amaçlarla geliştirilen sistemler dahi fiilen stratejik gözetim araçlarına dönüşmektedir[614]. Bu durum, rıza dışı izleme faaliyetlerinin dijital egemenlik ihlali sayılıp sayılmayacağı sorusunu gündeme getirmektedir. Artık egemenlik yalnızca toprak üzerinde değil, dijital altyapı, veri setleri ve gözetim teknolojileri üzerinde hâkimiyetle tanımlanmaktadır. Uydu haritalama sistemleri, veri trafiğini işleyen algoritmalar ve anlık konum bazlı gözetim sistemleri, artık yalnızca fizikî değil, aynı zamanda algoritmik ve siber mekânlar üzerinde de gücü mümkün kılmaktadır. Bu platformlar üzerinden elde edilen konum verileri, hareket profilleri ve mekânsal eğilimler, gerektiğinde istihbarat servisleriyle paylaşılmakta veya askeri amaçlarla değerlendirilebilmektedir. Google Maps, Starlink, Yandex veya Beidou gibi platformlar, sivil hizmetlerin ötesinde jeopolitik güç projeksiyonunun araçlarıdır.

Davranış ve içerik denetimi; güvenlik kameralarının yapay zekâ ile bütünleşmesi, toplumsal hareketlerin analiz edilmesi ve kamusal alanın sürekli gözetimi şeklinde somutlaşmaktadır. Devletler de gelişmiş büyük teknoloji şirketleri gibi veri analitiği yapmaktadırlar. Pahalı ve teknik açından zor olan bu teknoloji, aktarılan bilgiyi filtreleyip analiz etmeyi sağlayan ve devletin bir internet sayfasına erişimi engellemesinden ileri bir düzeydir[615]. Çin'in yüz tanıma sistemlerine dayalı kent

[614] AB Copernicus Programı, teknik olarak çevre ve iklim izleme gibi insani hedefleri desteklemeye yönelik bir yeryüzü gözlem sistemi olsa da pratikte yüksek çözünürlüklü uydu görüntüleriyle ülkelerin anlık hareketlerini izleyebilecek düzeyde bir dijital gözetim aracıdır. 2024 yılında İran Cumhurbaşkanı'nı taşıyan helikopterin düşmesi sonrası İran'ın bu sistemden yardım talep etmesi, bu tür sistemlerin kriz anlarında ne kadar stratejik hâle geldiğini göstermiştir.

[615] Jack Margolin, "Russia, China, and the Push for 'Digital Sovereignty'", *Globalvioces*, 2 Aralık 2016, https://tr.globalvoices.org/2016/12/rusya-cin-ve-dijital-egemenlik-ihtiyaci/ (1 Şubat 2026).

gözetimi[616] Birleşik Krallık[617] ve Singapur'un[618] kamusal alanda anlık davranış ve potansiyel tehdit analizi altyapıları bu modellerin en ileri örnekleridir. Bu denetim biçimi kamu düzeni gerekçesiyle meşrulaştırılsa da gözetim toplumunu ve otoriter eğilimleri beslemekte; anonim hareket ve ifade özgürlüğünü zayıflatmakta; denetlenebilir, hesap verebilir ve hak temelli bir gözetim rejimi ihtiyacını gündeme getirmektedir.

Dijital içerik kontrolü; sansür, filtreleme, erişim engelleme ve algoritmik bastırma teknikleriyle yürütülmektedir. Türkiye'de 5651 sayılı Kanun çerçevesindeki teknik erişim engelleri[619] Çin'in Great Firewall'u ve Hindistan'ın toplumsal düzeni gerekçesiyle içeriği teknik önlemler bu denetimin farklı örnekleridir.

Devletler, dijital alanı yalnızca güvenlik için değil, siyasi istikrar ve resmi söylemi korumak amacıyla da teknik denetimlerle kontrol etmektedir. Bu denetimler bilgi akışını kısıtlayarak dijital söylem egemenliğini yeniden üretir; algoritmik sansürle uygunsuz görülen içerikler otomatik biçimde kaldırılır. Dijital alanın müdahaleye daha elverişli olması, ifade özgürlüğü ve bilgiye erişim açısından ciddi riskler doğurur; demokratik katılımı zayıflatır, idari takdiri genişletir ve yargısal denetimi güçsüzleştirir.

İnternet kesintileri ve iletişim engellemeleri, protesto ve siyasi kriz dönemlerinde devletlerin dijital alandaki en sert müdahale araçlarından biridir. Sık sık

---

[616] Çin'de yüz tanıma teknolojileri, şehir çapında kurulan kameralarla bütünleştirilerek vatandaşların kimlik tespiti ve hareket takibi sağlanmaktadır. "Behind the Rise of China's Facial Recognition Giants", *Wired,* https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/ (E.T.: 01.02.2026).

[617] "The use of overt surveillance camera systems in public places by police forces in England and Wales: an assessment of compliance with the Protection of Freedoms Act 2012" Police Survey 2022: responses and key findings, UK Government (Home Office), https://www.gov.uk/government/publications/police-survey-2022-responses-and-key-findings/the-use-of-overt-surveillance-camera-systems-in-public-places-by-police-forces-in-england-and-wales-an-assessment-of-compliance-with-the-protection-o (E.T.: 01.02.2026).

[618] "Police surveillance system using video analytics to detect targets wins Home Team Science & Technology Agency award", *The Straits Times,* https://www.straitstimes.com/singapore/community/police-surveillance-system-using-video-analytics-to-detect-targets-wins-home (E.T.: 01.02.2026).

[619] Türkiye'de 5651 sayılı İnternet Kanunu m. 8 ve devamındaki hükümler çerçevesinde Bilgi Teknolojileri ve İletişim Kurumu, mahkeme kararları ya da idari işlemlerle içeriklere müdahale edebilmektedir. Bkz. "Engellenen Siteler", Journo.com.tr, https://journo.com.tr/engellenen-siteler (E.T.: 01.02.2026). Ayrıca, sosyal medya içeriklerinin kaldırılması talepleri vatandaşlar tarafından e-Devlet sistemi aracılığıyla iletilebilmektedir. "Erişim Sağlayıcıları Birliği Erişim Engeli Başvurusu", e-Devlet (turkiye.gov.tr), https://www.turkiye.gov.tr/esb-erisim-engeli-basvurusu (E.T.: 01.02.2026).

gündeme gelen Keşmir[620] İran, Mısır[621] Türkiye[622] Rusya[623] Suriye ve Venezuela örnekleri, bu uygulamaların güvenlikten çok eleştirel sesleri bastırmaya ve kriz anlarında toplumsal mobilizasyonu kontrol etmeye yönelik olduğunu göstermektedir. Seçici site engellemeleri ve sosyal medya yasaklarıyla devletler dijital kamusal alanı yönlendirilmiş bir iletişim ortamına dönüştürmekte; dijital içerik sansürü, modern devletin dijital egemenlik stratejilerinin merkezi bir unsuru hâline gelmektedir. Benzer şekilde dezenformasyon ve propaganda araçları; bot ağları, trol hesaplar ve sahte haberlerle kamuoyunu yönlendirmek için kullanılmaktadır. Rusya'nın 2016 ABD seçimlerindeki dezenformasyon kampanyası, Kuzey Kore'nin nükleer programı hakkında yaydığı bilgi kirliliği[624] Çin'in Hong Kong protestolarına yönelik çevrim içi müdahaleleri[625] ve Suriye'nin dijital propaganda birlikleri[626] bu kapasitenin uluslararası boyutunu ortaya koyar.

Bütün bu teknik mekanizmalar, dijital çağda egemenliğin yalnızca toprak üzerinde değil, veri akışları, gözetim kapasitesi ve dijital altyapı üzerindeki hâkimiyetle

---

[620] Hindistan, 2019 yılında Jammu ve Keşmir'deki kitlesel protestolar sırasında interneti uzun süreli olarak kapatmıştır. Bu müdahale, ifade özgürlüğü ve bilgiye erişim hakkı açısından uluslararası alanda yoğun eleştirilere konu olmuştur. "India: A grim milestone 365 days of internet shutdown in Kashmir", International Federation of Journalists (IFJ), https://www.ifj.org/media-centre/news/detail/article/india-a-grim-milestone-365-days-of-internet-shutdown-in-kashmir (E.T.: 01.02.2026).

[621] Mısır, 2011'de Arap Baharı olarak adlandırılan dönemde ülke genelinde interneti tamamen devre dışı bırakarak dijital muhalefetin örgütlenme olanaklarını ortadan kaldırmıştır. "Egypt's Internet Went Down for Days: Here's What Happened", *Wired*, https://www.wired.com/2011/01/egypt-internet-down/ (E.T.: 01.02.2026).

[622] Nagihan Tufan Yeniçıktı, "İletişimsel Eylem ve Facebook: Gezi Parkı Olaylarında Sosyal Medyanın Gücü", **Selçuk İletişim Dergisi,** Vol.8, (2014), s.2.

[623] "Submission to the Human Rights Committee: Human Rights Watch Russian Federation", *Human Rights Watch,* 15 February 2022, https://www.hrw.org/news/2022/02/15/submission-human-rights-watch-russia-human-rights-committee (E.T.: 01.02.2026).

[624] Kuzey Kore, nükleer programını meşrulaştırmak ve uluslararası kamuoyunu etkilemek amacıyla sosyal medyada sahte hesaplar üzerinden bilgi kirliliği yaymaktadır. "North Korea Turns to Cyber and Disinformation Attacks Amid Global Coronavirus Outbreak", *Foundation for Defense of Democracies* (FDD), 1 April 2020, https://www.fdd.org/analysis/2020/04/01/north-korea-turns-to-cyber-disinformation-attacks-amid-global-coronavirus-outbreak/ (E.T.: 01.02.2026).

[625] Çin, Hong Kong'daki protestoları itibarsızlaştırmak için sosyal medya üzerinden organize dezenformasyon faaliyetleri yürütmektedir. "China's internet censorship uses distraction as well as repression", *The Guardian,* 22 January 2017, https://www.theguardian.com/commentisfree/2017/jan/22/chinese-internet-censorship-uses-distraction (E.T.: 01.02.2026).

[626] Suriye rejimi, iç savaş süresince 'Suriye Elektronik Ordusu' gibi yapılar aracılığıyla dijital ortamda propaganda üretmiştir. Syria's 'social media war' (since 2011), *International Cyber Law Wiki* (CCDCOE), https://cyberlaw.ccdcoe.org/wiki/Syria%E2%80%98s_%E2%80%98social_media_war%E2%80%99_%28since_2011%29 (E.T.: 01.02.2026).

tanımlandığını göstermektedir. Devletler dijital araçları kullanarak hem içeriyi kontrol altında tutmakta hem de dış politikada yeni bir dijital güç biçimi inşa etmektedir. Bu nedenle veri yerelleşmesi ve teknolojik özerklik, ekonomik tercihler değil, egemenliği koruma stratejileridir. Gücün, konvansiyonel klasik askerî kapasiteden dijital tekno-güce doğru evrildiğinin göstergesidir.

(2) Dijital Adalet Mekanizmaları

Dijital adalet, geleneksel adalet süreçlerinin dijital ortama taşınmasıdır. Dijital adalet mekanizmaları; devletlerin yargı süreçlerini hızlandırmak, erişilebilir kılmak ve teknik altyapı üzerinden merkezi kontrolü güçlendirmek amacıyla geliştirdiği dijital araçları ifade eder. E-duruşma, e-arabuluculuk, e-tahkim ve çevrimiçi dava yönetim ve belge sunma sistemleri birçok ülkede yaygınlaşmış; Türkiye'deki UYAP gibi Almanya[627] Estonya[628] Fransa[629] ve İngiltere[630] gibi ülkelerdeki örnekler dijital başvuru ve çevrimiçi yargılama platformları kurarak adalete erişimi kolaylaştırmıştır.

Çin'in 2016 tarihli Akıllı Mahkeme Reformu, yargı süreçlerini dijitalleştirirken aynı zamanda yargıçları merkezi denetime daha açık hâle getirmiş; yapay zekâ tabanlı karar destek sistemleri düşük profilli davalarda otomatik öneri ve karar üretmeye başlamıştır. Fakat teknik modernleşmenin ötesinde yargısal takdir yetkisinin daralması ve Partinin yargı üzerindeki kontrolünün güçlenmesi nedeniyle eleştirilmiştir[631].

Ceza adaletinde yapay zekâ destekli öngörücü analizler ve dijital izleme araçları suçun önceden tahmin edilmesine ve müdahaleye imkân vermektedir[632]. Ancak

---

[627] "Remote courts in Germany: digital transformation of the judiciary", Dispute Resolution Germany, 6 May 2020, https://www.disputeresolutiongermany.com/2020/05/remote-courts-in-germany/ (E.T.: 01.02.2026).
[628] Artificial Intelligence as the New Reality of e-Justice, e-Estonia, https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (E.T.: 1 Şubat 2026).
[629] CMS Expert Guide to Digital Litigation: France, CMS (Expert Guides), https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-litigation/france (E.T.: 1 Şubat 2026).
[630] Money Claim Online platformu, küçük meblağlı (konusu 10.000 sterlin ile sınırlı) davaların tamamen dijital yürütülmesini sağlar. Making a small claim, Citizens Advice, https://www.citizensadvice.org.uk/law-and-courts/legal-system/small-claims/making-a-small-claim/ (E.T.: 1 Şubat 2026).
[631] Papagianneas ve Knight, s.39-41.
[632] İlknur Aydın, "Suç Tahmini", **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.45.

masumiyet karinesi, özgürlükler ve ayrımcılık riski açısından ciddi sorunlar doğurmaktadır. Dijital arama-el koyma ve risk analiz sistemlerinin yaygınlaşmasında teknolojik verimlilik gerekçesi henüz kesinlik kazanmamakla birlikte özgürlüklerin korunması daha öncelikli bir hassasiyettir[633].

Uluslararası karşılıklı hukuki yardım mekanizmaları açısından sınır ötesi veri talepleri bağlamında, karşılıklı hukuki yardım mekanizmaları egemenliğe saygı ve prosedürel meşruiyet açısından önem taşımaktadır. Avrupa Konseyi'nin 1959 tarihli Karşılıklı Yardım Sözleşmesi ve 2008 tarihli Siber Suçlara Karşı İş Birliği Kılavuz Esasları, doğrudan hizmet sağlayıcıya başvurmak yerine uluslararası hukuk çerçevesinde iş birliği yapılmasını tavsiye etmektedir[634]. Bu yöntem, hem dijital delil taleplerinin şeffaflığını artırmakta hem de ilgili ülkeler arasında güven esasına dayalı bir veri paylaşımı sistemi geliştirmektedir[635].

Dijital adalet mekanizmaları açısından hukuki işlemlerin dijitalleşmesi artık sadece pratiklik değil, hukuk güvenliği ve öngörülebilirliğin gereğidir. Dokunmatik imzalı belgeler uyuşmazlıklarda delil olarak kullanılabilse de mevzuat, yalnızca güvenli elektronik imzaya senet güvencesi tanımaktadır. Bu nedenle dokunmatik imzalı belgeler kural olarak HMK m.199 kapsamında takdiri delildir; imzanın kopyalanabilmesi ve orijinal/tek nüsha güvencesinin zayıflığı nedeniyle doğrudan senet sayılmaları güçtür[636].

Dijitalleşmenin yargıya entegrasyonu, aynı zamanda güvenilirlik ve hukuki altyapı tartışmalarını da büyütmektedir. 2024'te ABD'de bir mahkemenin yapay zekâ tarafından hazırlanmış raporu güvenilir bulmaması, teknolojinin yargıda kullanılabilmesi

---

[633] Özge Sırma Gezer, "Koruma Tedbirleri Bakımından Dijitalleşme", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.58; Saka, s.76.

[634] 2008 tarihli Kanun Yürütme Makamları ve İnternet Hizmet Sağlayıcıları Arasında Siber Suçlara Karşı İşbirliği Kılavuz Esasları m. 36, Council of Europe, Guidelines on Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, Strasbourg, 1–2 April 2008, https://rm.coe.int/16802fe14d (E.T.: 1 Şubat 2026).

[635] Irion, *"Government Cloud Computing and National Data Sovereignty",* s.63.

[636] Süleyman Topak, "Dokunmatik Ekran İmzası ile Oluşan Dijital Belgenin Delil Değeri", **GSÜHFD**, Cilt.2025, Sayı.2, 2025, s.1594-1596.

için bilimsel standartların ve açık yasal çerçevelerin zorunlu olduğunu ortaya koymuştur[637].

Dijital adalet sistemleri verimlilik ve erişim sağlasa da aşırı otomasyon, yargıcın takdir yetkisinin daralması, siyasal denetimin artması ve adaletin insani boyutunun zayıflaması gibi ciddi riskler taşır. Özellikle otoriter rejimlerde dijital araçlar, yargıyı merkezîleştiren ve standartlaştıran bir iktidar teknolojisine dönüşerek adaletin niteliğini ve yargıya duyulan güveni zedeleyebilir[638]. Bu nedenle dijitalleşme, kolaylıklarının yanı sıra güvenilirlik, şeffaflık ve hesap verebilirlik açısından dikkatle ele alınmalıdır.

(3) Siber Güvenliğe Yönelik Teknik Araçlar

Devletlerin siber güvenliğe yönelik teknik araçları, dijital altyapılarını ve kritik sektörlerini (enerji, sağlık, ulaşım, finans gibi) korumanın ötesine geçerek dijital egemenliği pekiştiren stratejik bir güç alanı hâline gelmiştir. Ulusal siber güvenlik stratejileri; kritik altyapıların korunması, siber istihbarat[639] aktif savunma ve tehdit tespiti gibi unsurlarla hem savunma kapasitesini hem de devletin dijital alandaki otoritesini güçlendirmektedir. ABD[640] Almanya[641] Birleşik Krallık 2022 Siber Güvenlik Stratejisi, Fransa 2021 Siber Güvenlik ve Savunma Stratejisi gibi girişimlerle saldırı tespit araçları,

---

[637] Hâkim, yapay zekanın destekleyici bir araç olabileceğini kabul etmekle birlikte, bu tür teknolojilerin mahkemelerde kullanılabilmesi için güvenilirliklerinin bilimsel olarak kanıtlanması ve net yasal kuralların oluşturulması gerektiğini belirtmiştir. Matter of Weber 2024 NY Slip Op 24258 Decided on October 10, 2024 Surrogate's Court, Saratoga County Schopf, https://law.justia.com/cases/new-york/other-courts/2024/2024-ny-slip-op-24258.html; "Davada Yapay Zeka Kullanımı Mahkemede Tartışma Yarattı", *TürkiyeHukuk.org*, https://www.turkiyehukuk.org/davada-yapay-zeka-kullanimi-mahkemede-tartisma-yaratti/ (E.T.: 1 Şubat 2026).

[638] Papagianneas ve Knight, s.43, 44.

[639] Siber casusluk işlerine karşı siber istihbarat; kritik altyapıların ve verilerin korunması, hedef sistemlere yönelik aktif siber operasyonlar ve potansiyel tehditlerin tespiti ve önlenmesini içerir. "Çağın dijital atom bombası," *Yirmidort.tv,* 22 Kasım 2024, https://www.yirmidort.tv/gundem/cagin-dijital-atom-bombasi-210490 (E.T.: 1 Şubat 2026).

[640] ABD'nin 2018 Siber Güvenlik Stratejisi ve NIST'in 2014 Siber Güvenlik Çerçevesi, kamu-özel sektör iş birlikleriyle birlikte yürütülen savunma odaklı politikaların hukuki zemine oturtulmasına öncülük etmektedir. ABD'nin oluşturduğu ulusal güvenli iletişim ağları, dijital ortamda mutlak kontrol sağlamayı amaçlamaktadır. DifferenceBetween.net, "Difference Between NIPRNet and SIPRNet," https://www.differencebetween.net/technology/protocols-formats/differences-between-niprnet-and-siprnet/ (E.T.: 1 Şubat 2026).

[641] Federal Ministry of the Interior and Community (BMI), "Better protection for critical infrastructure," 28 Temmuz 2023, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2023/07/ge-kritis.html (E.T.: 1 Şubat 2026).

şifreleme teknikleri ve yapay zekâ tabanlı analiz sistemlerine yatırım yaparak dijital savunmalarını kurumsallaştırmıştır[642].

Bu gelişmeler, siber güvenliğin yalnızca bir savunma hattı değil, aynı zamanda devletin dijital alandaki otoritesini pekiştirdiği araçlar haline geldiğini göstermektedir. Çin örneği, bu eğilimin en keskin biçimlerinden biridir. Çin, siber güvenliği ulusal güvenlik doktrininin merkezine yerleştirerek hem savunma hem de saldırı kapasitesini dijital güç projeksiyonu için kullanmakta, kamu-özel sektör entegrasyonunu derinleştirmektedir[643].

Siber saldırı simülasyonları ve uluslararası tatbikatlar, siber güvenliğin askeri ve diplomatik boyut kazandığını göstermektedir. NATO'nun Estonya'daki tatbikatları[644] ve ABD'nin Cyber Command yapılanması[645] siber alanın yeni çatışma zemini hâline geldiğini ortaya koyar.

Siber güvenlik faaliyetleri yalnızca savunma ile sınırlı değildir. Rus hackerların Ukrayna altyapısına müdahaleleri[646] ve Almanya'ya yönelik APT28'in SolarWinds siber

---

[642] AB'nin GDPR kapsamındaki şifreleme yükümlülüğü (m. 32), bu teknik yaklaşımın farklı örneklerini oluşturur. Yapay zekâ ve makine öğrenimi, saldırı tespiti ve müdahale süreçlerini otomatikleştirme vaadiyle öne çıkarılmakta; Fransa'nın geliştirdiği analiz araçları ve ABD'nin kritik altyapılar için oluşturduğu tehdit yanıt sistemleri buna örnektir. Commission Nationale de l'Informatique et des Libertés (CNIL), "The CNIL creates an Artificial Intelligence Department and begins to work on learning databases," 26 Ocak 2023, https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases (E.T.: 1 Şubat 2026); Cybersecurity and Infrastructure Security Agency (CISA), "National Cybersecurity Protection System (NCPS)," https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system (E.T.: 1 Şubat 2026).

[643] Başkan Xi Jinping'in siber güvenlik olmadan ulusal güvenlik olmaz vurgusu, siber güvenliğin yalnızca koruyucu değil, aynı zamanda saldırgan kapasitenin inşasında da stratejik bir unsur olarak değerlendirildiğini ortaya koyar. Mei Danowski, "Becoming a Cyber Superpower: China Builds Offensive Capability with Military, Government, and Private Sector Forces", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (171-196), Maryland: Rowman & Littlefield Publishers., 2023, s.187.

[644] NATO bünyesinde Estonya'da her yıl gerçekleştirilen "Kilitli Kalkanlar" tatbikatı sadece siber savunma stratejilerini değil aynı zamanda uluslararası iş birliği olanaklarını da sınamaktadır. T.C. Millî Savunma Bakanlığı, "Kilitli Kalkan-2025 Tatbikatı Basın Duyurusu," https://www.msb.gov.tr/Basin-ve-Yayin/Aciklamalar/2baf4d7de031407e801609e83c11a606 (E.T.: 1 Şubat 2026).

[645] National Security Agency (NSA), "How NSA, U.S. Cyber Command are defending midterm elections: One team, one fight," 25 Ağustos 2022, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight/ (E.T.: 1 Şubat 2026).

[646] Cybersecurity and Infrastructure Security Agency (CISA), "ICS Alert: IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure," 20 Temmuz 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (E.T.: 1 Şubat 2026).

saldırısı[647] ve Kuzey Kore'nin 2017'deki WannaCry saldırısı gibi örnekler devletlerin siber casusluk faaliyetleri ve saldırı operasyonları yürüterek dijital alanı doğrudan bir çatışma sahasına dönüştürdüğünü göstermektedir.

Askerî alanın dijitalleşmesiyle siber güvenlik, küresel güç dengelerini belirleyen stratejik bir unsur hâline gelmiştir. Yapay zekâ destekli otonom sistemler, insansız araçlar ve hedef tanıma teknolojileri savaş kapasitesini dönüştürerek siber güvenliği teknik bir savunma alanının ötesine taşımakta, devlet egemenliğinin merkezî bir bileşeni yapmaktadır. Tarihsel olarak askerî teknolojide üstünlük sağlayan aktörlerin stratejik avantaj elde ettiği düşünüldüğünde, yapay zekânın günümüzde bu güç döngüsünü yeniden üretmesi olasıdır.

c. Egemenlik ile Ekonomik Rasyonalite Arasında Korumacı Politika İkilemi: Veri Yerelleşmesi

Verinin stratejik ekonomik meta ve güvenlik unsuru hâline gelmesi, dijital veri ekonomisine devlet müdahalesini meşrulaştırmıştır. Devletler egemenliklerini güçlendirmek amacıyla korumacı politikalara yönelmekte; veri yerelleşmesi, yerli girişimlerin desteklenmesi ve yabancı teknoloji şirketlerinin sınırlandırılması bu politikanın merkezinde yer almaktadır. Avrupa Parlamentosu'nun stratejik şirketlerin yabancı yatırımlarla satın alınmasını sınırlayan düzenlemesi bu eğilimin somut bir örneğidir[648]. Ancak veri yerelleşmesi, egemenlik kaygıları ile ekonomik rasyonalite arasında yapısal bir gerilim alanı yaratmaktadır.

Veri yerelleştirme; devletin dijital egemenlik iddiası, fikri mülkiyetin korunması, sanayi casusluğunun önlenmesi ve ekonomik verilerin güvence altına alınması gerekçeleriyle verilerin ülke içinde saklanması ve işlenmesini zorunlu kılarak

---

[647] "Almanya'da kamuya ait veri ağlarına siber saldırı," *Anadolu Ajansı,* 28 Şubat 2018, https://www.aa.com.tr/tr/dunya/almanyada-kamuya-ait-veri-aglarina-siber-saldiri/1076539 (E.T.: 1 Şubat 2026).

[648] European Parliament, Compromise Amendments to the Draft Report on "A New Industrial Strategy for Europe" 15 Ekim 2020, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2020/10-15/CAs_Industrial_Strategy_EN.pdf (E.T.: 1 Şubat 2026), s.9.

devlet kontrolünü artırır[649] ama aynı zamanda küresel veri akışını sınırlandırdığı için ekonomik maliyetler ve hukuki riskler doğurur.

AB, kişisel verilerin korunmasını merkeze alan birey odaklı ve hukuki güvencelerle şekillenmiş ölçülü bir yerelleştirme modeli benimser. Bazı durumlarda verilerin yerelde saklanmasını öngören GDPR'da veri transferlerinde bireyin hak ve özgürlüklerinin korunması önceliklidir. Bu çerçevede, veri yerelleştirme girişimlerini sınırlayarak dijital iç pazarın işleyişini kolaylaştırmayı amaçlayan 2018 tarihli Kişisel Olmayan Verilerin Serbest Akışı Yönetmeliği (2018/1807), kişisel olmayan verilerin herhangi bir üye devlette depolanması zorunluluğu getiren ulusal düzenlemeleri yasaklamaktadır[650]. Avrupa Komisyonu, güvenli sınır ötesi veri akışının ekonomik büyüme için kritik olduğunu vurgulamaktadır[651]. Avrupa Parlementosu ise korumacı veri stratejilerinin açık, ölçülü ve hukuki standartlarla uyumlu olması gerektiğini belirtmiştir[652].

Çin, veri yerelleşmesi açısından ulusal güvenlik gerekçesiyle daha katı ve kapsamlı bir kontrol sistemi kurmuştur. 2016 Siber Güvenlik Yasası ve 2021 Kişisel Bilgilerin Korunması Yasası ile verilerin Çin sınırları içinde işlenmesi ve kritik altyapının ülke içinde işletilmesi zorunlu hale getirmesi Çin'in ulusal güvenlik gerekçeleriyle veri transferlerinde geniş takdir yetkisi kullandığını göstermektedir. 100.000 kişisel veri veya 10.000 hassas veri içeren yurtdışı veri transferlerinde yerelleştirme ve güvenlik denetimi zorunlu hale getirilmiştir. Bu eşikler, Çin'in ulusal güvenlik gerekçesiyle geniş bir takdir yetkisi kullandığını göstermektedir[653]. Buna karşılık, Çin için veri, ekonomik kalkınma ve ulusal güvenlik arasında stratejik bir kavşak oluştururken, bu tür sıkı yerelleştirme

---

[649] Laurens Cerulus, "French cyber czar promotes European tech sovereignty", *Politico*, 2021. https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/ (E.T.: 1 Şubat 2026).
[650] Roberts ve Diğerleri, s.8.
[651] European Commission, Communication from the Commission to the European Parliament and the Council: Two years of application of the General Data Protection Regulation: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition (COM(2020) 264 final), 24 Haziran 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264 (E.T.: 1 Şubat 2026), s.13.
[652] European Parliament, Draft report on a European strategy for data, 2020, https://www.europarl.europa.eu/doceo/document/ITRE-PR-657163_EN.pdf (E.T.: 1 Şubat 2026), s.8.
[653] Dorwart, s.133-135.

politikaları ticari faaliyetlerde belirsizlik ve idari keyfiyet riskleri yaratmaktadır[654]. Devletin veri üzerindeki mutlak kontrolü temel haklar ve küresel hukuki standartlarla çelişmekte; bu durum, Çin'in önde gelen ulusal şirketlerinin rekabet gücünü sınırlandırmakta ve Çin modelinin küresel ölçekte yaygınlaşmasını zorlaştırmaktadır[655]. Facebook, Twitter ve WhatsApp gibi yabancı dijital hizmetleri sınırlandırıp Renren, Weibo ve Weixin gibi yerli alternatifleri destekleyen modeli dijital egemenlik ve küresel ekonomik entegrasyon arasındaki gerilimi somutlaştıran örnektir[656]. Veri yerelleştirme politikalarıyla bağlantılı bu düzenlemeler, stratejik sektörlerde yabancı yazılım kullanımının sınırlandırılması ve verilerin ülke içinde tutulması yönündeki eğilimi güçlendirmektedir.

Dijital egemenlik gerekçesiyle hayata geçirilen veri yerelleştirme uygulamaları, hukuki, siyasi ve ekonomik riskler barındırmaktadır.

Öncelikle; Çin, Hindistan, Rusya, İran ve Vietnam gibi otoriter ülkelerde devlet kontrolünü artıran ve bireysel hakları sınırlayan baskın bir araca dönüşmüştür[657]. Küresel dijital ekonomi ve bilgi toplumunun doğasına ters düşen[658] veri yerelleştirmesi uygulaması, birçok ülkede internetin ülkeselleşerek ulusal sınırlar içinde parçalanmasına (cyber fragmentation) ve özgürlüklerin sınırlanmasına neden olmaktadır[659]. Oysa dijital ekonomi, sınır ötesi veri akışlarına dayanır[660] ve bu akışlar küresel ekonomik büyümenin temel unsurlarındandır. OECD'ye göre sınır aşan veri transferleri, 2020 yılında küresel GSYİH'nın %3,5'ini oluşturan önemli bir ekonomik faaliyet yaratmıştır[661].

Fizikî bağlantı altyapısının egemenlik gerekçesiyle denetlenmesi cazip görünse de hukuk bu noktada sanayi temelli stratejiler için araçsallaştırılmaktadır. Hukuku bir araç

---

[654] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.122, 124.
[655] Dorwart, s.137.
[656] Schneider, *China's Digital Nationalism,* s.68.
[657] Christakis, s.67.
[658] Creemers, "Introduction", s.3.
[659] Freedom House'un 2020 raporu veri yerelleştirmenin özgür internet yapısını tehdit ettiğini vurgular. Adrian Shahbaz, Allie Funk ve Andrea Hackl, "User Privacy or Cyber Sovereignty?", *Freedom House,* Special Report, 2020 https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sover-eignty)
[660] Christakis, s.82.
[661] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector, 2020, https://www.globaldataalliance.org/downloads/GDAeverysector.pdf, (E.T.: 1 Şubat 2026). s.1.

olarak kullanan modern devletin; ekonomik ve sosyal dinamizmin bir engeline ve sınırına dönüştüğü tezini[662] dijital alanda bir daha doğrulamaktadır. Veri yerelleştirme çoğu zaman veriyi korumaktan çok, yerel düzenlemeleri dayatma ve denetimi sağlama amacı taşımakta, bu nedenle baskıcı ve araçsal bir karakter kazanabilmektedir. Nitekim bazı çalışmalar, veri yerelleştirmenin yolsuzluk oranı yüksek ve kurumsal kapasitesi düşük yönetimlerle ilişkili olduğunu öne sürmektedir[663]. Liaropoulos'a göre siber alan, ne tamamen küresel bir kamu malı ne de sınırsız özgürlük alanıdır; klasik kamu mallarından farklı olarak çok aktörlü ve parçalı bir yapı arz eder. Bu durum, veri yerelleştirme politikaları dayalı egemenlik söylemlerinin yeniden değerlendirilmesini iktiza etmektedir[664].

İkinci olarak; veri yerelleştirmesi politikalarının uluslararası hukukla çatışması, DTÖ nezdinde ihtilaflar yaratması ve ticari misillemeleri tetiklemesi ciddi riskler doğurmaktadır. Devletlerin bu politikaları ulusal güvenlik gerekçesiyle meşrulaştırması, çözüm mekanizmalarını tıkamakta ve dijital alandaki stratejik gerilimleri artırmaktadır. Huawei yaptırımları ve ABAD'ın Schrems II kararı çerçevesinde AB-ABD Privacy Shield Anlaşması'nın veri koruma garantilerinin yetersizliği nedeniyle iptali gibi örnekler, yabancı teknoloji şirketlerine yönelik korumacı adımların diplomatik ilişkileri ve ekonomik ortamı zedelediğini göstermektedir.

Misillemeler yalnızca teknoloji alanını değil, diğer analog sektörleri de etkileyerek dijital alanı iş birliğinden uzaklaştırıp çatışmaya açık hâle getirmektedir[665]. Dijital egemenliğini pekiştirmek isteyen devletlerin içe kapanan düzenlemeleri, uluslararası düzeyde ortak norm ve standartların gelişimini engellemekte, küresel iş birliğini zayıflatmaktadır. Tekno-milliyetçi veri politikaları, uluslararası normların

---

[662] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.84.

[663] Vincent Manancourt, "Europe's data grab", *Politico,* 19 Şubat 2020, https://www.politico.eu/article/europe-data-grab-protection-privacy/ (E.T.: 1 Şubat 2026).

[664] Andrew Liaropoulos, "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics", **Journal of Information Warfare,** Vol.15, No..4, (2016), s.16.

[665] Örneğin, Fransa'nın ABD'li teknoloji firmalarına karşı aldığı korumacı önlemler karşısında Trump yönetimi, Fransız şarapları ve lüks markalarına yönelik yaptırımlarla misillemede bulunacağını açıklamıştır. "EU digital protectionism risks damaging ties with the US," *Financial Times,* 2 Ağustos 2020, https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103 (E.T.: 1 Şubat 2026).

oluşumunu zayıflatmakta ve çok taraflı dijital yönetişimi parçalayarak dijital merkantilizmi teşvik etmektedir[666].

Veri yerelleştirmesinin üçüncü ve kritik riski, uzun vadede dijital egemenliği zayıflatabilmesidir. Dijital ekosistemin tüm bileşenlerinde tam bağımsızlık sağlamak teknik ve ekonomik olarak sürdürülebilir değildir; bu yöndeki çabalar yenilik kapasitesini azaltabilir, kaynak israfına yol açabilir, küresel teknolojilere uyumu geciktirebilir ve yabancı yatırımı caydırarak yerel şirketlerin ileri teknolojilere erişimini zorlaştırabilir. Oysa sosyal medya platformları ve veri paylaşım teknolojileri gibi küresel dijital araçlar, eğitimden sağlığa kadar birçok sektörde yerel girişimlerin verimliliğini artırmakta ve bilgiye erişimi kolaylaştırmaktadır[667]. Timmers, dijital egemenliği her şeyi kendin yap şeklinde yorumlamanın yanıltıcı olduğunu vurgulamıştır[668]. Christakis, yeterli veri koruma güvenceleri sağlandığında verinin fiziksel konumunun ikincil önem taşıdığını, aksi hâlde dışlayıcı politikaların maliyetleri artırıp dijital dönüşümü sekteye uğratacağı belirtmiştir[669]. Veri yerelleştirme, teknik açıdan da güvenlik açıkları doğurabilir; zorunlu ulusal yeniden yapılandırmalar güncellemeler sırasında siber saldırılara zemin hazırlayabilir[670].

Veri yerelleştirme, dijital egemenliği güçlendirme iddiasına rağmen ekonomik, teknik ve hukuki maliyetleri nedeniyle dikkatle dengelenmesi gereken korumacı bir politikadır. Ulusal güvenlik ve egemenlik gerekçeleriyle meşrulaştırılan bu yaklaşım, serbest ticaret ve sınır aşan veri akışlarıyla çatışmakta; devletlerin veri üzerindeki kontrol arzusu ile küresel dijital ekonomi arasında derin bir gerilim yaratmaktadır. Yerelleştirme ve millileştirme eğilimleri, küresel dijital ekonominin parçalanma riskini artırmakta; özellikle ABD-Çin eksenli bloklaşma, dijital egemenlik adına atılan adımların küresel bilgi akışını sekteye uğratabileceğini göstermektedir[671].

---

[666] Christakis, s.60.
[667] Demir ve Özbuğday, s.11.
[668] Laurens Cerulus, "Europe's litmus test over cloud computing push", *Politico,* 28 Temmuz 2020, https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/ (E.T.: 1 Şubat 2026).
[669] Christakis, s.62, 63.
[670] Christakis, s.84.
[671] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.131.

B. Düzenleyici Teknik Kuruluşlar

Düzenleyici teknik kuruluşlar, dijital dünyanın işleyişini mümkün kılan küresel teknik standartları belirleyen ve internet ekosisteminin sürdürülebilirliğinde merkezi rol oynayan yapılardır. ICANN, ITU, Internet Architecture Board (IAB) ve World Wide Web Consortium (W3C) gibi çok paydaşlı veya hükümetler arası kurumlar; teknik tasarım, protokol geliştirme ve altyapı yönetimi alanlarında fiilî düzenleyici işlevler üstlenmektedir. Devletlerin küresel dijital teknolojiler üzerindeki doğrudan ve mutlak kontrolünün sınırlı olması, bu kuruluşları dijital yönetişimin vazgeçilmez aktörleri hâline getirmiştir[672].

Bu kurumların yükselişi; deniz altı kabloları gibi yüksek maliyetli küresel altyapıların yönetimi, siber güvenlik tehditlerinin koordinasyonu, tarafsız teknik hakemliğe duyulan ihtiyaç, veri akışlarının düzensizliği ve uluslararası hukuktaki boşluklarla yakından ilişkilidir[673]. Bununla birlikte, bu küresel yapıların yetkileri, onları kuran devletlerin rızasına ve uluslararası anlaşmalara dayanmakta; dolayısıyla devletler egemenliklerini tamamen kaybetmekten ziyade belirli alanlarda paylaşmakta veya sınırlı ölçüde devretmektedir[674].

Teknik standartlar, dijital teknolojilerin küresel ölçekte uyumlu ve birlikte çalışabilir olmasını sağlar[675]. Alan adı sistemi (DNS), İnternet Protokolü (IP) ve 5G gibi standartlar yalnızca teknik istikrar açısından değil, ekonomik rekabet ve jeopolitik güç dengeleri bakımından da hayati öneme sahiptir[676]. Ortak standartların benimsenmesi, otonom araçlardan akıllı şehirlere ve uzaktan sağlık hizmetlerine kadar pek çok alanda

---

[672] Mark Leiser ve Andrew Murray, "The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies", Roger Brownsword, Eloise Scotford ve Karen Yeung (Ed.) **The Oxford Handbook of Law, Regulation and Technology, Oxford Handbooks** içinde (1-35), Oxford: Oxford Academic, 2017, s.5-7.
[673] Tipper ve Krishnamurthy, s.2-3.
[674] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.131.
[675] Julia Voo ve Rogier J.E.H. Creemers "China's role in digital standards for emerging technologies: impacts on the Netherlands and Europe", Leiden: **Leiden Asia Centre** 2017, s.3. Bu tür standartların oluşturulmasında merkezi bir otorite bulunmamaktadır. Günümüzde bu alanda faaliyet gösteren 200'den fazla standart geliştirme organizasyonu mevcuttur.
[676] Voo ve Creemers, s.20.

altyapı yatırımlarının verimliliğini artırmakta[677] standartlaşmanın başarısız olması ise internetin teknik parçalanması riskini doğurmaktadır. Standart belirleme süreçleri teknik gerekçelerle yürütülüyor gibi görünse de ABD, Çin ve AB arasındaki rekabetin gösterdiği üzere bu alan yoğun siyasi ve ekonomik güç mücadelelerine sahnedir. Standartlara patent dâhil edebilmek, lisans gelirleri ve pazar hâkimiyeti bakımından stratejik üstünlük sağlamaktadır[678].

Düzenleyici teknik kuruluşlar, çoğunlukla devletleri, özel sektörü ve teknik toplulukları bir araya getiren çok paydaşlı ve çok katmanlı yapılardır. Karar alma süreçleri çoğu zaman herhangi bir devletin doğrudan denetimi dışında, iç prosedürler aracılığıyla yürütülür. Bu durum, küresel bir idareye benzer yeni bir modelin doğmasına ve dijital yönetişimde devlet dışı aktörlerin güç kazandığı çok merkezli (polycentric) bir egemenlik yapısının ortaya çıkmasına yol açmıştır[679]. İnternetin liberteryan döneminde gelişen çok paydaşlı model, bu kuruluşlarda fiilî norm hâline gelmiştir[680].

Bu yapının en çarpıcı örneği, uluslararası hukukla kurulmamış olmasına rağmen küresel alan adı sistemini yöneten ICANN'dir. 1998 yılında ABD'de kurulan ICANN, alan adları, IP adresleri ve kök sunucular gibi internetin temel teknik bileşenlerini yönetmekte[681] hükümetlere yalnızca danışma rolü tanıyan özel sektör ve teknik uzmanların hâkim olduğu neoliberal bir yönetişim modelini temsil etmektedir. Bu yapı, internetin teknik altyapısının devletler arası bir örgüt yerine piyasa temelli ve çok paydaşlı bir mekanizma aracılığıyla yönetilmesini sağlamış[682] özellikle ITU'nun etkisini sınırlayan bir alternatif oluşturmuştur[683].

---

[677] Kristina Irion, "Separated Together: The International Telecommunications Union and Civil Society", **International Journal of Communications Law and Policy,** Vol.13, 2009, s.5

[678] Voo ve Creemers, s.4-5.

[679] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.131.

[680] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.113.

[681] Wolfgang Kleinwacher, "Beyond ICANN Vs ITU? How WSIS tries to enter the new territory of Internet governance", **The International Journal for Communication Studies,** Vol.66, No.3-4, (2004), s.233.

[682] Internet Corporation for Assigned Names and Numbers (ICANN) ve U.S. Department of Commerce, "Memorandum of Understanding Between the U.S. Department of Commerce and ICANN," 31 Aralık 1999, https://www.icann.org/en/governance/documents/memorandum-of-understanding-between-the-us-department-of-commerce-and-icann-31-12-1999-en (E.T.: 1 Şubat 2026), Madde II.

[683] Negro, s.157-158.

Günümüzde, çok paydaşlı model, internet yönetişiminde fiili norm haline gelmiş, bu yapının korunması ABD'nin siber stratejilerinin temel unsurlarından biri olmuştur. ABD, bu modelin devlet merkezli alternatif yönetişim anlayışlarına karşı üstünlüğünü savunmaktadır[684]. Aynı zamanda dijital çağda çok merkezli bir egemenlik yapısının, devlet dışı aktörlerin "yumuşak" ama etkili bir egemenlik türünün ortaya çıktığını göstermektedir[685].

Buna karşılık ITU, hükümetler arası niteliğiyle devlet merkezli bir modeli temsil etmektedir. Birleşmiş Milletler'in uzman kuruluşu olan ITU, uluslararası telekomünikasyon alanında bağlayıcı normlar üretmekte; özel sektörün katılımını kabul etmekle birlikte nihai karar yetkisini üye devletlerde tutmaktadır[686]. Kamu tekellerinden piyasa temelli yapılara geçiş, ITU'nun kurumsal yapısını da etkilemiş; özel sektörün karar alma süreçlerine daha aktif katılımını mümkün kılacak reformlar gündeme gelmiştir. Yapısı gereği yalnızca devletlerden değil, devlet dışı aktörlerden de oluşan tek BM kuruluşudur[687].

ITU, özellikle Çin'in savunduğu devlet egemenliğini önceleyen internet anlayışıyla uyumludur ve ITU'yu hem piyasa aktörlerini içeren hem de devlet egemenliğini koruyan hibrit bir yönetişim modeli hâline getirmektedir[688].

Sonuç olarak düzenleyici teknik kuruluşlar, teknik standartlar ve altyapı yönetimi üzerinden işleyen, devlet egemenliğini tamamen ortadan kaldırmayan fakat onu dönüştüren yeni bir dijital idare mimarisinin merkezinde yer almaktadır. Bu kuruluşlar, dijital çağda egemenliğin yalnızca hukuki ve askerî değil, teknik ve normatif araçlar üzerinden de kurulduğunu açıkça göstermektedir.

---

[684] Zhang ve Creemers, s.10.
[685] Timmers, *"Sovereignty in the Digital Age",* s.575.
[686] International Telecommunication Union (ITU), "Our members," https://www.itu.int/hub/membership/our-members/ , (E.T.: 1 Şubat 2026).
[687] Irion, *"Separated Together: The International Telecommunications Union and Civil Society",* s.2-4.
[688] Negro, s.154.

C. Büyük Teknoloji (Big Tech) Şirketleri

Dijitalleşmenin ürettiği başat aktörler olarak Big Tech şirketleri; platform ekonomisi ve gözetim kapitalizmi aracılığıyla dijital altyapıdan veri akışına, kullanıcı davranışlarından kamuoyu oluşumuna ve devletlerin düzenleme kapasitesine kadar uzanan merkezî bir iktidar ağı kurmuştur. Veri işleme teknolojilerindeki ilerlemeler sayesinde, bireylerin davranışları benzeri görülmemiş ölçekte izlenebilmekte, ilişkilendirilebilmekte ve öngörülebilir hâle getirilmektedir. Bu süreç, yasal çerçevenin izin verdiği ölçüde yalnızca devletler tarafından değil, özel sektör tarafından da yürütülmektedir[689].

Big Tech; dijital dünyanın teknik tasarımını, altyapısını, veri ekonomisini ve davranışsal yönlendirme mekanizmalarını kontrol eden küresel platform-imparatorluklarıdır. 5651 sayılı Kanun'un tanımlar maddesinde yer alan ve internet üzerinden görsel, işitsel veya yazılı içeriklerin oluşturulup paylaşılmasını sağlayan gerçek ve tüzel kişiler olarak tanımlanan sosyal ağ sağlayıcıları(platformlar) bu şirketlerin ilk akla gelenleridir. GAFAM (Google, Apple, Meta, Amazon, Microsoft) başta olmak üzere bu şirketler, üretimi düşük maliyetli küresel taşeron ağlarına yayarken; fikrî mülkiyet, patentler[690] ve veri tekelleri üzerinden değeri merkezde toplamaktadır. Bu yapı, devletleri teknik, ekonomik ve hukuki düzeylerde kendilerine bağımlı hâle getirerek dijital egemenlik üzerinde ciddi bir baskı üretmektedir[691].

Big Tech şirketleri veri temelli organizasyon yapıları üzerinde yükselir. İçerik filtreleme, kaldırma, askıya alma ve görünürlük düzenlemeleri gibi veri moderasyonu

---

[689] Erol, s.49.

[690] Standartlara Esaslı Patentler (SEP), teknik standartların işleyişi için vazgeçilmez olan patentlerdir. Standartlar; güvenlik, birlikte çalışabilirlik ve uyumluluk amacıyla teknik ve kalite kriterleri belirler. Bir ürün, belirli bir patenti ihlal etmeden üretilemiyorsa bu patent "esaslı" kabul edilir. Bir patentin SEP sayılabilmesi için, standart belirleyici kuruluşlarca tanınması ve standardın uygulanması açısından kaçınılmaz bir teknolojiyi kapsaması gerekir. Magna Law Legal & Consulting, "Standarda Esas Patentler ve FRAND Şartları – Türkiye'den SEP'e İlişkin İlk Karar: Vestel-Philips Kararı," 10 Şubat 2022, https://www.lexology.com/library/detail.aspx?g=0337fc92-fe36-4fc3-b59f-11338a9a5205 (E.T.: 1 Şubat 2026).

[691] Standart temel patentlerin bu şirketlerin elinde bulunması, ulus-devletlerin teknolojik gelişmeleri yönlendirme kapasitesini sınırlayarak, söz konusu şirketleri dijital alanın fiilî düzenleyicileri konumuna getirmektedir. Leiser ve Murray, s.5-7.

faaliyetleri yoluyla dijital alanın normatif yapısını fiilen belirlerler[692]. Teknik kuruluşlar internetin sürdürülebilirliğini sağlarken, Big Tech şirketleri altyapıyı fiilen kurup işletmektedir. Uydu tabanlı internet hizmetleri (örneğin Starlink) bu şirketlerin fiziksel altyapı bağımlılığını da aşarak dijital alan üzerindeki fiilî hâkimiyetini genişlettiğini göstermektedir.

Varoufakis'e göre Big Tech'in küresel gücü yalnızca teknik sermayeden değil, emeği örgütleme biçiminden de kaynaklanır. Üretim düşük maliyetli ülkelerde yoğunlaşırken, katma değer fikrî mülkiyet ve marka üzerinden merkezde toplanır. Dijital platformların işleyişi; uzaktan, güvencesiz ve görünmez dijital emekçiler tarafından sağlanmakta; içerik moderatörleri bu yeni emek rejiminin en kırılgan halkasını oluşturmaktadır[693].

Zuboff'un tanımladığı gözetim kapitalizmi çerçevesinde kullanıcı verileri, davranışsal öngörü ürünlerine dönüştürülerek reklam ve manipülasyon piyasalarında pazarlanır. Bu rejimde insanlar müşteri değil, davranışsal hammadde sağlayıcılarıdır. Kullanıcılar farkında olmaksızın dijital davranışlarıyla ücretsiz emek sunmakta; insan deneyimi mülksüzleştirilerek ekonomik girdiye indirgenmektedir[694].

Castells'in işaret ettiği üzere, kapitalizm kâr maksimizasyonuna, devlet ise iktidar ve denetimin sürekliliğine dayanır[695]. Devletler daha çok kontrol; şirketler kâr maksimizasyonu ile ilgilenir[696]. Dijital çağda bu iki mantık iç içe geçmiş; Big Tech şirketleri, kamusal hizmet sağlıyor görünmelerine rağmen merkezî, kâr odaklı ve hatta kimi yönleriyle devlet benzeri planlama teknikleri kullanan yapılara dönüşmüştür[697]. Dijital alanın ticarîleşmesi, toplumsal fayda ile şirket kârı arasındaki sınırları belirsizleştirmiştir. Dijital teknolojilerin kolaylık sağlaması, bu faydanın şirket çıkarlarıyla uyumlu olduğu ölçüde mümkündür. Verinin işlenmesi ve kullanılmasıyla

---

[692] Işık, s.20.
[693] Varoufakis, *Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,* s.107.
[694] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.609-612.
[695] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.19.
[696] Rogier J.E.H. Creemers, "Uneven coverage and blank spaces: bringing the state back in", Asiascape: **Digital Asia,** Leiden, Vol.10, No.1-2, 2023, s.138.
[697] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.456; Lehdonvirta, s.210.

ilgili teknik açıdan farklılaşan şirket işleyişleri, devletin müdahalesinden önce geliştirilmiş ve ticari çıkarlarla şekillenmiştir[698].

Telekomünikasyon, ulaşım ve uluslararası finans alanlarında yaşanan gelişmeler neticesinde ekonomik ilişkilerin küresel ölçekte yoğunlaşmasında bilgi ve iletişim teknolojilerinin rolü inkâr edilemez niteliktedir[699]. Sanal alanlar fizikî altyapılarla maddi dünyaya sabitlenmiştir ve bu altyapıların kontrolü büyük ölçüde kapitalist işletmelerin elindedir[700].

Klasik piyasa anlayışını kökten dönüştürerek insan deneyimini ham maddeye dönüştüren, öngörü ve davranış tahmini üzerine kurulu bu yeni ekonomik rejimde şirketler, özgürlük adı altında düzenlemelerden kaçmak ister ve sahip oldukları bilgi ve rekabet avantajını kendi gücünü büyütmek için kullanırlar[701]. Fakat bilgi tek taraflı tekelleşmiş şirketlerde birikmekte; toplumsal öğrenme süreçleri parçalanmakta, kamu düzeni yerine özel kâr düzeni işlemektedir.

Başlangıçta özgürleştirici araçlar olarak sunulan bu teknolojiler, zamanla ifade özgürlüğü, mahremiyet ve demokratik süreçler üzerinde tartışmalı bir iktidar formuna evrilmiştir[702]. Dijital ekosistem, özgürlük vaadine rağmen yoğun bir şekilde merkezileşmiş[703] ve gözetimci bir iletişim altyapısı hâline gelmiştir. Meta, Google, Amazon ve Apple gibi şirketler; sosyal ağlar, arama motorları, reklamcılık, bulut hizmetleri, mobil donanım ve yazılım alanlarında küresel ölçekte tekeldir.

Ekonomik düzlemde Big Tech; vergi cennetleri, transfer fiyatlandırması ve karmaşık şirket ağları yoluyla ulusal vergi sistemlerini aşındırırken, devletler yatırım ve teknoloji bağımlılığı nedeniyle kırılgan bir dengeye sıkışmaktadır. Şirketlerin farklı rejimlere uyum sağlayabilen çoklu stratejileri (Çin'de sansür, AB'de GDPR uyumu,

---

[698] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.3.
[699] Akdenizli, s.36.
[700] Schneider, *China's Digital Nationalism,* s.14.
[701] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.607-608.
[702] Coroado, s.4-5.
[703] Balázs Bodó ve Diğerleri, *"Tackling the Algorithmic Control Crisis: the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents"*, s.138.

ABD'de gevşek düzenlemelerden yararlanma) onlara fiilî devletler üstü bir manevra kabiliyeti kazandırmaktadır[704].

Big Tech ile devletler arasındaki ilişki çift yönlüdür: Şirketler bir yandan devletin dijital denetimini zayıflatırken, diğer yandan güvenlik ve gözetim alanlarında iş birliği yapmaktadır. AB'nin GDPR, DSA, DMA gibi düzenlemeleri Big Tech'i sınırlama girişiminde bulunsa da Big Tech; lobi, kurumsal siyasi faaliyet stratejileri[705] ve bilgi asimetrisi ile pazar dışı ortamda[706] bu baskıyı yumuşatarak ve politikaları etkilemeye çalışırlar[707]. Bu ilişki, makro düzeydeki siyasi rejimlerin, bazı orta (mezo) düzey şirketlerini diğerlerinin aleyhine desteklemesine ve güçlü işletmelerin baskısının makro düzeydeki yasal veri çerçevelerini etkilemesine uzanmaktadır[708].

Devletle güvenlik iş birliği açısından, dijital alandaki güçlerini korumak amacıyla gerektiğinde sansür ya da denetime destek verirler[709]. Snowden belgelerinin ortaya koyduğu gibi NSA'nın PRISM programı ve FBI ile yapılan veri paylaşımı toplantıları, Big Tech ile devlet arasında erişime izin veren gizli ve güçlü bir gözetim ortaklığı olduğunu kanıtlamaktadır[710]. Çinli Baidu, Sina Weibo ve Renren gibi platformlar da yapısal olarak Batılı şirketlerle benzer kapitalist mantıkla çalışmakta; tümü, devlete, finans piyasalarına ve reklam verenlere bağımlı olarak faaliyet göstermektedir[711]. Bu ortaklık, dijital alanın özgürlük vaadini merkezî bir gözetim rejimine dönüştürmüş; Big Tech'i kitlesel gözetimin asli taşıyıcısı hâline getirmiştir.

---

[704] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.25.

[705] Amy J. Hillman ve Michael. A. Hitt, "Corporate Political Strategy Formulation: A Model of Approach, Participation, and Strategy Decisions". **Academy of Management Review,** Vol.24, No.4, 1999, s.833-835.

[706] David. P. Baron, "Integrated Strategy: Market and Nonmarket Components", **California Management Review,** Vol.37, No.2, 1995, s.48.

[707] Eugenie Coche ve Ans Kolk, "When digitalization meets regulation across borders: An explainer with actionable insights". **AIB Insights,** Vol.24, No.3, 2024, s.1-7; Václav Ocelík, Ans Kolk ve Kristina Irion, "Shifting battlegrounds: Corporate Political Activity in the General Data Protection Regulation", **Business & Society,** s.2.

[708] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.3.

[709] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.238.

[710] Aust ve Ammann, s.167-169.

[711] Christian. Fuchs, "Baidu, Weibo and Renren: the global political economy of social media in China", **Asian Journal of Communication,** Vol.26, No.1, 2015, s.21-23.

Algoritmalar, Big Tech iktidarının temel egemenlik aracına dönüşmüş; kendilerinin de kabul ettiği üzere[712] bilgi akışı, görünürlük ve kamusal tartışmanın çerçevesi şeffaf olmayan teknik kararlarla belirlenir hâle gelmiştir[713]. Demokratik meşruiyetten yoksun bu güç, teknik ve ekonomik kapasiteye dayanarak küresel ölçekte normatif dayatmalarda bulunabilmektedir[714].

Sonuç olarak Big Tech iktidarı; demokratik meşruiyet taşımayan, devletlerin mali ve hukuki kapasitesini aşındıran, emeği görünmezleştiren ve kullanıcıyı veri hammaddesine indirgeyen bir tahakküm düzeni üretmektedir. Demokrasi; eşitlik, insan hakları ve kamusal meşruiyet üzerine kurulu modern düşüncenin kazandırdığı bir değerler kümesi[715] Big Tech merkezli dijital güç ilişkileri tarafından sistematik biçimde aşındırılmaktadır. Bu nedenle Big Tech, siyasal temelden yoksun, yalnızca teknik ve ekonomik güce dayanan, asalak bir iktidar biçimi olarak nitelendirilebilir[716].

D. Kullanıcılar

Dijital bilgi toplumunda bilginin taşıyıcısı bireydir; zira bilgi, ancak insan zihninde anlam kazanır[717]. Bu nedenle dijital çağda kullanıcı, yalnızca içerik tüketen pasif bir unsur değil; veri üreten, içeriği dolaşıma sokan ve dijital ekosistemi fiilen etkileyen aktif bir aktördür[718]. Dijitalleşme, medya üretimini merkezsizleştirerek herkesin herhangi bir editöryel süzgeçten geçmeden içerik üretebildiği katılımcı bir iletişim ortamı yaratmıştır[719].

---

[712] Yanlış bilgilerin negatif etkileri nedeniyle Facebook ve Twitter başta olmak üzere sosyal medya platformları büyük baskı altında kalmış; bu etkileri azaltmak için etiketleme, uyarı ekleme, hesap dondurma, içerik kaldırma gibi farklı türde politikalar denemeye başlamışlardır. Andı, s.2.

[713] All Tech Is Human, AI and Human Rights: Building a Tech Future Aligned With the Public Interest, 2022, https://alltechishuman.org/ai-human-rights-report (14 Aralık 2024), s.24; Serkan Bulut, s.91-92.

[714] Hatipoğlu Aydın, s.102-103.

[715] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.81.

[716] Hardt ve Negri, *İmparatorluk,* s.86.

[717] Drucker, s.292.

[718] Florian A. Schneider, "The Cultural Governance of Mass Media in Contemporary China", Michael Keane (Ed.), **The Handbook of Cultural and Creative Industries in China: Handbook of Research on Contemporary China** içinde (189-206), Cheltenham & Northampton (MA): Edward Elgar. 2016, s.204; Hatipoğlu Aydın, s.90-91.

[719] Sosyal medyada yanlış haberler doğrulardan üç kat daha hızlı yayılmaktadır. Dijital okuryazarlığı ve analitik düşünme düzeyi düşük bireyler bu içeriklere daha kolay inanır. Andı, s.1.

Kullanıcının dijital aktör olarak konumlanması, kişisel veriler üzerindeki tasarruf ve paylaşım kararlarının da bireye ait olmasını zorunlu kılar. Bu çerçevede GDPR ve tasarımda gizlilik[720] ilkesi, kullanıcıların veri üzerindeki denetimini güçlendirmeyi amaçlar[721]. World-Wide-Web'nin kurucusu Tim Berners-Lee'nin verinin bireyde kalması gerektiğine ilişkin yaklaşımı[722] ile kişisel veri üzerinde sosyal ve hukuki hâkimiyetin bireye ait olması gerektiği yönündeki görüşler[723] dijital özneliğin temel koşulunun veri üzerindeki kontrol olduğunu göstermektedir.

Alman anayasa hukukunda geliştirilen "kişisel veri üzerinde kaderini belirleme hakkı", bireyin verilerinin işlenmesi süreçlerinde yüksek düzeyde denetim sahibi olmasını gerekli kılar. Bu bağlamda veri koruması, bireyin kendi yaşamına ilişkin kararları özgürce verebilmesini sağlayan kurucu bir meta-değer niteliğindedir[724].

Teknolojik gelişmeler, bireyin dijital alandaki konumunu güçlendiren merkezsiz mimariler de üretmektedir. Dağıtık ağ yapıları, şifreleme, veri minimizasyonu ve kendinden egemen kimlik[725] (self-sovereign identity) çözümleri; bireyin verilerini

---

[720] GDPR, m. 25: bkz. Avrupa Birliği Genel Veri Koruma Tüzüğü (Regulation (EU) 2016/679) Unofficial Turkish Translation, 27 Nisan 2016, https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf (E.T.: 1 Şubat 2026).
KVKK doğrudan düzenlenmemekle birlikte dolaylı olarak m. 12'de yer almaktadır.

[721] Roberts ve Diğerleri, s.8; Fabiano, s.272.

[722] Christakis, s.17.

[723] Osman Gökhan Antalya, s.1211-1212.

[724] Oostveen ve Irion, s.3,6.

[725] 2012'de The Moxy Tongue blogunda ortaya atılan 'kendinden egemen kimlik' kavramı, bireyin kimliğini devlet aracılığıyla tanımlamaya karşı çıkarak, kimliğin bireyin denetiminde olması gerektiğini savunur. "What is 'Sovereign Source Authority'?" *The Moxy Tongue,* (15 Şubat 2012), https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html (E.T.: 1 Şubat 2026). Kendinden egemen kimlik (self-sovereign identity) uygulamaları, bireylerin merkezi bir konuma yerleşerek dijital kimliklerini devlet ya da özel aktörlerden bağımsız biçimde yönetmelerini mümkün kılan ademimerkeziyetçi bir sistem önerir. Emily Fry ve Elizabeth M. Renieris, "SSI? What we really need is full data portability," *Women in Identity*, 31 Mart 2020, https://www.womeninidentity.org/articles/ssi-what-we-really-need-is-full-data-portability (E.T.: 1 Şubat 2026).

paylaşma ve yönetme süreçlerinde daha fazla inisiyatif kullanmasını hedefler[726]. Bu teknolojiler, devlet ve şirket merkezli veri rejimlerine alternatifler sunmaktadır[727].

Buna karşın kullanıcının tamamen özerk ve rasyonel bir dijital aktör olarak idealize edilmesi eleştirilmiştir. Neoliberal dönüşüm, bireyi yurttaş olmaktan ziyade tüketiciye indirger; siyaset ve iletişim alanı piyasa mantığıyla yeniden şekillenir. Dijital aracısızlaşma, yüzeyde bireye kontrol hissi verse de fiilen karar alma süreçlerini platformlara ve algoritmalara devreder. Böylece kullanıcı, manipülasyona açık bir veri profiline indirgenir[728].

Sunstein'ın belirttiği üzere, tüketici egemenliği anlayışı, siyasal alanı da dönüştürerek demokrasiyi kamusal akıl yürütmeden uzaklaştırır; tercihlerin pazarlama ve yönlendirme teknikleriyle belirlendiği bir yapıya sürükler. Filtre balonları ve yankı odaları, bilgi dolaşımını daraltarak kamusal alan üzerinde yapısal bir erozyon yaratır[729]. Dijital teknolojilerin özgürleştirici potansiyeli, kullanıcıların yalnızca doğrulanmış bilgilere eriştiği, farklı görüşleri ifade etmekten çekindiği ortamlarda zayıflamaktadır. Diğer dijital aktörlerden gelen müdahaleler, iletişim ağlarındaki çeşitliliği azaltmakta ve bireyin dijital alandaki yetkinliğini sınırlayabilmektedir[730].

Zuboff'a göre veri korumasını bireyin sorumluluğuna indirgemek bir yanılsamadır. Gözetim kapitalizmi karşısında birey yapısal olarak güçsüzdür; algoritmik karar süreçlerine erişim ve itiraz imkânı fiilen yoktur. Bu nedenle etkin veri koruması bireysel değil, kolektif ve kurumsal mekanizmalarla mümkündür: güçlü düzenlemeler, şeffaflık ve algoritmik denetim zorunludur[731].

---

[726] Shapiro, s.15-17; Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.3, 17; Heleen Janssen, Jennifer Cobbe, Chris Norval, Jatinder Singh, Decentralized data processing: personal data stores and the GDPR, International Data Privacy Law, Volume 10, Issue 4, November 2020, Pages 356–384, https://doi.org/10.1093/idpl/ipaa016, s. 357-359.

[727] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.19.

[728] Shapiro, s.18-19, 56.

[729] Sunstein, s.44.

[730] Schneider, *"The Cultural Governance of Mass Media in Contemporary China",* s.204.

[731] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.591-595.

Öte yandan, "bireysel egemenlik" kavramı teorik olarak cazip olsa da egemenlik devletlere özgü bir yetkidir. Birey açısından doğru kavram, veri özerkliğidir. Dağıtık teknolojiler bireyin dijital alandaki konumunu güçlendirebilir; ancak bu durum bireysel egemenlik değil, bireyin kendi kaderini tayin hakkının dijital uzantısı olarak değerlendirilmelidir.

Sonuç olarak kullanıcı, dijital alanda çift yönlü bir aktördür: Güçlüdür; çünkü dağıtık teknolojiler ve gizlilik araçları veri üzerinde daha fazla inisiyatif sağlar. Zayıftır; çünkü platform egemenliği, algoritmik yönlendirme ve bilgi asimetrisi bireyi edilgen bir veri kaynağına dönüştürür.

E. Sivil Toplum Örgütleri

Dijital alandaki önemli aktörlerden biri, küreselleşme ile bilgi ve iletişim teknolojilerinin sağladığı imkânlar sayesinde güç kazanan hükümet dışı sivil toplum örgütleridir[732]. Devlet otoritesi dışında konumlanan sivil toplum, ulusal ve uluslararası karar alma süreçlerinde hükümetlerin dikkate almak zorunda olduğu bir etki alanı oluşturmakta; bu yönüyle klasik egemenlik anlayışı açısından potansiyel bir dengeleyici unsur olarak ortaya çıkmaktadır[733].

Dijitalleşme, sivil toplumu yalnızca görünür kılmakla kalmamış; onu internet yönetişimi ve teknoloji politikaları alanında fiilen etkili bir aktöre dönüştürmüştür[734]. Çevrimiçi kampanyalar, farkındalık çalışmaları ve dijital aktivizm, sivil toplum örgütlerinin siyasal alana müdahale kapasitesini artırmış; bu aktörler hükümetler ve uluslararası kuruluşlarla eş zamanlı etki yaratabilen bir konuma gelmiştir. Dijital araçların sağladığı hız, erişim ve ölçek, sivil toplumun kamusal alandaki etkisini geleneksel yöntemlerin ötesine taşımaktadır.

---

[732] Akdenizli, s.38.
[733] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.132-134.
[734] Creemers, *"China's Conception of Cyber Sovereignty: Rhetoric and Realization",* s.113.

Sivil toplumun internet yönetişimindeki rolü, uluslararası belgelerle de tanınmıştır. BM Dünya Bilgi Zirvesi (WSIS) Prensipler Bildirgesi[735] sivil toplumu insan odaklı bilgi toplumunun inşasında hükümetler ve özel sektörle birlikte temel bir paydaş olarak kabul etmektedir[736]. İnternet Yönetişimi Çalışma Grubu (WGIG) raporu[737] ise sivil toplumun; uzmanlık, temsil ve savunuculuk kapasitesi sayesinde kamu yararını gözeten politikaların oluşumuna katkı sunduğunu ve karar alma süreçlerine katılım sağladığını vurgular[738].

Açık kaynak hareketleri, özgür internet savunuculuğu, gözetim karşıtı inisiyatifler ve teknoloji politikalarına yönelik müdahaleler, sivil toplumun dijital alandaki başlıca faaliyet alanlarıdır. Cypherpunk hareketi, Privacy International, Open Rights Group ve AlgorithmWatch gibi oluşumlar; şifreleme, mahremiyet, algoritmik şeffaflık ve adalet gibi konularda kamuoyu oluşturarak hem devletlerin hem de teknoloji şirketlerinin uygulamalarını denetleyen bir işlev üstlenmektedir[739].

Dijitalleşme aynı zamanda ulus-devlet merkezli toplumsal düzenin yanında, dijital iletişim yoluyla şekillenen yeni bir etik ve siyasal sorumluluk alanı yaratmıştır. Kullanıcı katılımına dayalı platform yönetişimi ve kolektif denetim mekanizmaları, sivil toplumun bu yeni alandaki rolünü pekiştirmektedir[740]. Sivil toplumun güçlendirilmesi;

---

[735] Dünya Bilgi Zirvesi (World Summit on the Information Society, WSIS) Prensipler Bildirgesi, BM öncülüğünde düzenlenen bir zirve kapsamında kabul edilmiştir. WSIS, 2003'te Cenevre'de ve 2005'te Tunus'ta olmak üzere iki aşamada gerçekleştirilmiştir. Zirve, Birleşmiş Milletler Genel Sekreterliği gözetiminde, bilgi toplumu ile ilgili global vizyon ve ilkeleri belirlemek amacıyla ITU liderliğinde düzenlenmiştir.

[736] International Telecommunication Union (ITU), "WSIS: Declaration of Principles: Building the Information Society: a global challenge in the new Millennium," 12 Aralık 2003, https://www.itu.int/net/wsis/docs/geneva/official/dop.html (E.T.: 1 Şubat 2026), par.20.

[737] İnternet Yönetişimi Çalışma Grubu (Working Group on Internet Governance, WGIG), BM Dünya Bilgi Zirvesi (WSIS) süreci kapsamında 2004 yılında kurulmuştur. Amacı internet yönetişiminin küresel düzeyde nasıl yapılması gerektiğini araştırmak ve öneriler geliştirmektir. Çalışma grubu; hükümet temsilcileri, akademisyenler, özel sektör, teknik topluluklar ve sivil toplumdan oluşan çok paydaşlı bir yapıya sahiptir. WSIS Raporu'nun doğrudan sonucu olarak, 2006'da BM çatısı altında her yıl toplanan Internet Governance Forum kurulmuştur. Working Group on Internet Governance (WGIG), Report of the Working Group on Internet Governance, Haziran 2005, https://www.wgig.org/docs/WGIGREPORT.pdf (E.T.: 1 Şubat 2026).

[738] Working Group on Internet Governance., par.32.

[739] Leiser ve Murray, s.5-7.

[740] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.236.

internet yönetişimi süreçlerinde daha kapsayıcı, adil ve insan haklarıyla uyumlu sonuçlar doğurma potansiyeline sahiptir[741].

Sonuç olarak sivil toplum, dijital alanda kolektif eylemi örgütleyen, kamu yararını savunan ve devlet ile Big Tech kaynaklı algoritmik güce karşı dengeleyici bir rol üstlenen temel bir dijital aktör hâline gelmiştir.

[741] Irion, *"Separated Together: The International Telecommunications Union and Civil Society",* s.10.

İKİNCİ BÖLÜM

MODERNİTEDEN POST MODERNİTEYE: DEVLETİN KLASİK UNSURLARININ DÖNÜŞÜMÜ VE EGEMENLİĞİN ETKİ ALANININ YENİDEN DEĞERLENDİRİLMESİ

I. DÖNÜŞÜMÜN DİNAMİĞİ: TARTIŞMAYI MÜMKÜN KILAN ETKENLER

Savaşların çoğu zaman ilan edilmeden başlatılması gibi, dijitalleşme de modern devletin egemenlik tasarımını hem aşındıran hem de onu yeniden inşa etmeye zorlayan çok katmanlı bir dönüşüm yaratmıştır. Bu dönüşüm, yalnızca teknoloji kullanımındaki niceliksel artışla açıklanamaz; ülkesellik, hukukî otorite, siyasal meşruiyet ve kamusal düzen gibi modern egemenliğin kurucu unsurlarını doğrudan tartışmaya açmaktadır.

Doehring'in de vurguladığı üzere, günümüzde ortaya çıkan bu yeni gelişmeler, devleti yalnızca iç yapısı üzerinden ele alarak açıklamayı yetersiz kılmaktadır[742]. Dijital ağların sınır aşan niteliği, kod ve algoritmaların fiilî norm üretme kapasitesi ile platform aktörlerinin siyasal ve ekonomik güçle bütünleşmesi, iktidarı tekil bir merkezden ziyade ilişkisel, dağınık ve çok aktörlü bir alana dönüştürmektedir. Bu çerçevede dijital dönüşümün dinamiği, egemenlik tartışmasını mümkün kılan beş temel etkende somutlaşmaktadır.

Birinci etken, klasik egemenlik anlayışının sarsılması ve yeniden kurulum ihtiyacıdır. Modern egemenlik kuramı; güvenlik sağlama, yasa koyma ve meşruiyet üretme işlevlerini merkezî bir otorite etrafında toplayan bir modele dayanır. Hukuksal bir kavram olarak egemenliğin temel amacı, ulus-devletin bütünleşmesini sağlayacak merkezî otoriteyi güçlendirmek için aklî ve siyasal bir zemin oluşturmaktı[743]. Bodin'in egemenliğin bölünmezliği vurgusu, Hobbes'un mutlak otorite anlayışı ve Rousseau'nun genel irade kavramsallaştırması, ulus-devletin merkezileştirici kurumsallaşmasına teorik

[742] Doehring, s.1.
[743] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.55.

dayanak sağlamıştır[744]. Merkezileşen devlet tekelleştirdiği güçlerle donanmaktayken aynı zamanda bu durum merkezileştirmeyi daha da güçlendiren simbiyotik bir ilişki yaratmıştır.

Bu model, feodal düzenin tasfiyesiyle birlikte modern ulus-devletin yükselişini mümkün kılmış[745] summa potestas[746] çerçevesinde devlet, bürokrasi, maliye, diplomasi ve ordu gibi aygıtlar aracılığıyla kamusal alanı, özel alanı ve ülke içindeki uluslararası faaliyetleri düzenleyebilen kapsamlı bir hukuk düzeni kurabilmiştir[747]. Okullar ve kışlalı ordular üzerinden ortak dilin yerleşmesi, yurttaşlık sorumluluklarının öğretilmesi ve ulusal aidiyetin inşası, bu merkezî egemenlik modelinin toplumsal dayanaklarını oluşturmuştur[748]. Liberal ve sosyal devlet biçimleri de bu çekirdeği ortadan kaldırmamış, yalnızca devletin düzenleyici işlevlerini yeni araçlarla yeniden örgütlemiştir[749].

Ancak küresel sermaye hareketleri, dijital altyapılar ve sınır aşan veri akışları, ulus-devletin mutlak egemenlik kapasitesini giderek sınırlamaktadır. Devletler, artık mutlak egemen aktörler olmaktan ziyade, daha geniş ve çok aktörlü ağlar içinde göreli güç kullanan aktörlere dönüşmektedir. Böylece tek merkez-tek otorite varsayımına dayanan klasik egemenlik anlayışı, dijital çağın çoğul ve ilişkisel güç yapıları karşısında açıklayıcılığını yitirmektedir[750].

Dijitalleşme ve küreselleşmeyle birlikte siyasal düzen, devletin egemenliğinin hem içeriden hem dışarıdan aşındığı bir eşiğe gelmiştir[751]. Günümüz egemenliği ne Bodin'in bölünmezlik kurgusunda ne Hobbes'un mutlak Leviathan'ında ne de Rousseau'nun halk iradesinde tam karşılığını bulabilmektedir. Güç, artık yalnızca devlet

---

[744] Timmers, *"Sovereignty in the Digital Age",* s.575.

[745] Bodin'in merkezileşmiş devlet anlayışı ile bürokratik-askerî yapının güçlenmesi, feodal otoriteleri tasfiye ederek modern ulus-devletin kurumsallaşmasını mümkün kılmıştır. İmparatorluklardan ulus-devlete geçiş, dağınık güç odaklarını merkezileştirme ve siyasal bütünlüğü sağlama ihtiyacının zorunlu bir sonucuyken; ulus-devlet bu tarihsel baskılara verilen cevaptı. Drucker, s.164-165, 199.

[746] Summa potestas, bir hükümetteki en yüksek veya nihai güç anlamına gelir. Önemli kararları veren ve her şeyi kontrol eden nihai otoritedir. LSDefine, "summa potestas," https://www.lsd.law/define/summa-potestas (E.T.: 1 Şubat 2026).

[747] Ayferi Göze, s. 142.

[748] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.83.

[749] Jürgen Habermas, **Kamusal Alanın Yapısal Dönüşümü,** İstanbul: İletişim, 2003, s.368.

[750] Hardt ve Negri, *İmparatorluk,* s.115-117.

[751] Drucker, s.161.

eliyle değil; platform şirketleri, algoritmalar ve veri altyapıları üzerinden de işlemektedir. Bu nedenle klasik egemenlik anlayışı tartışmaya açılmış; devlet, çoklu aktörlerle rekabet eden sınırlı bir egemenlik odağına dönüşmeye zorlanmaktadır. Devletin güncel arayışı, bu aşınmayı telafi edecek yeni egemenlik araçlarını ve biçimlerini geliştirme çabası olarak ortaya çıkmaktadır.

İkinci etken, dijitalleşmenin egemenlik üzerinde aynı anda hem aşındırıcı hem de yeniden inşa edici bir etki üretmesidir. Dijital ağlar, devletin ülkeselliğini zayıflatarak egemenliği mekâna bağımlı olmaktan çıkarır; veri akışları, yapay zekâ sistemleri, algoritmik denetim ve platform ekonomileri, kontrol ve hesap verebilirliği çok aktörlü yeni güç alanlarına taşır. Bu bağlamda egemenliğin klasik dayanakları olan ülkesellik, hiyerarşi ve hukukilik; sınır tanımayan, akışkan ve büyük ölçüde özel aktörlerin yön verdiği dijital alanda açıklayıcılığını yitirmektedir[752]. Dijital alan, giderek fiziksel devlet aygıtlarından ziyade algoritmalar ve şirket çıkarları doğrultusunda şekillenmektedir[753].

Bu dönüşüm yalnızca coğrafi sınırları değil, hukuki otoritenin yerleşik biçimlerini de çözmekte; birey-devlet ilişkisini mekânsal aidiyetten koparmaktadır. Dijitalleşme, post-modern dönemin karakteristik bir olgusu olarak devleti kuşatmakta, coğrafi temellerini aşındırarak egemenliği sanallaştırmaktadır. Devlet, giderek fiziksel bir varlık olmaktan uzaklaşmakta; bireyler devleti somut bir mekândan ziyade soyut ve ağsal bir yapı olarak algılamaktadır. Siber alanın bir infosfer katmanına dönüşmesi, devleti de kaçınılmaz biçimde sanal bir egemenlik biçimine zorlamaktadır[754].

Bu noktada norm üretiminin karakteri değişmekte; algoritmalar yeni bir normatif güç olarak ortaya çıkmaktadır. Dijital alanda neyin mümkün olduğuna giderek artan ölçüde kod karar verir. Hukuk ile kod arasında tek yönlü bir üstünlük ilişkisi değil, karşılıklı bir etkileşim söz konusudur: Hukuk kodu düzenlemeye çalışırken, kod fiilî pratikleri belirleyerek hukuk üzerinde baskı kurar[755]. Bu nedenle dijital çağda egemenlik, yalnızca siyasal yetkiye değil; veri altyapısı ve kod üzerinde etkili denetim kapasitesine

[752] Şimşek Öner, s.155.
[753] Eren s.557.
[754] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.75-76.
[755] Han, s.16; Küzeci, s.245.

de dayanmaktadır. Kodun değişebilirliği, egemenliği son derece akışkan kılmakta; birkaç satır kodla erişim engellenebilmekte, veri yönlendirilebilmekte ve dijital rejimler yeniden şekillendirilebilmektedir.

Dijitalleşmenin egemenlik üzerindeki etkisi bu nedenle çift karakterlidir. Bir yandan ulus-devletin mutlak egemenlik iddiasını sermaye akımları, küresel piyasalar ve platformlar aracılığıyla belirgin biçimde sınırlandırırken[756] diğer yandan gözetim, denetim ve yönlendirme kapasitesini tarihte görülmemiş ölçüde artırarak egemenliğin yeniden inşasına imkân tanımaktadır[757]. Egemenlik artık yalnızca yönetme yetkisi değil, toplumsal yaşamı üretme gücü olarak biyopolitik bir niteliğe bürünmektedir. Ekonomik, siyasal ve kültürel alanların iç içe geçtiği bu düzende egemenlik, rıza ve itaat üretiminin aktif bir mücadele alanı hâline gelmiştir[758]. Bu tablo, egemenliğin zombileştiği yönündeki iddiaların[759] aksine, onun tarihsel koşullara göre biçim değiştiren ve dijital çağda yeni araçlarla yeniden kurulan bir kavram olduğunu ortaya koymaktadır.

Üçüncü etken, klasik egemenlik anlayışının dijital çağın gerçeklikleriyle uyumsuzlaşması sonucu ortaya çıkan yeni kuramsal yorumlardır. Timmers'e göre, sınır aşan veri akışları, küresel krizler ve teknoloji devlerinin yoğunlaşan etkisi, insan eliyle çizilmiş sınırları işlevsizleştirerek egemenliği parçalı ve kırılgan bir zemine taşımaktadır. Bu bağlamda sarsılan uluslararası sistem, köklü bir yeniden yapılanmanın eşiğindedir. Egemenlik artık yalnızca dış müdahaleden bağımsızlık olarak değil; dijital stratejik özerklik, kritik dijital altyapıları yönetebilme ve yurttaşların dijital haklarını güvence altına alma kapasitesi üzerinden de okunmaktadır[760].

---

[756] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.452.
[757] Küzeci, s.323; Leiser ve Murray, s.5-7; Şimşek Öner, s.155.
[758] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.349.
[759] Devletin dijital alana egemenlik kuramına dayanarak müdahale etmesi eleştirilmekte; çünkü egemenliğin mutlak, bölünmez ve sorumsuz yetkiler içeren klasik tanımı günümüzde hem uygulanamaz hem de tehlikeli görülmektedir. Kavram, otoriter rejimlerce istismar edilmesi nedeniyle artık çağdışı, müphem ve riskli bir güç anlayışını temsil ettiği; bu yüzden "zombi bir kavram" olarak günümüz siyasetinde dolaştığı iddia edilmektedir. (Don Herzog, **RIP Sovereignty**, New Haven: Yale University Press, 2020, s.291). Küreselleşme ve bilgi-iletişim teknolojilerinin gelişimiyle devlet coğrafyalarının artık bir anlam taşımadığı ve geleneksel milli sınırların önemini yitirdiği savunulmuştur: Akdenizli, s.40.
[760] Timmers, *"Sovereignty in the Digital Age",* s.572.

Bu çerçevede sanal devlet ve siber politika gibi kavramlar, devletin giderek ağlar, veri altyapıları ve algoritmik düzenlemeler üzerinden işleyen bir yapıya evrildiğini göstermektedir[761]. Söz konusu dönüşüm yalnızca teknolojik değil; hukuki, siyasal ve kurumsal boyutlarıyla birlikte ele alınmalıdır. Küzeci'nin de vurguladığı üzere, bu süreçte yalnızca devletin bütününün değil, yapısal bileşenlerinde meydana gelen dönüşümlerin de incelenmesi gerekmektedir[762].

Bu yeni bağlamda dijital Leviathan, biyopolitik değil, veripolitik bir nitelik kazanmakta; fiziksel güçten ziyade dijital kontrol ve veri işleme kapasitesine dayalı bir siyasal otorite biçimi olarak yeniden şekillenmektedir. Uluslararası yönetişim tartışmaları egemenliği yeniden merkeze taşımış; ABD, Çin ve AB gibi aktörler dijital egemenlik söylemini stratejik gündemlerinin ayrılmaz bir parçası hâline getirmiştir[763]. Sonuç olarak egemenlik, bütünlüklü ve soyut bir kavram olmaktan çıkarak; dijitalleşme, ilişkisel ağlar ve değişken güç dengeleri içinde biçimlenen çok katmanlı ve yeniden tanımlanması gereken bir olguya dönüşmüştür. Bu yeni egemenlik anlayışı, birey-devlet-dijital sistemler arasındaki karmaşık etkileşimler temelinde yeniden düşünülmelidir.

Dördüncü etken, devletin dijital çağda yeni rolü ve egemenliğin yeniden kurulumu ihtiyacıdır. Devlet kudreti, birey ve grupların toplam gücünü aşan, düzeni ve hiyerarşiyi mümkün kılan üstün bir iktidar biçimidir[764]. Dijitalleşme egemenliği parçalamış olsa da devlet, meşru düzenleyici olma vasfını yitirmemiştir. Teknolojik gelişmenin yönü, bastırılması ya da hızlandırılması, büyük ölçüde devlet müdahalesine

---

[761] Dikmengil, s.172.

[762] Küzeci, s.300.

[763] AB Avrupa Komiseri Thierry Breton, GAFAM şirketlerinin dijital alanı kontrolsüz şekilde yönlendirme çabalarına karşı dijital alanın kara, deniz ve hava sahaları gibi egemenlik alanı olarak düzenlenmesini savunmaktadır. Bertille Bayart ve Jacques-Olivier Martin, "Thierry Breton: «C'est aux Gafa de s'adapter à nos règles, pas l'inverse»", *Le Figaro*, April 10, 2018. Safari Tarayıcı çevirisi. https://www.lefigaro.fr/secteur/high-tech/2018/04/06/32001-20180406ARTFIG00280-thierry-breton-c-est-aux-gafa-de-s-adapter-a-nos-regles-pas-l-inverse.php Çin'in dijital egemenlik vurgusu yalnızca kendi iç politikalarında değildir. Küresel düzeyde de bir lokomotif gibi normatif bir etki yaratmaktadır. Avrupa Birliği, son yıllarda bu söylemi diplomatik pozisyonlarına dahil ederken; ABD, söylemsel düzeyde egemenlikten kaçınsa da pratikte dijital üreticilere yönelik sert müdahalelerde bulunarak bu kavramı fiilen hayata geçirmiştir. Creemers, *"Uneven coverage and blank spaces: bringing the state back in",* s.148.

[764] Recai Galip Okandan, "Devletin İktidar Unsurunun Vasıfları ve Bu Hususta Sürülen Doktrinler", **Journal of Istanbul University Law Faculty,** Vol.16, No.3-4, (2011), s.555.

bağlıdır; toplumların tarihsel kaderi, stratejik teknolojilerde ustalaşma kapasitesiyle yakından ilişkilidir[765].

Bu bağlamda devlet, teknik standartlar, ulusal güvenlik stratejileri, veri koruma rejimleri ve platform düzenlemeleri aracılığıyla dijital alanın normatif çerçevesini belirlemeyi sürdürmektedir[766]. Belirleyici ölçüt fiilî düzenleme gücüdür: Dijital alanı kim etkin biçimde düzenleyip kuralları işletebiliyorsa, egemenlik o aktöre yaklaşır. Devletin geri çekildiği durumlarda ortaya çıkan boşluk, meşruiyet sorunu taşıyan büyük teknoloji şirketleri tarafından doldurulmakta; bu da dijital alanın kamu yararından ziyade şirket çıkarları doğrultusunda şekillenmesi riskini artırmaktadır. Kripto varlıklar, algoritmik hizmetler ve sınır aşan platform ekonomileri, düzenleme boşlukları yarattıkları ölçüde devlet müdahalesini hem iç politikada hem de uluslararası rekabette zorunlu kılmaktadır[767].

Bununla birlikte, ulusötesi şirketlerin veri ve altyapı üzerindeki gücü, nihai olarak devletin sağladığı hukuki çerçeveye dayanır ve bu çerçevenin sınırlarında durur. Küreselleşme ve dijitalleşme, düzen ihtiyacını artırmış; bu durum devleti zayıflatmak yerine, onu küresel hukuk üretiminde hâlâ temel belirleyici aktör konumunda tutmuştur[768]. Şirketlerin yoğun lobi faaliyetleri, sürdürülebilir güçlerinin devlet güvencesi ve hukuki düzenlemelere bağımlı olduğunu fiilen ortaya koymaktadır. Dolayısıyla dijital alanın fiziksel egemenlikten farklı bir zemine sahip olması, devletin merkezi rolünü ortadan kaldırmamış; aksine onu yeni bir düzenleme ve liderlik sorumluluğuyla karşı karşıya bırakmıştır[769].

Bu süreç, devleti tasfiye etmekten çok, dijital güç mimarisi içinde yeniden tanımlamayı ve kod temelli bir egemenlik anlayışına geçişi zorunlu kılmaktadır. Devletler

---

[765] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.8.
[766] Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.2.
[767] Creemers, *"Uneven coverage and blank spaces: bringing the state back in",* s.142.
[768] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.128.
[769] "Google, Facebook, Amazon regulation: Europe vs Washington on privacy, competition and tax," *Politico* https://www.politico.eu/article/google-facebook-amazon-regulation-europe-washington-brussels-privacy-competition-tax-vestager (E.T.: 1 Şubat 2026).

egemenliklerini yeniden tesis etmeye çalışırken, bunun demokratik krizlere yol açabilecek maliyetlerini de göze almak durumundadır[770]. Siber saldırılar, veri ihlalleri, dezenformasyon ve platform kaynaklı güvenlik söylemleri, temel hak ve özgürlüklerin sınırlandırılmasını meşrulaştıran kalıcı bir yönetim mantığı üretmektedir. Böylece güvenlik, istisna olmaktan çıkıp gündelik yönetim tekniğine dönüşürken; özgürlük alanı gözetim, veri toplama ve algoritmik denetim içinde daralmaktadır. Bu durum, Hobbesyen güvenlik karşılığında özgürlükten vazgeçme düşüncesini dijital çağda sürekli bir risk rejimi olarak yeniden üretmektedir[771].

Beşinci etken, dijital egemenliğin etik, toplumsal ve hukukî boyutlarının merkezîleşmesidir. Dijitalleşme, kamusal ve özel alan arasındaki sınırları bulanıklaştırarak bireyi yalnızca vatandaş değil, dijital toplumun sorumluluk taşıyan bir aktörü hâline getirmiştir[772]. Bu durum, bireysel özerklik ile toplumsal yarar, piyasa dinamikleri ile kamu otoritesi arasında yeni bir denge ihtiyacını zorunlu kılar.

Dijital dünya bir yandan bireysel hak ve özgürlükleri genişletme potansiyeli taşırken, diğer yandan mahremiyetin aşınması, demokratik süreçlerin zayıflaması ve kamusal alanın parçalanması gibi ciddi riskler üretmektedir[773]. Dezenformasyon, algoritmik manipülasyon ve siber suçlar, devletin düzenleme sorumluluğunu kaçınılmaz biçimde artırmış; siber güvenlik ve bilişim suçları çağdaş toplumların temel hukuki ve siyasal meseleleri arasına yerleşmiştir[774].

Dijital çağda ifade özgürlüğü yalnızca bireysel tercihlerin tatmini değil, demokratik öz-yönetimin ön koşuludur. Ancak algoritmik sıralama ve kişiselleştirme pratikleri bireyleri yankı odalarına hapsederek yurttaşı kamusal özne olmaktan çıkarıp tüketiciye indirger; ortak kamusal deneyimi ve kamusal akıl yürütmeyi aşındırır[775]. Bu

---

[770] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.464.
[771] Nihat Bulut, "Sahte Bir Karşıtlığın Çözümü: Hukuk Devletinde Özgürlük Güvenlik İlişkisi". **Marmara Üniversitesi Hukuk Fakültesi Mehmet AKAD'a Armağan** içinde (297-318), İstanbul: Der Yayınları, 2012, s.317-318.
[772] Shapiro, s.xii.
[773] Christakis, s.25.
[774] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.5.
[775] Sunstein, s.166-167.

nedenle devletin ifade özgürlüğü ile kamu güvenliği arasında kuracağı normatif denge, demokratik düzenin devamı açısından belirleyici önemdedir. Bu çerçevede platformların, algoritmaların ve içerik akışlarının düzenlenmesi özgürlüğü bastıran değil; aksine demokratik çoğulculuğu ve kamusal alanı korumayı amaçlayan meşru bir müdahale olarak değerlendirilmelidir[776]. Dolayısıyla platform denetimi, içerik yönetişimi ve bilgi güvenliği, teknik düzenleme alanlarının ötesinde, dijital çağda demokrasinin sürdürülebilirliğini doğrudan etkileyen etik ve hukukî sorunlar hâline gelmiştir.

Sonuç olarak dijitalleşme, klasik egemenlik anlayışını sarsarak devleti hem sınırlayan hem de yeni araçlarla yeniden inşa etmeye zorlayan bir dönüşüm üretmiştir. Bu dönüşümün tartışmayı mümkün kılan temel dinamiği, egemenliğin artık yalnız güç tekeli olarak değil; dijital altyapıların yönetimi, yurttaşların dijital haklarının korunması ve demokratik iletişimin güvenceye alınması gibi normatif hedeflerle birlikte düşünülmek zorunda olmasıdır. Dijital çağda verinin stratejik bir iktidar kaynağına dönüşmesi, devlet müdahalesi açısından yeni ve sert bir gerekçe yaratmıştır. Bu bağlamda veri-temelli yeni güç düzeni (dijital kapitalizm veya dijital feodalizm) devletin egemen niteliğini aşınması açısından içerdiği iki temel tehdit belirginleşmiştir:

(i) özel dijital aktörlerin devletin düzenleme alanına ve yurttaşını belirlemesine fiilen ortak olması,

(ii) bireysel hak ve özgürlüklerin aşınması karşısında devletin koruma yükümlülüğünün genişlemesi.

Bu iki tehdit, dijital egemenlik tartışmasının neden yalnız teknik değil, kaçınılmaz biçimde siyasal ve anayasal bir mesele olduğunu göstermektedir.

[776] Sunstein, s.142, 153-154.

II. İNSAN UNSURUNUN DÖNÜŞÜMÜ

Devletin genel teorisi, tarihsel olarak belirli kurucu unsurlar üzerine inşa edilmiştir. Georg Jellinek'in üç unsur teorisi, devleti belirli bir ülke, bu ülke üzerinde yaşayan insan topluluğu ve bu topluluğu yöneten siyasal iktidar bileşenleriyle tanımlar[777]. Kamu hukuku öğretisinde de devletin varlığı, iktidarın kullanılacağı bir insan topluluğu ile bu topluluğun yaşadığı toprak parçası ve bunları örgütleyen siyasal otoritenin birlikteliğini zorunlu kılar. Okandan'a göre bu beşerî unsur, rastlantısal bir kalabalık değil; birlikte yaşama iradesi geliştirmiş, siyasal örgütlenme düzeyine ulaşmış olgun bir toplumsal bütündür[778]. Vitoria'nın ifadesiyle bu bütün, üyelerinin sayısal toplamını aşan bağımsız bir *corpus* (beden) niteliği taşır[779].

Tarihsel süreç, bu üç unsurun her dönemde aynı ağırlıkta kavranmadığını göstermektedir. Antik polis düzeninde insan unsuru ön plandayken, erken kent devletlerinde toprak unsuru belirleyici olmuş; modern çağda ise insan unsuru "ulus", toprak unsuru "vatan" ve iktidar unsuru "egemenlik" kavramları etrafında ideolojik ve hukuki olarak merkezîleştirilmiştir[780]. Modern devlet, bu merkezîleştirme sayesinde yurttaşlığı mekânsal aidiyet, hukuki statü ve siyasal sadakat temelinde tanımlayabilmiştir.

Bu bölüm, söz konusu üçlemenin en dinamik ve kırılgan bileşeni olan insan unsurunun, dijitalleşme süreciyle geçirdiği yapısal dönüşümü incelemektedir. Klasik egemenlik anlayışında insan unsuru; belirli bir ülkeye bağlı, vatandaşlık bağıyla tanımlanan ve hukuki statüsü mekânla ilişkilendirilmiş bireyler bütünüyken dijitalleşme bu çerçeveyi köklü biçimde dönüştürmektedir. İnsan, artık yalnızca hukuki bir özne değil; dijital ağlarda sürekli veri üreten, kimliği algoritmik süreçlerle çözümlenen ve mekânsal bağlardan kısmen kopan bir veri öznesine (data subject) dönüşmektedir. Bu dönüşüm, bireyin siyasal ve ahlaki özneliğini zayıflatma; onu giderek tüketici profiline indirgeme riskini de beraberinde getirmektedir.

---

[777] Georg Jellinek, "Allgemeine Staatslehre", 3. Baskı, 1914, s.394 vd. Aktaran: Doehring, s.24.
[778] Recai Okandan, "Devletin Beşeri Unsuru", **İstanbul Hukuk Mecmuası,** Cilt.13, Sayı.4, 1947, s.1295.
[779] Akal, *Modern Düşüncenin Doğuşu: İspanyol Altın Çağı,* s.41.
[780] Uygun, s.10.

Nitekim Sunstein, tercihlerin platform mimarileri ve algoritmik yönlendirmeler tarafından şekillendirilmesi nedeniyle özgür iradeye dayalı birey varsayımının fiilen aşındığını; bireyin kendi arzusunu dahi üretmeyen yönlendirilmiş bir özneye dönüştüğünü vurgular[781]. Bu bağlamda dijitalleşme, bireyi bir yandan fiziksel sınırların ötesine taşırken, diğer yandan daha yoğun bir gözetim, ölçümleme ve sınıflandırma rejiminin içine yerleştirmektedir.

İnsan unsurundaki bu dönüşüm, yalnızca insan-teknoloji ilişkisinin araçsal boyutuyla açıklanamaz. Burada söz konusu olan, bireyin kendini, toplumu ve devleti algılama biçiminin ontolojik düzeyde yeniden yapılandırılmasıdır. Bilişim teknolojileri, modern devletle özdeşleşmiş ulus ve yurttaşlık kavramlarını aşındırmakta; mekâna bağlı siyasal aidiyet yerine ağlara dayalı, akışkan ve parçalı kimlik biçimlerini öne çıkarmaktadır[782]. Dijitalleşme böylece bireyi hem merkezsizleştirmekte hem de daha yoğun biçimde denetlenebilir hâle getirmektedir.

Bu bölüm, söz konusu paradoksu yani güçlenme ile zayıflamanın eşzamanlılığını insan unsurunun dönüşümü üzerinden ele almaktadır. Analiz; modern insan tasavvurunun felsefi temellerinden başlayarak kapitalist rasyonalitenin etkilerine ve dijital çağın psikolojik, siyasal ve teknolojik kırılmalarına uzanmaktadır. Bu çerçevede yurttaşlığın verileşme süreci, bireyin egemenlik ilişkileri içindeki konumunun yeniden tanımlanması ve ulus-devlet sonrası toplumsal örgütlenme biçimleri tartışılacaktır. Özellikle Shapiro'nun kontrol toplumuna ilişkin yaklaşımı, Anderson'ın hayali cemaatler kavramının dijital izdüşümleri ve Varoufakis'in teknofeodalizm tezi, insan unsurunun yeni egemenlik mimarisi içindeki konumunu çözümlemek için kuramsal dayanaklar sunmaktadır.

[781] Sunstein, s.106-107.
[782] Küzeci, s.233.

A. Ulustan Yeni Toplum Biçimlerine: Dijital Cemaatler

1. Ulus, Yurttaş ve Küreselleşme

Modern siyasal düşüncede devletin insan unsuru ve egemenliğin meşruiyet kaynağı, büyük ölçüde millet/ulus kavramları üzerinden açıklanır. Ulus, rastlantısal bir nüfus yığını değil; ortak anlatılar, paylaşılan semboller ve birlikte yaşama iradesi etrafında bütünleşmiş, kendisinin farkında olan bir siyasal topluluktur[783]. Bu yönüyle ulus, yalnızca sosyolojik bir birlik değil; siyasal iktidarın meşrulaştırılmasında işlev gören kurucu bir kategoridir.

Okandan'a göre devletin varlığı, belirli niteliklere sahip bir insan topluluğunu zorunlu kılar; bu topluluğun tarihsel ve toplumsal koşullar altında uluslaşma düzeyine erişmiş olması[784] devletin kuruluşu açısından belirleyicidir. Bu nedenle nüfus veya halk gibi betimleyici kavramlar, devlet kurucu siyasal topluluğu açıklamakta yetersiz kalırken; ulus kavramı devletin maddi ve objektif beşerî zeminini ifade eder[785]. Batı Avrupa'da modernitenin ürünü olarak şekillenen ulus, bu bağlamda yalnızca kültürel bir aidiyet değil; siyasal ve hukuki bütünleşmeyi sağlayan bir örgütlenme modeli olarak işlev görmüştür[786].

Bununla birlikte ulus, modern anlamda kendiliğinden var olan doğal bir olgu değil; büyük ölçüde ulus-devletin kuruluş sürecinde işletilen uluslaştırma pratikleriyle inşa edilen siyasal bir projedir. Eğitim, zorunlu askerlik, seçim mekanizmaları, resmî dil ve tarih anlatıları, toplumu ulusal birlik kurgusuna uygun hâle getiren başlıca araçlar olmuştur[787]. Bu süreçte ulus, bireyin kutsallığına dayanan türetilmiş bir kutsallık kazanmış; siyasal meşruiyetin kaynağı olarak yüceltilmiştir[788]. Ancak Akkaya'nın

---

[783] Akad, Dinçkol ve Bulut, s.125; Erözden, s.47.
[784] Hatice Kübra Pehlivan, "Türk Anayasalarında Millî Devlet, Ülke ve Vatandaşlık Kavramları", (**Yüksek Lisans Tezi,** Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü, 2006), s.4.
[785] Recai Okandan, *"Devletin Beşeri Unsuru",* s.1282-1283.
[786] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.37.
[787] Akad, Dinçkol ve Bulut, s.124; Ali Coşkun Kırca, "Devlet ve Üniversite (Bir Reform Taslağının Anahatları)", **İnan Kıraç'a Armağan,** İstanbul: Galatasaray Üniversitesi Yayınları, Yayın No: 1, 1994, s.143.
[788] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.8-9.

vurguladığı gibi, sosyal sözleşme söylemi içinde ulus, sözleşmeden önce var olan kurucu bir özne değil; egemenlik eliyle, yani devlet tarafından kurulan bir yapıdır[789].

Bu inşa karakteri, Anderson, Hobsbawm ve Renan'ın yaklaşımlarında kuramsal karşılığını bulur. Anderson'ın "hayali cemaat" kavramsallaştırması, ulusun yüz yüze ilişkilerden değil; matbaa kapitalizmi, ortak dil ve sembolik dolaşım yoluyla kurulan bir tahayyül birliği olduğunu ortaya koyar[790]. Hobsbawm'a göre millet değil, milliyetçilik önceldir; uluslar çoğu zaman modernleşme sürecinde milliyetçilik ideolojisi aracılığıyla üretilmiştir[791]. Renan ise ulusu, ortak geçmiş kadar geleceğe yönelik birlikte yaşama iradesine dayanan ve sürekli yeniden üretilen bir "günlük plebisit" olarak tanımlar[792]. Bu yaklaşımlar, ulusun doğal değil, tarihsel ve siyasal bir inşa olduğunu ortak biçimde teyit eder.

Ulus inşasının merkezinde yurttaşlık yer alır. Yurttaşlık, birey ile devlet arasında karşılıklı hak ve yükümlülüklere dayanan hukuki-siyasal bir statü[793] olmanın ötesinde, siyasal aidiyet ve katılım rejimidir[794]. Antik Polis'ten modern devlete uzanan çizgide yurttaşlık; eşitlik, özgürlük ve kamusal sorumluluk fikriyle birlikte düşünülmüştür[795]. Modern hukukta yurttaşlık, bireyi hem hak sahibi bir özne[796] hem de egemenliğin

---

[789] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.54-55.

[790] Benedict Anderson, **Hayali Cemaatler: Milliyetçiliğin Kökenleri ve Yayılması,** İskender Savaşır (çev.), İstanbul: Metis Yayınları, 1995, s.33, 58; Erözden, s.87; Serkan Bulut, s.26.

[791] Eric Hobsbawm, **1780'den Günümüze Milletler ve Milliyetçilik: "Program, Mit, Gerçeklik",** Osman Akınhay (çev.), İstanbul: Ayrıntı Yayınları, 2010, s.24-30; Recai Okandan, *"Devletin Beşeri Unsuru",* s.1286.

[792] Ernest Renan, **Ulus Nedir?,** Gökçe Yavaş (çev.), İstanbul: Pinhan Yayıncılık, 2016, s.37-38, 50-52; Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.71.

[793] Ergin Nomer, "Türk Vatandaşlık Hukukunun Genel İlkeleri", **Cumhuriyetin 75. Yılı Armağanı** içinde, İstanbul: İstanbul Üniversitesi Yayınevi, 1999, s**.**733.

[794] Cemil Caca Arslan, "Politik Hukukbilim Çerçevesinde Dijital Anayasacılık", **Muhafazakâr Düşünce Dergisi**, Cilt.20, Sayı.67, (2024), s.257.

[795] Akad, Dinçkol ve Bulut, s.25-28; Ağaoğulları ve Köker, *İmparatorluktan Tanrı Devletine*, s.54-55; Şenel, s.198; Bihterin Vural Dinçkol ve Alper Işık, "1924 Anayasası Döneminde Yurttaşlık Anlayışı", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.21, Sayı.1, (2015), s.15; Uygun, s.107-108.

[796] Dinçkol ve Işık, s.16.

taşıyıcısı[797] olarak konumlandırır[798]. Bu yönüyle özgürleştirici olduğu kadar disipline edici bir işleve de sahiptir[799].

Ulus-devlet pratiğinde yurttaşlık çoğu zaman türdeşleştirme ve dışlama mekanizmalarıyla birlikte işler[800]. Ortak dilin resmîleştirilmesi ve eğitim yoluyla yaygınlaştırılması, yalnızca iletişim ihtiyacını karşılamaz; aynı zamanda iktidarın, statünün ve ideolojinin yeniden üretimine hizmet eder[801]. Bu nedenle ulus-devlet, kapsayıcı bir siyasal birlik iddiası taşırken, aynı anda farklılıkları bastıran ve homojen bir kimlik dayatan bir yapı üretir[802]. Uluslaşma, bu anlamda olgusal çoğulluğu monist kurguya yaklaştırmaya yönelik sürekli bir devlet pratiği olarak işler[803].

Küreselleşme ile birlikte bu yapı ciddi biçimde sarsılmıştır. Ulus-devletin yurttaşlık üzerinden kurduğu siyasal aidiyet, küresel sermaye akışları, ulus-aşırı kurumlar ve dijital iletişim ağları karşısında gevşemiş[804] yurttaşlık giderek kültürel, parçalı ve çok katmanlı kimlik biçimlerine dönüşmüştür[805]. Göç, çokkültürlülük, çifte vatandaşlık ve kozmopolit hak söylemleri, ulus-devletin homojen yurttaş varsayımını aşındırmıştır[806].

---

[797] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.223.

[798] Akad, Dinçkol ve Bulut, s.126; Bihterin Vural Dinçkol, "Laiklik, Aydınlanma, Modernleşme ve Türkiye Modeli", **Prof. Dr. Tankut Centel'e Armağan** içinde (653-662), İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Yayınları, 2011, s.659.

[799] Pierson, s.44-47; Akkaya Kia, *"Uygarlık, Modernite ve Medeniyet Sözcüklerinin Hukuka Bakan Yüzü",* s.113-114; Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.46-47; Eugene Enriquez, Sürüden Devlete, s. 334-335.

[800] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.421-422; Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.64-65; Erözden, s.124-125; Hardt ve Negri, *İmparatorluk,* s.124; Anderson, s.20-22.

[801] Rukiye Akkaya Kia, "1876 Kanun-i Esasi'nin 18. Maddesi Üzerine". **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.XV, Sayı.3-4, (2011), s.35; Hobsbawm, s.110-111, 135, 161; Anderson, s.20-22; Schneider, *China's Digital Nationalism,* s.231; Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.74.

[802] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.73; Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.135-141.

[803] Sulhi Dönmezer, "Devletin Ülkesi ve Millî ile Bütünlüğü ve Bölünmezliği İlkesi", **İstanbul Üniversitesi Hukuk Fakültesinin 50. Yıl Armağanı: Cumhuriyet Döneminde Hukuk** içinde, İstanbul: İstanbul Üniversitesi Yayınları, Yayın No: 1888, 1973, s.16; Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.32; Erözden, s.158-161; Anderson, s.157-163;

[804] Hardt ve Negri, *İmparatorluk,* s.344-345; Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.151.

[805] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.97.

[806] Bilge Bingöl Schrijer, "Vatandaşlık Hakkının Kapsamı ve Egemenlik İlişkisi Üzerine Bir Değerlendirme", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi** Cilt.XXII, Sayı.1, (2018), s.206, 246, 256-259; Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.88-89; Arif Dirlik, **Küreselleşmenin Sonu Mu?,** İsmail Kovacı ve Veysel Batmaz (çev.), İstanbul: Ayrıntı Yayınları, 2012, s.145-146.

Aynı süreçte devlet, küresel kapitalizmin yerel yöneticisi konumuna itilmiş[807] yurttaşlık bağı, siyasal katılımdan ziyade tüketim ve yönetişim pratikleri etrafında yeniden tanımlanmıştır[808].

Hardt ve Negri'nin "İmparatorluk" kavramsallaştırması bu dönüşümü ulus-devlet ötesi bir iktidar rejimi olarak açıklar: egemenlik artık sınırlar üzerinden değil; biyopolitik, dijital ve ekonomik ağlar üzerinden işlemektedir[809]. Bu düzende dijitalleşme, yurttaşı veri öznesine indirgerken; siyasal katılımın yerini gözetim, yönlendirme ve algoritmik kontrol almaktadır. Ulus-devlet bu nedenle yalnız kültürel değil, varoluşsal bir egemenlik kriziyle karşı karşıyadır[810].

Sonuç olarak küreselleşme, ulus-devlet ve klasik yurttaşlık bağını aşındırmakla birlikte, aynı zamanda kimlik krizlerini derinleştirerek milliyetçiliğin reaksiyonel biçimlerde yeniden yükselmesine de zemin hazırlamıştır. Bu durum, ulusun yalnızca kültürel bir ortaklık değil; tarihsel hafıza, siyasal proje ve kurumsallaşmış yurttaşlık kapasitesi sayesinde hâlen dirençli bir siyasal form olduğunu göstermektedir[811]. Modern ulus-devlet, dönüşmekte fakat bütünüyle ortadan kalkmamaktadır; egemenliğin ve yurttaşlığın yeni biçimleri, dijital ve küresel güç ilişkileri içinde yeniden müzakere edilmektedir[812].

2. Yurttaşın Verileşmesi: Küresel Yurttaşlıktan Dijital Yurttaşlığa Dönüşüm

Dijitalleşme, modern yurttaşlığın ulus-devlet düzeni içinde varsaydığı temel kabulleri dönüştüren yapısal bir kırılma yaratmaktadır. Ağ temelli toplumsal örgütlenmede birey, artık yalnızca kamusal karar süreçlerine katılan siyasal bir özne olarak değil; aynı zamanda sürekli veri üreten, izlenen, sınıflandırılan ve öngörülen bir

---

[807] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.137; Dirlik, *Küreselleşmenin Sonu Mu?,* s.171.
[808] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.97-98, 385; Dirlik, *Küreselleşmenin Sonu Mu?,* s.173.
[809] Hardt ve Negri, *İmparatorluk,* s.14-21.
[810] Drucker, s.242-243; Talip Kabadayı, "Felsefenin Işığında '(Haklı) Savaş' Üzerine Kısa Bir Deneme", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII Sayı.1, 2014, s. 97.
[811] Drucker, s.171-172.
[812] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.72-73.

profil olarak konumlanmaktadır. Bu dönüşüm, yurttaşlığı hak ve ödevlere dayalı politik bir statü olmaktan çıkararak, gözetim, ölçüm ve algoritmik yönetim üzerinden işleyen bir kimlik rejimine doğru kaydırmaktadır.

Bu kırılmanın ilk görünür düzlemi, kamusal hizmetlerin dijital platformlar aracılığıyla sunulmasıdır. E-devlet uygulamaları, yurttaşı giderek "kullanıcı" olarak tanımlamakta; devlet-yurttaş ilişkisi katılım ve temsil zemininden kısmen uzaklaşarak veri akışına dayalı bir hizmet ilişkisine indirgenmektedir. Dijital davranışların puanlanması, haklara erişimin performans skorlarına bağlanması ve yaptırımların otomatikleşmesi, yurttaşlığı hak sahipliğinden ziyade uyum ve ölçülebilirlik mantığına dayalı bir statüye dönüştürme riskini barındırmaktadır[813].

Dijitalleşme, yurttaşlığı mekân ve ulus temelinde tanımlayan klasik çerçeveyi de zayıflatmaktadır. Modernite, devleti rasyonel ve laik bir temelde belirli bir zaman ve mekâna bağımlı kılarak dünyevileştirirken; eş zamanlı olarak sosyal sistemi bu yerel bağlardan koparıp soyutlayarak evrensel ve sembolik bir yapıya dönüştürmüştü[814]. Dijitalleşme; çevrimiçi varlık, netizen (internet yurttaşı) gibi kavramlarla yeni aidiyet biçimleri üretirken, bu aidiyet çoğu zaman ortak siyasal iradeden ziyade etkileşim, görünürlük ve içerik dolaşımı üzerinden kurulmaktadır[815]. Böylece yurttaşlığın kolektif sorumluluk ve kamusal katılım boyutu, platform mimarilerinin teknik ve kültürel kodları tarafından yeniden biçimlendirilmektedir. Ortaya çıkan kimlik, siyasal bilinçten çok dijital performans ve tüketim davranışları etrafında şekillenmektedir[816].

Bu noktada belirleyici olan, platformların kullanıcıyla kurduğu ilişkinin niteliğidir. Dijital platformlar, kuralları tek taraflı belirleyen, erişimi ve görünürlüğü yöneten, yaptırımı doğrudan uygulayan yapılar olarak fiilî bir otorite tesis etmektedir. Hesabın kapatılması, görünürlüğün düşürülmesi veya erişimin sınırlandırılması, teknik bir işlem olmanın ötesinde, bireyin dijital kamusal alandan dışlanmasına benzer sonuçlar

---

[813] Florian A. Schneider, **Feeling the Nudge: Political Communication and Governance in Digital China,** Leiden University, 6 Mayıs 2024, s.13.
[814] Akkaya Kia, *"Uygarlık, Modernite ve Medeniyet Sözcüklerinin Hukuka Bakan Yüzü",* s.114.
[815] Dijital yerliler, dijital kültüre doğmuş ve onunla iç içe büyümüş bireyleri; dijital göçmenler, bu kültüre sonradan adapte olan kuşakları temsil eder.
[816] Schneider, *China's Digital Nationalism,* s.12.

doğurabilmektedir. Bu nedenle mesele, platformların egemenlik taşıyıp taşımadığı sorusundan ziyade, kamusal alanı yönetme kapasitelerinin egemenlik benzeri etkiler üretip üretmediği sorusu etrafında tartışılmalıdır.

Algoritmik yönetişim, yurttaşın dijital kamusal alandaki varlığını da köklü biçimde dönüştürmektedir. Yankı odaları ve kişiselleştirilmiş içerik akışları, bilgi çeşitliliğini daraltarak bireyi kamusal tartışmanın faili olmaktan çok yönlendirilen bir içerik tüketicisine dönüştürebilmektedir. Siyasal katılım, kolektif karar süreçlerine katkı olmaktan çıkarak; beğeni, tıklama ve paylaşım gibi ölçülebilir tepkilere indirgenmekte, bu tepkiler ise platformların veri ekonomisini besleyen davranışsal girdiler hâline gelmektedir. Böylece yurttaşlık pratiğinin yerini, ölçümlenen ve optimize edilen dijital etkileşim almaktadır[817].

Başlangıçta dijitalleşmenin devlet sınırlarını aşındıracağı varsayılsa da güncel pratikler, yeni sınırlar ve yeni egemenlik alanlarının ortaya çıktığını göstermektedir. Bir yandan Estonya'nın e-Residency modeli gibi mekândan bağımsız statüler geliştirilirken[818] diğer yandan büyük platformlar kendi topluluk kuralları üzerinden fiilî bir platform yurttaşlığı rejimi inşa etmektedir. Bu durum, yurttaşın edilgen, yönlendirilebilir ve kolayca manipüle edilebilir bir dijital özneye dönüşmesine işaret eden ontolojik bir kırılmayı beraberinde getirmektedir.

Bu yeni düzende yurttaşlık bilinçli katılım ve sorumluluk temelli bir statü olmaktan uzaklaşmakta; bireyin veri üretim kapasitesiyle tanımlanan ekonomik bir profile indirgenmektedir[819]. Yurttaşın kimliği ve davranışları, giderek ulusal hukuk sistemlerinden çok özel şirketlerin küresel veri altyapılarında işlenmektedir. Bu durum, devletin yurttaşını koruma ve yargılama kapasitesini zayıflatırken, bireyin tarihsel olarak

[817] Han, s.14-15, 30.

[818] Estonya e-Residency uygulamasında devlet, egemenliğini toprakla sınırlı tutmayıp, dijital alana taşımaktadır. Dünyanın herhangi bir yerindeki bir birey, Estonya'nın dijital yurttaşı (e-mukim) olarak, o ülkenin ticari ve hukuki altyapısını kullanabilmektedir. Bu, insan unsurunun mekândan kopuşunun en somut hukuki örneğidir.

[819] Sunstein, s.110-123; Roberts ve Diğerleri, s.2; Cemil Caca Arslan, s. 258.

hak sahibi özne olarak tanımlanan konumunu gözetlenen bir nesneye doğru kaydırmaktadır[820].

Bu bağlamda yurttaşlığın normatif çekirdeği aşınmaktadır. Aristoteles'te yönetime katılım ve kamusal sorumlulukla tanımlanan yurttaşlık, modern dönemde medeni, siyasal ve sosyal haklarla kurumsallaşmışken[821] dijital çağda kamusal alan; platformların piyasa mantığı ve algoritmik öncelikleri doğrultusunda yeniden düzenlenmektedir. Karar verici özne olarak demos'un yerini, kural koyucu ve uygulayıcı konumundaki platform mimarileri almaktadır. Bu nedenle dijital platform düzeni, öz-yönetim değil, hiyerarşik bir yönetim formu üretmektedir.

Dijital yurttaşlığın en kritik kırılmalarından biri, rıza ile tâbiiyet arasındaki sınırın belirsizleşmesidir. Kullanım sözleşmeleri ve algoritmik karar sistemleri, yurttaşlığın fiilî normlarını anayasal metinlerden ziyade kod ve veri mimarileri içinde üretmektedir. Bireyin deneyimi kendisine ait görünse de bu deneyimden çıkarılan verinin değeri üzerindeki denetim, bireyin elinde değildir[822]. Böylece veri ekonomisinin mülkiyet ve güç ilişkileri, yurttaşlığın eşitlik ve özgürlük iddiasıyla derin bir gerilim üretmektedir[823]. Bu noktada, Locke'un mülkiyet eşitsizliğini ve sınırsız kârı haklılaştırdığı emek-mülkiyet bağı[824] ilginç bir korelasyonla kendini yeniden göstermektedir: Deneyim bireyin, ama değeri yaratan emek dolayısıyla işlenen veri üzerinde hak iddiası şirketindir.

Dönüşümün bir başka boyutu, dijital toplulukların ulusal aidiyetle ilişkisi üzerindendir. Dijital platformlar, kültürel kodlar, ortak düşman imgeleri ve dil pratikleriyle yeni hayali cemaatler inşa edebilir. Bu, ulusal kimliği zayıflatabileceği gibi devlet açısından dijitalleşmeyi uluslaştırma stratejilerinin parçası haline getirme imkânı da doğurabilir. Veri yerelleştirme, milli teknoloji üretimi ve dijital içerik politikalarıyla,

---

[820] Joel R. Reidenberg, "Yahoo and Democracy on the Internet," **Jurimetrics,** Vol.42, No.261, (2001-2002), s.264.
[821] Bihterin Vural Dinçkol, "Yurttaşlık ve Seçilme Hakkı Üzerine Bir Değerlendirme", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.19, Sayı.2, (2013), s.103.
[822] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.129-130, 165170.
[823] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.20-21.
[824] Akad, Dinçkol ve Bulut, s.139-140.

ulusal bütünlük dijital araçlarla yeniden üretilebilir; Çin'de dijital milliyetçiliğin platformlar, algoritmalar ve devlet yönetişimi içinde çok katmanlı biçimde şekillenmesi bu tartışmaya önemli bir örnek sunar[825]. Bu modelde, duyguları hedefleyen içeriklerle ulusal aidiyet yeniden üretirken, bireylerin dijital çevresi algoritmik sosyal mühendislikle tasarlanmaktadır[826]. Devlet yalnızca düzenleyici değil, aynı zamanda dijital kamusal alanın doğrudan mimarıdır[827]. Bu yapıda milliyetçilik, ideolojik propaganda olmanın ötesinde, ulusal ticari platformların kâr mantığıyla birleşerek viral bir içerik formatına dönüşür[828]. Emojilerden görsellere kadar dijital sembollerle desteklenen bu yapı, bireyleri hızlı ve geniş çapta mobilize ederken, yurttaşlık anlayışını da kullanıcı sözleşmelerine indirger[829]. Bu yapı, dijital milliyetçiliği yalnızca bir ideolojik tercih olmaktan çıkarıp, algoritmik bir norm haline getirmektedir[830]. Devlet ve platformlar tarafından uygulanan bu dijital yönetim biçimi, klasik yurttaşlık anlayışını ciddi biçimde sarsar ama aynı zamanda algoritmik, davranışsal ve ekonomik süreçlerle yeniden inşa edilmektedir.

Sonuç olarak dijital yurttaşlık, ulusal yurttaşlığın çevrimiçi ortama taşınmış basit bir uzantısı değil; piyasa temelli, algoritmik ve ulus-sonrası bir toplumsal formun siyasal karşılığıdır. Bu düzende yurttaş, egemenliğin kaynağı olmaktan uzaklaşarak, egemenliğin veri üzerinden işlendiği bir nesneye indirgenme riskiyle karşı karşıyadır. Asıl mesele, dijital alanın varlığı değil; yurttaşın verisi üzerindeki denetimini, gerçek siyasal katılım kanallarını ve özne olma kapasitesini yeniden kurabilecek hukukî ve siyasal düzenlemelerin imkânıdır[831]. Sınır tanımayan dijital tahakküm karşısında ulus-devletin

---

[825] Çin'de dijital milliyetçilik, bireysel çevrimiçi tepkilerin ötesine geçerek devlet, teknoloji ve ekonomiyle bütünleşmiş kurumsal bir yönetim stratejisi hâline gelmiştir. Milliyetçi söylem, dijital bilgi ve iletişim teknolojileri aracılığıyla filtrelenmekte, yeniden yapılandırılmakta ve hızla dolaşıma sokularak ulusal aidiyet duygusu güçlendirilmektedir. Kullanıcılar, ulusal onura yönelik algılanan tehditlere çevrimiçi tepkiler vererek bu söylemi yeniden üretirken, Çin Komünist Partisi dijital milliyetçiliği siyasal bir araç olarak değerlendirmektedir. Schneider, *China's Digital Nationalism,* s.1-3, 7.

[826] Schneider, *China's Digital Nationalism,* s.173.

[827] Schneider, *China's Digital Nationalism,* s.205-206.

[828] Creemers, *"Disrupting the Chinese State: New Actors and New Factors",* s.176; Florian A. Schneider, "Nationalisms on China's evolving internet", **Communication and the Public,** Vol.9, No.4, (2024), s.2-3.

[829] Schneider, *Feeling the Nudge: Political Communication and Governance in Digital China,* s.15.

[830] Mercy A. Kuo, "China's Digital Nationalism and Activism: Insights from Florian Schneider", *The Diplomat,* 17 Ağustos 2017, https://thediplomat.com/2021/08/chinas-digital-nationalism-and-activism/ (2 Şubat 2026).

[831] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.639.

yurttaşı koruma yükümlülüğü yeniden tanımlanmalıdır[832]. Dijital toplum, teknik bir dönüşüm değil, yurttaşın kurucu özne ve hak sahibi konumunu güvenceye bağlayan derin bir siyasal-hukukî sorun olarak ele alınmalıdır[833]. Aksi halde yurttaşlık, hak ve sorumluluk temelli kamusal bir kimlik olmaktan çıkarak, platform mimarilerinin ürettiği davranışsal bir kategoriye dönüşecektir. Ulusu ya da yurttaşı olmayan egemen, bir topluma değil olsa olsa boş bir çöle hükmedebilir.

B. Dijitalleşmenin İnsana ve Topluma Etkisi

1. Ontolojik Bir Dönüşüm: Homo Juridicus'tan Homo Digitalis'e

Klasik siyasal düşüncede insanın toplumsal ve siyasal niteliği, Aristoteles'in zoon politikon kavramsallaştırmasıyla temellendirilir. İnsan, iyi yaşamı tek başına gerçekleştiremez; erdemli ve mutlu yaşam ancak ortak yarar etrafında örgütlenen siyasal topluluk içinde mümkündür[834]. Bu nedenle polis, yalnızca bir yönetim tekniği değil, insanın ahlaki ve siyasal özne olarak yetkinleştiği kurucu bir yaşam biçimidir[835]. İnsanı diğer canlılardan ayıran, iyi-kötü ve adil-haksız gibi normatif ayrımları kavrayabilme yetisidir[836]. Siyasal topluluk da bu normatif alanın kurumsal zemini olarak ortaya çıkar[837].

İlerleme odaklı dünya görüşü insanın doğaya karşı mücadelesinin akılcı ilkeleri modern uygarlığın temelini oluşturmuştur[838]. Modern dönemde hukuk ve siyaset kuramı, rasyonel karar verebilen, irade sahibi ve özerk birey varsayımı üzerinde yükselir. Aydınlanma ile birlikte hukukun ve siyasal iktidarın kaynağı, aşkın bir otoriteden koparılarak insan aklına dayandırılır; birey hem hakların taşıyıcısı hem de hukuk

---

[832] Castells, **Enformasyon Çağı: Ekonomi, Toplum ve Kültür Üçüncü Cilt Binyılın Sonu,** Ebru Kılıç (çev.), İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2008, s.492.
[833] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.348.
[834] Akal, *Modern Düşüncenin Doğuşu: İspanyol Altın Çağı,* s.41.
[835] Şenel, s.170.
[836] Zeynep Özlem Üskül, "Ortaçağda Teologların Akılla Buluşmasının Bir Örneği: St. Thomas D'aquin", **Prof. Dr. Necip Kocayusufpaşaoğlu İçin Armağan,** Ankara: Seçkin Yayınları, 2004, s.777.
[837] Uygun, s.131.
[838] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.92.

düzeninin kurucu öznesi olarak düşünülür[839]. Homo Juridicus modeli, meşruiyeti bireysel rıza ve genel irade kavramları üzerinden kurarken, siyasal düzeni bireysel özerklik ve haklar aracılığıyla temellendirir[840]. Bu çizgide siyaset, yalnızca iktidarın örgütlenmesi değil, akla uygun yaşamın kurumsal koşullarını tesis eden bir düzenleme pratiği olarak anlaşılır[841].

Modern egemenlik açısından temel kırılma, yasanın kaynağında yaşanır. Hukukun ilahi referanslardan koparılması, bireyin değer kazanmasını ve devletin toplum mühendisliği yapan hukuki-siyasal bir aygıt olarak düşünülmesini mümkün kılar[842]. Kantçı anlamda rüşt, bireyin aklını başkasının kılavuzluğu olmaksızın kullanabilme yetisini[843] ifade ederken; Locke'un deneyimci *tabula rasa* yaklaşımı, modern öznenin epistemik temelini güçlendirir[844]. Böylece insan hem siyasal düzenin öznesi hem de onun meşruiyet kaynağı olarak konumlanır.

Dijital çağ ise bu modern özne modelini ontolojik düzeyde dönüştürmektedir. Homo Digitalis, dijital ağlarla çevrili, hafızası dışsallaştırılmış, davranışları veri izlerine indirgenmiş ve karar süreçleri algoritmik yönlendirmelerle çerçevelenen bir varlık olarak belirir. Tercihler; açık baskı veya yasak yoluyla değil; görünmez dürtme mekanizmaları, büyük veri analitiği ve olasılık hesapları üzerinden yapılandırılmaktadır. Böylece modern yurttaşın özerklik iddiası, zorlayıcı iktidar biçimleri olmaksızın aşınmaktadır[845].

---

[839] Rukiye Akkaya, "J.B. Bossuet: 'Devlet Sizsiniz Majesteleri'!", **GSÜHFD**, Cilt.2025, Sayı.2, (2025), s.815; Yasemin Işıktaç, "İrade Özgürlüğüne Giriş Açısından 'Ben İnşâsı'", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII, Sayı.1, (2014), s.85.

[840] Alain Supiot, **Homo Juridicus: Hukukun Antropolojik İşlevi Üzerine Bir deneme,** Bilge Açımuz Ünal (çev.) Ankara: Dost Kitabevi Yayınları, 2014, s.75; Zeynep Özlem Üskül Engin, "Birey Kavramının Gelişimi ve İnsan Hakları", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII, Sayı.1, (2014), s.204.

[841] Uygun, s.127-128.

[842] Dinçkol, *"Laiklik, Aydınlanma, Modernleşme ve Türkiye Modeli",* s.653-654; Üskül Engin, *"Birey Kavramının Gelişimi ve İnsan Hakları",* s.205; Akad ve Diğerleri, s.18; Akal, *Devlet, Yasa, Hakimiyet*, s.36-37.

[843] Rukiye Akkaya Kia, "Hukukun Kadına Bakışı: Ergen ve Eşit Olamama Hali", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi,** C.XIII, Sayı.1-2, (2009), s.88-89.

[844] Uygun, s.229.

[845] Şebnem Özdemir, "Post-Panoptikon Çağı: Gözetimin Dijitalleşmesi ve Çevrimiçi Kimliğin Gizliliği Üzerine Bir Analiz", **Anadolu Üniversitesi Sosyal Bilimler Dergisi,** Cilt.20, Sayı.3, 2020, s.91-94.

Bu dönüşüm, modern toplumun insan unsurunu kuran ulus-devlet-kapitalizm eksenli düzenle[846] de gerilim içindedir. Hak sahibi, rasyonel yurttaş olarak kurgulanan modern birey; dijitalleşmeyle birlikte gözetlenen, yönlendirilen ve çoğu zaman edilgen bir kullanıcıya evrilmektedir. Ortaya çıkan kırılma yalnızca psikolojik değil; devlet ile birey arasındaki temsil, bağlılık ve yurttaşlık ilişkilerinin zemininde yapısal bir erozyondur.

Protagoras'ın "İnsan her şeyin ölçüsüdür" ifadesi, sofist düşüncede insanı merkeze alan yaklaşımın özlü bir ifadesidir. Buna karşılık Pindaros'un "Yasalar her şeyin kralıdır" sözü, ölçütün insan iradesinden değil, bireyden bağımsız ve üstün kabul edilen kurallardan kaynaklandığını vurgular. Bu iki görüş birlikte ele alındığında, Protagoras'ın değişmez ve mutlak olduğu varsayılan yasal düzenlere eleştirel bir mesafe alarak, ölçüyü insanın kendisine ve onu diğer varlıklardan ayıran aklına dayandırdığı görülür[847]. Oysa dijital çağda birey, ne kamusal düzeni kendi aklıyla kurabilen etkin bir özne ne de hukuki ve siyasal düzenin merkezinde yer alan asli bir fail olma konumunu sürdürebilmektedir. Bu nedenle dijitalleşmeden uzak durma ya da "matrixten çıkıp analog kalma" yönündeki arayışlar, salt teknik bir tercih değil, özne olarak varlığını koruyabilmenin mümkün olup olmadığına ilişkin normatif bir sorgulama olarak ortaya çıkmaktadır.

Ontolojik dönüşüm, hakikat rejiminde de belirgin bir kırılma üretir. Bilginin aşırı çoğalması ve algoritmik sıralama pratikleri, modern dönemde ortak gerçeklik algısı etrafında kurulan kamusal hakikat zeminini zayıflatırken; yankı odaları ve post-truth dinamikleri nesnel gerçeklik algısını parçalamaktadır. Mahremiyetin ortadan kalkması ve hakikatin çözülmesi birlikte ilerleyerek bir körleşme yaratırken[848] dijital çağda birey, kendi bilgi evrenine hapsolma riskiyle karşı karşıya kalmaktadır.

Bu bağlamda dijitalleşme, yalnızca bir teknoloji dalgası değil, aynı zamanda bir birikim rejimi olarak ortaya çıkar. Veri, sermaye gibi depolanır, işlenir ve sürekli yeniden üretilir. Yurttaşlık ve toplumsal yaşam, giderek bu enformasyon mantığına göre yeniden

---

[846] Antony Giddens, **Ulus Devlet ve Şiddet,** Cumhur Atay (çev.), İstanbul: Kalkedon Yayınları, 2008, s.8-12.
[847] Şenel, s.131.
[848] Rukiye Akkaya Kia, "'Körleşme' Üzerine (2)", **Hukuk Kuramı,** Cilt.5, Sayı.3, (Eylül–Aralık 2018), s.72.

düzenlenmektedir. Akıllı şehir ve akıllı toplum projeleri, verimlilik ve uyum söylemleri altında ideal yurttaş tipleri üretirken, gözetimi ve teknik yönetişimi gündelik yaşamın altyapısına yerleştirir[849].

Sonuç olarak Homo Juridicus'tan Homo Digitalis'e geçiş, insanın siyasal ve ahlaki özne olma kapasitesini zayıflatan ontolojik bir kırılmaya işaret etmektedir. Dijital çağda temel sorun, teknolojinin varlığı değil; insanın kamusal aklın kurucu öznesi olmaktan çıkarak veri temelli yönetimin nesnesine dönüşmesidir. Bu nedenle dijitalleşme, insan unsurunu merkeze alan hukukî ve siyasal bir yeniden düşünmeyi zorunlu kılmaktadır.

2. Kapitalist Aklın Dehümanizasyonu: Algoritmik Tahakküm Karşısında Nesneleşme ve Gerçeklik Algısının Kaybolması

İnsan, yalnızca biyolojik ihtiyaçlarla tanımlanan bir varlık değil; bilinç, edim ve anlam üretimi aracılığıyla toplumsal bir özne olarak kurulan bir varoluştur. İnsan olma hâli, doğanın sınırlarını aşan bu bilinç ve toplumsallık içinde anlam kazanır[850]. Ne var ki kapitalist rasyonalite, bireyi tarihsel ve kültürel bağlamından koparak ölçülebilirlik, performans ve hesaplanabilirlik ekseninde standartlaştırır. Akıl, bu süreçte hakikati arayan eleştirel bir yeti olmaktan çıkar; zamanın, mekânın ve düşüncenin araçsallaştırıldığı bir tahakküm mantığına eklemlenir. Yararlı olanın yüceltilmesi, işe yaramayanın değersizleştirilmesi ve eşitsizliklerin bireysel yetersizliklere indirgenmesi, bu rasyonalitenin meşrulaştırıcı söylemlerini oluşturur. Güçlüler, kendilerini hiyerarşinin tepesinde sabitlerken, geride kalanları yalnızca bu konumu sürdürmenin araçları olarak görür[851].

Dijital kapitalizm, bu nesneleştirici mantığı derinleştirerek bireyi ilişkilerinden, hafızasından ve tarihsel bağlamından daha radikal biçimde koparır. Modernitenin;

---

[849] Örneğin, Çin, Singapur, Hong Kong, Taipei, Güney Kore, Japonya ve Hindistan gibi ülkelerin teknolojik çözümlerle yeniden tasarladıkları kentsel yaşamda teknik altyapıların yanında yeni bir toplum vizyonu da inşa edilmektedir. Florian A. Schneider "Digital smartness, rethinking communities and citizenship in the face of 'smart' technology", **Asiascape: Digital Asia,** Leiden, Vol.6, No.3, (2019), s.152-155.

[850] Çalgan, s.197.

[851] Çalgan, s.181-189.

inanmak ve itaat etmek yerine düşünmek ve düşünen yurttaş vaadi[852] veri merkezli dijital işleyişte tersyüz olur; birey, platform mimarileri ve giyilebilir teknolojiler içinde şekillenen bir veri profiline indirgenir. Tarihsel bilinç, kültürel hafıza ve eleştirel düşünme geri plana itilirken; yönetilen, sorgulamayan ve hafızasız kitleler üretilir[853]. Bu indirgeme yalnızca kültürel bir yoksullaşma değil, aynı zamanda siyasal alanın daralması anlamına gelir; manipülatif biçim değişimleriyle insanın tutsaklığı derinleştirilir[854]. Algoritmik karar sistemleri, siyasal tercihleri özgür iradeye dayalı muhakemenin ürünü olmaktan çıkararak görünmez yönlendirmelerle biçimlendirilmiş davranış kalıplarına dönüştürür.

Algoritmik tahakkümün temel mekanizmalarından biri, kişiselleştirme söylemi altında işleyen dijital yönetişimdir. Algoritmalar, bireyleri veri noktalarına indirgerken insanî nitelikleri silikleştirir; algoritmik yanlılık, tarihsel önyargıları ve yapısal eşitsizlikleri yeniden üreterek dehümanizasyonu kurumsallaştırır[855]. Bu bağlamda kişiselleştirme, bireysel özerkliği genişleten bir imkân olmaktan ziyade, eğilimler ve kırılganlıklar üzerinden işleyen bir manipülasyon tekniğine dönüşür. İçerik akışları ve öneri sistemleri, bireyin düşünsel süreçlerini aşındırarak yalnızlaşmayı ve toplumsal atomizasyonu derinleştirir[856]. Dijital alanda sürekli görünür olma, onaylanma ve kendini bir "profil" olarak kurma baskısı, duygusal-psikolojik düzeyde de kırılmalar üretir; bu bağlamda TDK'nın 2024 yılının kelimesi seçtiği "kalabalık yalnızlık" olgusu, dijital toplumsallığın paradoksal sonucu olarak yaygınlaşır.

Dijital kapitalizmin tahakkümü, yalnızca gözetim ve yönlendirme yoluyla değil; zaman ve dikkat rejimi üzerinden de işler. Zamansız ve mekânsız bir akış içinde birey "an"a hapsedilir; etkileşim ve performans göstergeleri varoluşun temel ölçütleri hâline gelir. Bu kontrol biçimi çoğu zaman fiziksel zor yerine bağımlılık üretimi, dikkat ekonomisi ve zihinsel sömürü üzerinden işler. Sürekli teknik yenilik, toplumsal ilerleme

---

[852] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.52.
[853] Çalgan, s.92-99.
[854] Çalgan, s.107-108.
[855] Oğuz Kuş, "Algoritmaları Dehümanizasyon Kavramı Çerçevesinde Tartışmak", **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021, s.53, 62-63.
[856] Çalgan, s.69-70.

üretmek yerine kolektif anlamın boşalmasına ve toplumsal hareket kapasitesinin zayıflamasına yol açar. Birey hızlanırken toplumun bütünsel hareket kabiliyeti felce uğrar[857].

Bu süreç, gerçeklik algısında da ciddi bir kırılma yaratır. Algoritmik filtreleme, yankı odaları ve simülasyon pratikleri, gerçek ile kurgu arasındaki sınırı belirsizleştirir. Distopik anlatılarda -örneğin Matrix metaforunda- betimlenen simülasyon rejimi, burada yalnızca bir kurgu değil; gerçekliğin algoritmik olarak üretildiği bir siyasal duruma işaret eder[858]. Gerçekliğin bu şekilde yeniden kurulması, egemenliğin ve meşruiyetin hangi zeminde üretildiği sorusunu da yeniden gündeme getirir.

İnternetin başlangıçtaki vaadi, aracıları ve kapı bekçilerini azaltarak bireyi güçlendirmekti. Ancak pratikte ortaya çıkan yapı, merkezi otoriteleri tasfiye etmek yerine dijital biçimde yeniden üretmiştir. Platformlar, kullanıcıları veriye indirgeme yoluyla yeni kapı bekçileri hâline gelmiştir[859]. Birey; özerk bir özne olmaktan ziyade sınıflandırılan, yönlendirilen ve ekonomik değere dönüştürülen bir nesneye evrilmiştir. Dijital altyapı, bu anlamda kapitalist tahakkümün yoğunlaştığı yeni bir toplumsal düzenleme alanı hâline gelmiştir.

Son olarak otomasyonun özgürleştirici vaadi de yeniden değerlendirilmelidir. Otomasyon, emeği azaltarak insanı özgürleştirmek yerine, bireyi sürekli veri üreten ve algoritmik denetime tabi bir dijital bileşene dönüştürebilmektedir. Bu nedenle özgür yurttaş ile dijital çağın otomatik öznesi arasındaki fark, teknolojik ilerleme söylemi içinde gözden kaçırılmaması gereken temel bir siyaset felsefesi ve hukuk teorisi sorunu olarak ortaya çıkmaktadır.

---

[857] Ahmet Gürbüz, "Günümüz Batılı Politik Yaklaşımların Kökeni Olarak İngiliz Yararcılığı/Utilitarianism", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan**, Cilt.LXXII, Sayı.1, (2014), s.167.
[858] Varoufakis, *Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,* s.101-102; Çalgan, s.59-63.
[859] Lehdonvirta, s.205.

3. Küreselleşmiş Bilgi Toplumunda Kimlik ve Kültür

Dijitalleşme ile toplum, sanayi toplumunun maddi üretim merkezli yapısından bilgi ve ağ temelli bir toplumsal düzene evrilmiştir. Bu yeni yapıda birey, toplumsal ilişkileri kuran bir özne olmayı sürdürmekle birlikte, aynı zamanda sürekli veri üreten, izlenen ve algoritmik süreçlerle analiz edilen bir profile dönüşmektedir. Dijital medya teknolojilerinin gündelik yaşamın altyapısı hâline gelmesi, kimliğin de iletişim ve dolaşım pratikleri içinde yeniden üretildiği yeni bir alan yaratmıştır. Platform ekosistemlerinin iletişim, ticaret, bankacılık ve kamusal hizmetleri tek bir dijital çatı altında bütünleştirmesi, gündelik hayatın giderek platformlaştığını göstermektedir[860].

Modern ulus-devletler, özellikle 19. yüzyılda farklı toplulukları merkezi bir siyasal yapı altında birleştirirken ulusal kimliği kurucu bir aidiyet formu olarak inşa etmiştir. Bu kimlik, yalnızca ortak köken anlatılarıyla değil; duygu, sadakat ve fedakârlık gibi sembolik bağlarla da güçlendirilmiştir[861]. Ancak sanayi toplumundan bilgi toplumuna geçişle birlikte kimlik üretiminde devletin tekelci konumu zayıflamış; ulus-ötesi aktörler, küresel sermaye ve dijital platformlar kimliğin biçimlenmesinde belirleyici rol üstlenmiştir. Bu süreçte kültürel hegemonya, doğrudan siyasal tahakkümden ziyade bilgi üretimi, dolaşım ve temsil pratikleri üzerinden yeniden kurulmaktadır.

Bu nedenle kültür, günümüzde yalnızca yaşam tarzlarının veya sembollerin toplamı değil; aynı zamanda iktidarın kurulduğu ve sürdürüldüğü stratejik bir alandır. Batı-merkezli kültürel düzen, kimi zaman evrensellik iddiasıyla Batılı normları dayatırken, kimi zaman da gelenek söylemi aracılığıyla ötekini tarihsel olarak sabitleyen bir işleyiş sergiler[862]. Küreselleşmenin baskın biçimleri ulusal kültürleri homojenleştirme eğilimi taşıdığında, kültürel kimlik bireysel bir tercih olmaktan çıkarak küresel güç ilişkileri karşısında varoluşsal bir savunma alanına dönüşür. Bu bağlamda Batı kaynaklı kuramların evrensel kabul edilerek farklı toplumsal bağlamlara doğrudan uygulanması, yalnızca yöntemsel değil, aynı zamanda hegemonik bir bilgi rejimi sorunu

[860] Florian Schneider, "Reality Decoupling: Rumours, Disinformation, and Studying the Politics of Truth in Digital Asia", **Asiascape: Digital Asia,** Vol.10, No.1-2, (2023), s.183.
[861] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.64.
[862] Dirlik, *Postkolonyal Aura: Küresel Kapitalizm Çağında Üçüncü Dünya Eleştirisi,* s.49-55.

üretmektedir[863]. Bu nedenle Amerikanizasyona karşı ulusun savunulması, yalnızca bir siyasal biçimin sürdürülmesine değil, aynı zamanda bir kültürel varlığın muhafazasına da hizmet eder[864].

Küreselleşme; siyasal, kültürel ve ekonomik katmanları iç içe geçiren asimetrik bir süreçtir. Devletler bu düzene eş zamanlı ve eşit koşullarda eklemlenmez. Dijital iletişim ağları farklı kültürleri görünür ve temas hâlinde kılarken, bu karşılaşmalar kimi zaman çoğulluğu artırmakta, kimi zaman ise kimlik çatışmalarını derinleştirmektedir[865]. Bu nedenle küreselleşmiş bilgi toplumunda kimlik, yalnızca ulusal siyaset tarafından değil; sınır aşan dijital akışlar ve platform mimarileri tarafından da sürekli yeniden biçimlendirilen dinamik bir yapıya dönüşmüştür.

Bu dönüşümün en kritik boyutlarından biri, kimliğin platformlaşmasıdır. Dijital bilgi toplumunda kimlik, giderek devletin tanıdığı hukuki statülerden ziyade, platformların kullanıcıya atadığı sanal profiller ve algoritmik temsiller üzerinden şekillenmektedir. Büyük dijital platformlar; kimlik doğrulama, görünürlük, erişim ve hesap bütünlüğü gibi mekanizmalar aracılığıyla davranışları yönlendirme kapasitesine sahiptir. Böylece kimliğin üretilmesi ve denetlenmesi, devletin tekelinden kısmen çıkarak özel dijital altyapıların eline geçmektedir. Bireyin kamusal ve sosyal varlığı, giderek bu platformlara bağımlı hâle gelmektedir[866].

Buna karşılık yurttaşlık perspektifinden bakıldığında kimlik, yalnızca kültürel bir aidiyet değil; ortak yaşamın sorumluluklarını içselleştiren ve kamusal alana katılımı mümkün kılan siyasal bir bağdır[867]. Dijitalleşme ile birlikte ulus-ötesi yapılar ve platform aktörleri, devlet sınırlarını aşan paralel iktidar biçimleri üreterek bireyi yalnız siyasal alanda değil; kültürel, hukuki ve epistemik düzeylerde de kendi normatif çerçeveleri içine çekmektedir. Küresel kapitalizm, kültürel çeşitlilik söylemini dolaşıma sokarken aynı anda ekonomik ve kültürel merkezileşmeyi derinleştirmekte; böylece kimlik alanı, ulusal

[863] Dirlik, *Postkolonyal Aura: Küresel Kapitalizm Çağında Üçüncü Dünya Eleştirisi,* s.62.
[864] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.122.
[865] Akdenizli, s.43.
[866] Lehdonvirta, s.68-69.
[867] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.83-87.

sınırların ötesinde sınıfsal, kültürel ve dijital hiyerarşilerle yeniden yapılandırılmaktadır[868].

Sonuç olarak küreselleşmiş bilgi toplumunda kimlik, ne yalnızca devlet tarafından belirlenen ulusal bir aidiyet ne de bütünüyle bireysel bir tercih alanıdır. Kimlik, dijital platformlar, küresel sermaye ve ulus-devlet arasındaki güç ilişkileri içinde sürekli yeniden üretilen, çatışmalı ve çok katmanlı bir toplumsal form hâline gelmiştir. Bu durum, kültür ve kimliği yalnız sosyolojik değil; egemenlik, yurttaşlık ve demokratik meşruiyet açısından da merkezi bir sorun alanı hâline getirmektedir.

4. Kontrol Devrimi: Özgürlük Yanılsaması ve Kişiselleştirilmiş Tahakküm

Andrew Shapiro'nun "kontrol devrimi" kavramsallaştırması, dijital çağda özgürlük ve özerklik söyleminin nasıl tersyüz olabildiğini açıklamaya yöneliktir. Dijitalleşme başlangıçta bilgiye erişimi kolaylaştıran, bireyi aracı yapılardan kurtaran ve özerkliği artıran bir özgürleşme vaadi taşımıştır. Ancak Shapiro'ya göre bu vaat, zaman içinde paradoksal biçimde daha yoğun bir gözetim, yönlendirme ve kısıtlama rejimine dönüşmüş; böylece klasik yurttaşlık modelinden farklı bir dijital toplumsallık biçimi ortaya çıkmıştır.

Bu dönüşümün merkezinde kişiselleştirme bulunur. Kişiselleştirme teknolojileri kullanıcıya, kendi deneyimini dilediği gibi düzenlediği ve kontrol ettiği izlenimini verir. "My Yahoo", "My Computer" gibi isimlendirmelerin ima ettiği mülkiyet ve kontrol duygusu, bireyin bilgi fazlalığıyla başa çıkma arzusuna seslenir. Ne var ki bu kontrol, çoğu zaman algoritmik filtrelerin sunduğu sınırlı bir seçki üzerinden gerçekleşir. Kullanıcı bilgi kirliliğinden arındığını düşünürken, gerçekte daha dar, daha mütecanis ve daha kolay yönetilebilir bir enformasyon alanına yönlendirilir; filtre balonları ve yankı odaları böyle bir daralmanın kurumsal sonucudur. Bu nedenle kişiselleştirme, özgürleşme değil; özerkliğin simülasyonu ve kontrolün içselleştirilmesi olarak işleyebilir[869].

---

[868] Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.107-112.
[869] Shapiro, s.44-45, 106.

Cass Sunstein'a göre aşırı kişiselleştirme, bireyleri yalnızca kendi görüşlerini doğrulayan içeriklerle çevreleyerek ortak gerçekliği aşındırmakta; kamusal alanı atomize etmekte ve kutuplaşmayı derinleştirmektedir. Yankı odaları ve siber yayılma dalgaları (cybercascades)[870] bilgiyi dar bir çevrimde tekrar ederek yanlışları bile ortak doğruya dönüştürür; benzer görüşlü gruplar giderek daha uç noktalara savrulur[871]. Birey, özgür seçim yaptığını sanırken, gerçekte önceden belirlenmiş seçenekler arasında dolaşan bilişsel olarak kapatılmış bir özneye dönüşmektedir. "Daily Me" tarzı bilgi akışı özerklik değil, rafine bir zihinsel yalıtım üretir. Bu durum, yurttaşı hak sahibi bir kamusal aktör olmaktan çıkararak tüketiciye indirgemekte; düşünceyi ise kamusal değer üreten bir faaliyet olmaktan uzaklaştırmaktadır[872].

Kontrol mekanizmasının yanılsama niteliği bu noktada belirginleşir. Birey kararlarını özgür iradesiyle verdiğini varsayar; ancak bu kararların çerçevesi, arayüz tasarımları, sıralama mantıkları ve algoritmik önceliklendirme tarafından önceden belirlenmiştir. Seçim hakkı biçimsel olarak korunur fakat seçeneklerin görünürlüğü ve erişilebilirliği algoritmik olarak üretildiği için özerklik içerik bakımından zayıflar. Özgürlük hissi, bu yönüyle, bireyi yönlendirilmeye daha açık hâle getiren bir araç işlevi görür.

Kontrol devriminin ayırt edici özelliği, tahakkümün açık zor yoluyla değil, gönüllü rıza üzerinden işlemesidir. Dijital özne, baskıyla itaat eden bir bireyden ziyade, özerklik inancı üzerinden yönlendirilen bir varlık hâline gelir. Davranışsal yönlendirme mantığıyla uyumlu biçimde sistem, kullanıcı davranışlarını gözlemler, tahmin eder ve belirli seçenekleri öne çıkararak tercihleri şekillendirir. Kullanıcı seçtiğini zannederken, çoğu kez dijital altyapının sunduğu güdümlü alternatifler arasından seçim yapar[873].

Kişiselleştirmenin etkisi bireysel düzeyle sınırlı kalmaz; kamusal alanın yapısını da dönüştürür. Kullanıcıların ağırlıkla kendi görüşlerini doğrulayan içeriklerle

[870] Cybercascades (Türkçeye siber taşma veya siber yayılma dalgaları olarak çevrilebilir) dijital ortamda doğru ya da yanlış bilgilerin algoritmaların da etkisiyle tekrar ve taklitle hızla zincirleme biçimde yayılmasını; bu süreçte düşük doğruluklu içeriklerin bile geniş kitlelerce gerçek gibi algılanmasını ifade eder.
[871] Sunstein, s.57.
[872] Sunstein, s.48, 65.
[873] Shapiro, s.180.

karşılaşması, ortak bir gündem ve ortak bir gerçeklik zeminini aşındırır. Demokratik kamusal alan açısından belirleyici olan çoğulculuk ve karşılaşma imkânları daraldıkça, empati, uzlaşma ve kamusal akıl yürütme kapasitesi zayıflar[874]. Böylece kamusal tartışma, ortak hakikat üretimi olmaktan çıkarak paralel ve yalıtılmış bilgi evrenlerine bölünür.

Bu süreçte mahremiyet de yapısal bir dönüşüm geçirir; metalaşır. Mahremiyet, kamusal özne olmanın ve siyasal özerkliğin koşullarından biri olmaktan çıkarak, sözleşme ve veri değişimi konusu hâline gelir. Rızaya dayalı görünse bile, bu rızanın bilgi asimetrisi ve tasarım yönlendirmeleri nedeniyle manipülatif bir zeminde üretilmesi, bireyin kamusal özne niteliğini aşındırır. Kişiselleştirilmiş deneyim, bu yönüyle, öznelliğin metalaştırılmasıyla sonuçlanır[875].

Kontrol devrimi ekonomik alanda da kişiselleştirilmiş tahakküm biçimleri üretir. Dijital pazarlar yüzeyde daha fazla seçenek sunduğu izlenimini verse de filtreleme ve sıralama mekanizmaları yoluyla tüketici davranışını merkezî biçimde yönlendirir[876]. Bu durum, ekonomik karar alma süreçlerinde platform-merkezli bir yoğunlaşmaya yol açarken, yerel ve ulusal piyasa aktörlerini giderek görünmezleştirir ve ekonomik egemenliği dijital altyapılara daha bağımlı hâle getirir.

Bu yönlendirme pratikleri gündelik deneyimde çoğu zaman küçük tasarım araçlarıyla görünür olur. Rozetler (badges) ve dürtme mekanizmaları (nudges), kullanıcıya özgürce karar veriyormuş hissi verirken; tercihleri platformun ekonomik ve yönetsel çıkarları doğrultusunda standartlaştıran görünmez bir kontrol katmanı oluşturur[877]. "Çok satan", "son ürün", "önerilen satıcı", "X kişi inceliyor", "indirim bitiyor" gibi işaretler, kararın bağlamını kurarak kullanıcının davranışını belirli yönlere iter. Bu nedenle kontrol, açık bir zorlamadan ziyade, gündelik seçimlerin mikro-düzenlenmesi üzerinden işler.

---

[874] Shapiro, s.123-124.
[875] Shapiro, s.164.
[876] Lehdonvirta, s.98.
[877] Lehdonvirta, s.104.

Sonuç olarak Shapiro'nun kontrol devrimi yaklaşımı, dijital çağda iktidarın yasaklayan değil, tercihleri üreten bir forma evrildiğini ortaya koyar. Kişiselleştirme ve özgürlük söylemi kesiştiğinde, rıza üzerinden işleyen kişiselleştirilmiş bir tahakküm rejimi ortaya çıkar. Bu düzende birey, klasik anlamda özerk yurttaş olmaktan uzaklaşarak; veriye tabi, gözetlenen ve davranışları ince ayarlanmış bir dijital özneye dönüşür.

5. Tekno-Feodalizm: Dijital Serfliğe Geçiş ve Platform Lordluğu

Yanis Varoufakis'in tekno-feodalizm kavramsallaştırması, dijital çağda modern yurttaşlığın nasıl yapısal bir çözülmeye uğradığını ve bu çözülmenin yerini platform egemenliği altında kurulan yeni bir hiyerarşik düzene bıraktığını açıklamayı amaçlar. Bu dönüşüm, yalnızca teknoloji kullanımındaki niceliksel artışla sınırlı değildir; hak, katılım ve temsil gibi yurttaşlık kategorilerinin anlam kaybına uğradığı, buna karşılık bireyin veri, dikkat ve dijital davranışları üzerinden sömürüldüğü serflik benzeri yeni bir bağımlılık ilişkisinin kurumsallaştığı bir rejim değişimini ifade eder[878].

Varoufakis'e göre dijitalleşme, kapitalist üretim ilişkilerinin merkezinde yer alan pazar mekanizmalarını bütünüyle ortadan kaldırmasa da onları belirleyici ölçüde baypas eden bir düzen üretir. Google, Meta ve Amazon gibi büyük platformlar, piyasanın dağınık ve rekabetçi yapısı yerine, kendi ekosistemleri içinde merkezî karar alanları yaratarak fiilî bir dijital mülkiyet tesis eder. Bu nedenle ortaya çıkan yapı, klasik kapitalizmden ziyade feodalizmin işleyiş mantığına yaklaşır: Değer üretimi serbest piyasa etkileşimleri içinde değil, platformun sahip olduğu dijital arazi üzerinde gerçekleşir; iktisadi ilişki, sözleşmesel eşitlikten çok bağımlılık ve bağlılık ekseninde kurulur.

Bu bağlamda modern yurttaş, pazarda üretici ya da tüketici olarak konumlanan özerk bir aktör olmaktan uzaklaşarak, platformların toprağında yaşayan bir dijital serfe dönüşür. Platform düzeninde kullanıcı, sistemin müşterisi değildir; aksine sistemin ürettiği ve pazarladığı değerin bizzat parçasıdır. Platformların gerçek müşterileri reklam verenler, veri analiz şirketleri ve politik kampanya endüstrileridir; kullanıcı ise

[878] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.159.

davranışları, tercihleri ve çevrimiçi alışkanlıkları üzerinden ekonomik değere çevrilen bir veri kaynağıdır. Bu nedenle kullanıcı, tüketici olmaktan çok tüketilen bir kaynak hâline gelir.

Tekno-feodal rejimde egemenlik, büyük ölçüde algoritmik olarak kurulur. Algoritmalar, kullanıcı davranışlarını izleyerek hem karar ufkunu biçimlendirir hem de bireyi veri temelli bir metaya dönüştürür. İlgi alanları, deneyimler, kimlik göstergeleri ve sosyal ilişkiler, dijital ekonominin hammaddesi hâline gelir. Platformlar dışarıdan hammaddesiz görünse de gerçekte ürünlerini insanın kendisinden üretir: dikkat, etkileşim ve veri, sermaye birikiminin asli kaynağına dönüşür[879].

Ücretsiz hizmet olarak sunulan dijital platformlar, bu düzenin meşruiyet zemininin önemli bir parçasını oluşturur. Kullanıcı, konfor ve erişim kolaylığı karşılığında dikkatini, etkileşimlerini ve verisini meta olarak sisteme devreder. Bu süreçte ortaya çıkan emek biçimi, klasik anlamda fiziksel ya da ücretli emek değil; platformların değer üretimini mümkün kılan sürekli veri üretimi ve dijital davranıştır. Böylece yurttaş, demokratik kamusal alanda karar süreçlerine katılan bir aktör olmaktan uzaklaşır; emeği tanınmayan, karşılıksız katkı sunan bir bulut emekçisine indirgenir[880].

Varoufakis'in tarihsel analojisinde bu dönüşüm, feodal dönemdeki çitleme süreçleriyle karşılaştırılabilir. Feodal beylerin ortak kullanım alanlarını özel mülke dönüştürmesi gibi, dijital çağda da bireyin verisi, davranışı ve kimliği çoğu zaman farkında olmaksızın platformların çevrili mülkü hâline gelir. Sonuç, dijital öznenin kendi kimliği ve dijital varlığı üzerinde denetim kuramaması; yani veri-serf olarak tanımlanabilecek bir bağımlılık ilişkisidir. Bu bağımlılık yalnızca iktisadi değil, aynı zamanda siyasal sonuçlar da üretir: Kamusal alanın kuralları giderek platform mimarilerinde belirlendikçe, yurttaşlık rejimi demokratik içeriğini kaybetmeye başlar[881].

Sonuç olarak tekno-feodalizm, dijital yurttaşlığın demokratik hakları genişleten bir aşamaya değil; platform lordlarının egemenliği altında şekillenen yeni bir dijital

[879] Çalgan, s.83-84.
[880] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.177.
[881] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.72.

serfliğe işaret ettiğini ileri sürer. Bu çerçevede modern yurttaş yerini dijital serfe, devlet otoritesi ise veri feodallerinin kurduğu altyapısal iktidara bırakma eğilimi gösterir[882]. Böyle bir dönüşüm, yurttaşlığın yeniden tanımlanmasını yalnızca normatif bir tartışma olmaktan çıkararak; ekonomik ve teknolojik mülkiyet ilişkileri üzerinden yürütülen yapısal bir egemenlik sorunu hâline getirir.

C. İnsan Odaklı Yaklaşım: Tahakküm veya Sömürü Değil Erdemli Toplum Düzeni

Dijital çağın baskın teknolojik yönelimi, bireyi özerk bir özne olmaktan uzaklaştırarak ölçülen, tahmin edilen ve yönlendirilen bir veri kaynağına indirgeme riski taşımaktadır. Bu risk, dijitalleşmenin özgürleştirici bir imkân olmasının yanı sıra, distopik bir toplumsal düzene de zemin hazırlayabileceğini göstermektedir. Buna karşılık insan odaklı yaklaşım; Society 5.0 gibi modeller[883] ve dijital hümanizm tartışmaları çerçevesinde, teknolojinin kâr maksimizasyonu ve kontrol mantığına değil, insan onuru, erdem ve ortak iyilik temelinde bir toplum düzenine hizmet etmesi gerektiğini savunur[884].

Bu tartışma, özünde klasik bir felsefi gerilimin güncel bir tezahürüdür: Teknolojik ilerleme insanı özgürleştirir mi, yoksa onu daha incelmiş bağımlılık ilişkilerine mi mahkûm eder? Bu gerilim, Rousseau'nun Bilimler ve Sanatlar Üzerine Söylev'de dile getirdiği eleştirilerle birlikte okunduğunda daha görünür hâle gelir. Rousseau'ya göre ilerleme, zorunlu olarak ahlaki yetkinleşme üretmez[885]. Bilakis lüks, konfor ve gösterişin yaygınlaşması, erdemin aşınmasına ve toplumsal çürümeye zemin hazırlayabilir[886]. Benzer biçimde, dijital çağda teknolojik konforun artışı eleştirel

---

[882] Varoufakis, *Technofeudalism: What Killed Capitalism,* s.160-161.

[883] Japonya tarafından 2016 yılında 5. Bilim ve Teknoloji Temel Planı ile ortaya atılan Toplum 5.0 (Society 5.0), insanlık tarihinin gelişim aşamalarını (1.0 Avcı, 2.0 Tarım, 3.0 Sanayi, 4.0 Bilgi) takip eden Süper Akıllı Toplum evresidir. The University of Tokyo Hitachi-UTokyo Laboratory (H-UTokyo Lab.), **Society 5.0: A People-centric Super-smart Society,** Singapore: Springer Nature, 2018, s. xii.

[884] Timmers, *"Sovereignty in the Digital Age",* s.572.

[885] Jean Jacques Rousseau, **Bilimler ve Sanatlar Üzerine Söylev**, İstanbul: Türkiye İş Bankası Kültür Yayınları, 2007, s.21.

[886] Rousseau'ya göre, bilim ve sanatlar çoğunlukla insanın zaaflarından doğmuştur: Astronomi boş inançlardan; güzel konuşma hırstan ve dalkavukluktan; geometri cimrilikten; fizik gereksiz meraktan türemiştir. Ona göre, lüks olmasaydı bu lükse hizmet eden sanatlar da gelişmezdi; haksızlıklar olmasaydı hukuk bilimine ihtiyaç kalmazdı; zalim yöneticiler ve savaşlar olmasaydı tarih yazımı anlamsız olurdu. Bilim ve sanatların yokluğu, toplumun daha kötü, zayıf ya da

düşüncenin güçlenmesiyle örtüşmeyebilir; aksine yönlendirme ve manipülasyonun sıradanlaşması, kamusal aklın zayıflamasına yol açabilir.

Rousseau'nun uyarısını güncelleyen temel nokta şudur: Bilim ve akıl, özgürleştirici bir kuvvet olmaktan saparak ideolojik bir aygıta dönüşebilir[887]. Egemen ideoloji, yalnızca aklı köreltmekle kalmaz; toplumsal bilimleri, sanatı ve felsefeyi de araçsallaştırarak sahte bir rasyonalite üretir[888]. Zor, hile ve manipülasyon yoluyla işleyen bu ideolojik akılcılık, özgürlük duygusunu aşındırır ve bireyi uygar toplumların pasif bir unsuruna dönüştürür[889]. Günümüzde dijital kapitalist düzen, özellikle algoritmik sistemler aracılığıyla nesnel ve tarafsız görünse de güç ilişkilerini yeniden üreten bir sahte kesinlik üretmektedir. Veri temelli optimizasyon ve ölçülebilirlik ideolojisi kamusal alanı kuşattıkça, eleştirel muhakeme geri plana itilir; bu kuşatma yalnız ekonomik değil, kültürel ve bilişsel üretim alanlarını da daraltır[890].

İnsan odaklı yaklaşım ise dijital çağın bireylerini yalnızca yönlendirilen tüketiciler ya da veri üreticileri olarak değil; özgür, sorumlu ve erdemli yurttaşlar olarak yeniden konumlandırmayı amaçlar. Buradaki erdem vurgusu, dijital düzenin yalnız teknik bir mimari değil, aynı zamanda normatif bir yapı olduğunu hatırlatır. Sokrates'in erdem anlayışı bu bağlamda işlevseldir: Erdem, iyi ile kötüyü ayırt edebilme bilgisine dayalı bir yetkinliktir ve erdemli birey, yalnız kendisi için değil, toplum için de sorumluluk taşır[891]. Dolayısıyla dijital toplumun insan onuruna uygun biçimde kurulması, yalnız ahlaki bir ideal değil, kamusal aklın sürekliliği açısından da zorunlu bir koşuldur.

Bu çerçevede dijital yurttaşlık, bireyi yalnızca gözetlenen ya da yönlendirilen bir veri noktası olarak değil; kamusal aklın ve ortak iyiliğin taşıyıcısı olarak ele alır. İnsan

---

ahlaksız olacağı anlamına gelmez. Rousseau ayrıca, sistemin bir parçası hâline gelen çıkarcı bilginlerin eserlerinin pek az yarar sağladığını ve kamu kaynaklarını sömürdüklerini ifade eder. Lüks ve konforun yayılmasıyla birlikte toplumsal çürüme artmış, bilim ve sanat bu yozlaşmış düzenin korunmasında bir araç hâline gelmiştir. Rousseau, *Bilimler ve Sanatlar Üzerine Söylev*, s.16-18.

[887] Rousseau, *Bilimler ve Sanatlar Üzerine Söylev*, s.20.

[888] Çalgan, s.188.

[889] Rousseau, *Bilimler ve Sanatlar Üzerine Söylev*, s.10; Mehmet Evren, "Jean Jacques Rousseau'da Bilim ve Sanatın Yeri", **Tabula Rasa Felsefe & Teoloji Dergisi**, No.35, (2020), s.10-11.

[890] Çalgan, s.80-82.

[891] Şenel, s.134.

odaklı yaklaşım, dijital düzenin merkezine algoritmik kâr maksimizasyonunu değil; hesap verebilirlik, katılımcılık ve etik dengeyi yerleştirmeyi gerektirir. Rousseau'nun özgürlük anlayışı burada yeniden anlam kazanır: Özgürlük, bilinçli, aktif ve eşit katılıma dayanır; bireyi pasifleştiren ve veriye indirgenen bir yönetim rasyonalitesini dışlar[892]. Bu nedenle davranışsal yönlendirmeye dayalı dijital yönetim biçimleri, Rousseau'nun özgürlük ve ahlaki sorumluluk ilkeleriyle yapısal bir gerilim içindedir.

Rousseau'nun "İnsan özgür doğar, oysa her yerde zincire vurulmuştur" ifadesi[893] bugün algoritmalar, gözetim sistemleri ve veri sömürüsüyle örülen görünmez zincirleri betimleyen güçlü bir metafora dönüşmektedir. Özgürlüğünden vazgeçmeyi insanlıktan vazgeçmekle eş tutan Rousseau'nun çizdiği hatta, insan odaklı dijital toplum hedefi, bireyin özgürlüğünü yok etmeden kolektif düzeni koruyacak yeni bir dijital toplumsal sözleşme ihtiyacını gündeme getirir[894]. Böyle bir sözleşme, bireyin verileri ve dijital kimliği üzerinde denetimini sürdürmesini; yönetimin ise şeffaf, katılımcı ve hesap verebilir mutabakat süreçleriyle meşrulaşmasını esas almalıdır.

İnsan odaklı yaklaşım, dijitalleşmeyi tahakküm ve sömürü aracı olmaktan çıkararak insan onurunu, özgürlüğünü ve özerkliğini güçlendiren bir toplumsal düzenin hizmetine yerleştirir. Bu doğrultuda dijital sistemler ve algoritmik karar mekanizmaları, bireyi denetleyen gizli iktidar araçları olarak değil; şeffaf, denetlenebilir ve temel haklara saygılı yapılar olarak tasarlanmalıdır. Dijitalleşmenin insan merkezli yorumu, verinin metalaştırılmasına ve bireyin araçsallaştırılmasına sınır çizerken, teknolojik ilerlemenin erdem, adalet ve ortak iyilik temelinde toplumsal değer üretmesini hedefler[895].

Sonuç olarak dijital çağda özgürleşme, teknolojinin kendisinden ziyade onu yöneten zihniyetin dönüşümüne bağlıdır[896]. Rousseau'nun erdem ve özgürlük merkezli uyarıları, dijital tahakküm karşısında insanlığın yeniden düşünmesi gereken normatif bir yol haritası sunmaktadır. Bu bağlamda dijital düzen tartışması, jeopolitik ve rejim tipleri

---

[892] Kriegel, s.142-145.
[893] Jean Jacques Rousseau, **Toplum Sözleşmesi**, İstanbul: Türkiye İş Bankası Kültür Yayınları, 2012, s.4.
[894] Akın, *Devlet Doktrinleri*, s.138; Şenel, s.361-362.
[895] Ergül, Ergin, **Yapay Zekâ ve Hukuk,** Ankara: Adalet Yayınevi, 2025. s.208-210.
[896] Çalgan, s.85.

bakımından da bir yol ayrımına işaret eder: Çin'in otoriter dijital yönetişim modeli ile ABD merkezli kâr odaklı serbest internet yaklaşımı arasında, insan haklarına dayalı üçüncü bir yol mümkündür[897]. Siyasal liberalizm her ne kadar eşitlik temelli hukuksal liberalizme dayanır görünse de uygulamada o, liberalizmin öbür yüzü olan ve vahşi kapitalizmi besleyen eşitsizlikçi ekonomik liberalizmin cilasıdır[898]. Bu nedenle üçüncü yol, demokratik devletler ile teknoloji şirketleri arasında şeffaflık, hesap verebilirlik, veri koruma ve ifade özgürlüğü temelinde kurumsal iş birliğini; yapay zekâ dâhil dijital teknolojilerin küresel ölçekte insan hakları ekseninde yönetilmesini zorunlu kılar[899]. Böyle bir perspektifte dijitalleşme, insanın haysiyetini zayıflatan bir kader değil; insan onuruna uygun bir dijital düzenin inşası için yeniden tasarlanabilir bir toplumsal proje hâline gelir.

Bu çerçevede insan merkezli bir dijital düzenin asgari ilkeleri şöyle formüle edilebilir:

(i) Kuvvet yerine hakka dayalı dijital yönetim mekanizmalarının kurulması,

(ii) Özgürlükleri koruyan şeffaf ve katılımcı dijital sözleşmelerin geliştirilmesi,

(iii) Algoritmik sistemlerin platform çıkarına değil kamu yararı ve adalet ilkesine göre tasarlanması.

---

[897] European Council, "The Digital in a fractious world: Europe's way - Speech by President Charles Michel at the FT-ETNO Forum," 29 Eylül 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/pdf (E.T.: 1 Şubat 2026).

[898] Özlem, s.93.

[899] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.232; Dijital karşılıklı bağımlılık çağında BM, dijital teknolojilerin insan haklarına dayalı bir zeminde gelişmesi ve tüm bireyler ile uluslar için fırsatlar sunması amacıyla dijital iş birliği çağrısında bulunmaktadır. Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.231. Ortak değerleri savunmak, açık interneti korumak, dezenformasyonla mücadele etmek ve siber güvenliği sağlamak için demokratik ülkeler teknoloji şirketleriyle iş birliği yapmalı, insan hakları, veri koruması, şeffaflık ve hesap verebilirliğe dayalı teknik standartlar geliştirmelidir. Christakis, s.87. Bu çerçevede; siber güvenlik, yasa dışı içerikle mücadele, ifade özgürlüğü, bilgiye erişim ve küresel normların oluşturulması gibi alanlarda ortak hareket edebilirler. Örneğin yapay zeka kullanımını desteklemek için Global Partnership on Artificial Intelligence gibi oluşumlar, benzer düşüncedeki ülkelerle oluşturulabilir: Government of Canada, "Joint Statement from founding members of the Global Partnership on Artificial Intelligence", 2020, https://www.canada.ca/en/innovation-science-economic-development/news/2020/06/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence.html (E.T.: 1 Şubat 2026);

III. ÜLKE UNSURU: DİJİTALLEŞMENİN MEKÂN VE SINIR KAVRAMINA ETKİSİ

A. Ülkenin Modern Siyasi Bir Değer Olarak Vatana Dönüşümü

Modern devlet kuramında ülke, egemenliğin icra edildiği sınırları belirli fizikî mekân olarak devletin kurucu unsurlarından biridir. Ülke, yalnızca coğrafi bir alan değil; devlet hukukunun geçerlilik sahasını, kamu gücünün uygulanabildiği yetki çerçevesini ve devlet-birey ilişkisinin kurulduğu mekânsal zemini ifade eder[900]. Bu yönüyle insan ve egemenlik unsurlarıyla birlikte, devletin maddî ve kurumsal varlığını mümkün kılan zorunlu koşuldur[901].

Ülkenin modern devlet açısından belirleyici önemi, ülkesellik ilkesinin egemenlik teorisindeki merkezi konumundan kaynaklanır. Devlet, belirli bir ülke üzerinde münhasır ve üstün otorite kurabildiği ölçüde içsel egemenliğini tesis eder; bu yetkinin dış müdahalelere kapalı olduğunu ileri sürerek dışsal egemenliğini de uluslararası alanda tanımlar[902]. Bu nedenle aynı coğrafi alan üzerinde birden fazla siyasal otoritenin egemenlik iddiasında bulunması, devletin hukuki ve siyasal varlığını doğrudan tehdit eden bir durum olarak değerlendirilir[903]. Devletin ülkesini savunma ve koruma yetkisi, devletler hukukunda, ülke üzerindeki tüm özel mülkiyet ilişkilerini kuşatan ve onlara üstün gelen bir egemenlik hakkı olarak kabul edilir[904]. Bu üstünlük, devletin ülke üzerindeki egemenliğinin hukuki ve siyasal sonucudur[905].

---

[900] Recai Okandan, "Devletin Fiziki Unsuru", **Journal of Istanbul University Law Faculty,** Cilt.14, Sayı.1-2, (Eylül 2011), s.183-188. Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.15; Başgil, *"Devletin Ülke Unsuru",* s.1267.

[901] Okandan, *"Devletin Fiziki Unsuru",* s.162; Ali Fuad Başgil, "Devletin Ülke Unsuru", **İstanbul Hukuk Mecmuası,** Cilt.3, Sayı.4, (1947), s.1262.

[902] Wolfgang H. Reinicke, **Global Public Policy: Governing without Government?,** Washington, D.C.: Brookings Institution Press, 1998, s.58.

[903] Okandan, *"Devletin Fiziki Unsuru",* s.173.

[904] Pehlivan, s.12.

[905] Okandan, *"Devletin Fiziki Unsuru",* s.193.

Modern devleti önceki siyasal örgütlenme biçimlerinden ayıran temel özelliklerden biri, sınırları açık biçimde tanımlanmış bir toprak[906] parçası üzerinde mutlak egemenlik iddiasında bulunmasıdır. Kara ülkesi esas olmak üzere deniz yetki alanları, hava sahası ve yer altı kaynakları bu egemenlik alanının kapsamına dâhildir[907]. Devlet hukukunun kural olarak ülke sınırları içinde uygulanması, sınır kavramına yalnızca coğrafi değil, aynı zamanda kurucu bir siyasal anlam kazandırır. Sınır, bu bağlamda, kamu gücünün geçerlilik alanını belirleyen ve egemenliği somutlaştıran temel yetki çizgisidir[908].

Ülke, devletin egemenliğini kullandığı mekân olarak vatandaş-yabancı ayrımını, hukuki statüleri ve normatif düzeni görünür kılar. Devlet ile birey arasındaki hukuki ilişkinin kurulması ve sürdürülmesi bu belirli mekân üzerinde mümkün olur[909]. Bu nedenle ülke, yalnızca egemenliğin konusu değil; aynı zamanda hukuk düzeninin mekânsal çerçevesidir. Egemenlik, ancak sınırları belirli bir toprak üzerinde hukukî anlam kazanır; bu toprak, hâkimiyetin etki alanını ve sınırlarını tayin eder. Ülkenin kaybı, egemenliğin icra edileceği alanın ortadan kalkması nedeniyle devletin varlığının sona ermesi sonucunu doğurur[910].

Bu hukuki ve siyasal çerçeve, modern dönemde yalnızca ülke kavramını değil, vatan fikrini de üretmiştir. Ulus-devlet, iktidarını kişisel sadakat ilişkilerinden koparark soyut bir egemenlik ilkesine dayandırırken, bu soyut iktidarı her zaman somut bir toprak parçası üzerinde icra eder[911]. Toprağın bütüncül biçimde kavranarak "vatan" adıyla siyasal bir değere dönüştürülmesi, egemenliğin sürekliliğini, meşruiyetini ve siyasal aidiyeti mümkün kılar[912]. Bununla birlikte vatan, salt fizikî bir toprak parçasına

---

[906] Her ne kadar ülke kavramı zaman zaman toprak kavramıyla eş anlamlı kullanılsa da hava sahası, deniz yetki alanlarını ve siber alemi tam olarak kapsayamaması nedeniyle toprak kavramı ülke kavramını karşılamakta yetersiz kaldığından devletin mekânsal temelini açıklarken ülke kavramının tercih edilmesi daha isabetlidir.
[907] Pierson, s.27-28.
[908] Akad, Dinçkol ve Bulut, s.126.
[909] Cemil Caca Arslan, s.259-260.
[910] Okandan, *"Devletin Fiziki Unsuru",* s.165-166, 174-175.
[911] Erözden, s.54.
[912] Okandan, *"Devletin Fiziki Unsuru",* s.163-164.

indirgenemez. Tarihsel hafıza, ortak inanç ve idealler, dil, kültür ve medeniyet birikimi, vatanı ülke unsurundan daha geniş ve derin bir siyasal değer hâline getirir[913].

Feodal dönemde siyasal sadakatin kişilere yönelmiş olması zamanla çözülmüş; sadakat, krallığın bütününü temsil eden soyut siyasal varlığa (corpus mysticum) ve onun somutlaştığı vatana yönelmiştir. Askerlik, vergi ve propaganda gibi pratikler, bireylerden bir senyöre değil, bütün bir vatana bağlılık talep eden yeni bir siyasal sadakat rejimi üretmiştir[914]. Bu çerçevede vatan, yalnız korunması gereken bir toprak parçası değil; uğruna fedakârlık yapılan, kutsallık atfedilen bir siyasal değer hâline gelmiştir[915].

Vatanın siyasal değeri, mülkiyet ve istiklâl kavramlarıyla daha da güçlenir. Ülke üzerindeki münhasır egemenlik, yalnızca nüfus üzerinde yetki kurmayı değil; toprak ve kaynaklar üzerinde sürekli tasarruf hakkını da içerir. Bu nedenle ülkeye yönelik saldırı, milletin ortak mülküne yönelmiş sayılır; vatan savunması ise yalnızca toprağın değil, geçmiş kuşakların emeğiyle oluşmuş ortak mirasın ve gelecek kuşakların hakkının korunmasını ifade eder[916]. Bu bağlamda vatan, birlik ve aidiyet kadar özgürlük ve yurttaşlık erdemleriyle de ilişkilendirilmiştir. On sekizinci yüzyıl düşünsel ikliminde vatanın özgürlükle özdeşleştirilmesi, vatanseverliği siyasal bir yurttaşlık erdemi olarak konumlandırmıştır[917].

Bununla birlikte ülke ve vatan arasındaki ilişkinin doğal değil, siyasal olarak inşa edilmiş bir yapı olduğu vurgulanmalıdır. Mekân, iktidarın toplumsal ilişkileri düzenlemek için kullandığı stratejik bir araçtır; sınırlar, kentler ve yerleşim düzenleri siyasal ve ekonomik ihtiyaçlara göre biçimlendirilir[918]. Fransız Devrimi ile sistematikleşen modern devlet, bölünmemiş toprak parçası üzerinde egemenliği aracısız

---

[913] Başgil, *"Devletin Ülke Unsuru",* s.1264-1265.
[914] Erözden, s.55-62.
[915] Akad, Dinçkol ve Bulut, s.121.
[916] Başgil, *"Devletin Ülke Unsuru",* s.1276-1277.
[917] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.45, 61, 78. Ansiklopedi'de yer alan "özgürlüğün bulunmadığı yer vatan değildir" ifadesi, vatan kavramının modern siyasal düşüncede özgürlükle kurduğu bağı ortaya koymaktadır. Buna göre vatan, özgürlüğün mümkün olduğu siyasal düzenin mekânıyken özgürlük düşüncesine inanmış herkes vatansever olarak kabul edilmiştir. Erözden, s.67.
[918] Henry Lefebvre, "The Production of Space", Jen Jack Gieseking ve Diğerleri (ed.), **The people, place, and space reader** içinde (289-293), New York and London: Routledge, 2014, s.289 vd; Serkan Bulut, s.51.

biçimde kurarken; nüfusu kayıt sistemleri, eğitim, askerlik ve iletişim ağları yoluyla sürekli tanımlamış ve denetlemiştir[919]. Bu saptama, modern devletin mekânsal dayanaklarının sabit olmadığını, küreselleşme ve dijitalleşmenin etkisiyle dönüşüme açık bir yapı sergilediğini ortaya koyan temel bir çıkış noktasıdır.

B. Küreselleşmenin Devletin Ülkesel Sınırlarına Etkisi: Post-Territorial Tartışma

Ulus-devletin tarihsel gücü ve işlevselliği, büyük ölçüde kendi toprakları üzerindeki egemenlik yetkisini etkin biçimde kullanabilmesine dayanmıştır. Siyasal otorite, belirli bir ülke ile özdeşleşmiş; hukukun geçerliliği, kamusal düzen ve demokratik temsil, bu mekânsal çerçeve içinde kurulmuştur[920]. Buna karşılık küreselleşme, mekânın sabitliğini aşındıran, yer kavramını soyutlaştıran ve siyasal, ekonomik ve kültürel süreçleri sınır aşan ağlar üzerinden yeniden örgütleyen bir dinamik olarak ortaya çıkmıştır. Bu yönüyle küreselleşme, klasik ulus-devlet modelinin ülkesel sınırlarını doğrudan sorgulayan yapısal bir meydan okuma niteliği taşımaktadır.

Küreselleşme literatüründe bu dönüşümü açıklamak üzere farklı yaklaşımlar geliştirilmiştir. Ulus-ötesicilik, ekonomik ve siyasal süreçlerin sınırları aşarak örgütlendiğini kabul etmekle birlikte, bu süreçlerin hâlen büyük ölçüde ulus-devletler aracılığıyla işlediğini savunur. Devletler, küresel ağların dışında kalan edilgen yapılar değil; bu ağları düzenleyen, yönlendiren ve çoğu zaman yeniden şekillendiren aktörlerdir. Yerel-ötesi etkileşim perspektifi ise küresel ve yerel düzlemler arasında gelişen, çoğu zaman merkezî devlet düzenlemelerini aşan çok yönlü ilişkiler ağına odaklanır. Yerel aktörlerin doğrudan sınır aşan bağlantılar kurabilmesi, ülkesel sınırların anlamını dönüştürmekte; ancak bu durum devletin varlığını ortadan kaldırmaktan ziyade, egemenliğin kullanım biçimlerini karmaşıklaştırmaktadır[921].

Bu yaklaşımlar, küreselleşmenin çok katmanlı yapısını görünür kılsa da ortak bir sınırlılık taşır: Devletin günümüzde hâlen elinde tuttuğu siyasal ve zorlayıcı kapasiteyi

---

[919] Hobsbawm, s.102-104.
[920] Akdenizli, s.41.
[921] Dirlik, *Küreselleşmenin Sonu Mu?,* s.58-59.

açıklamakta yetersiz kalmaları. Zira beklentinin aksine küreselleşme, birçok bağlamda devletleri zayıflatmamış; aksine devletleri reaksiyon göstermeye zorlayarak sınır güvenliğinin sertleşmesine, göç ve güvenlik politikalarının yoğunlaşmasına ve milliyetçi söylemlerin yeniden güç kazanmasına yol açmıştır. Küresel süreçler, evrensel ve tek yönlü sonuçlar üretmemekte; her devletin tarihsel, siyasal ve toplumsal bağlamına göre farklılaşan etkiler doğurmaktadır.

Bu çerçevede çağdaş siyasal düzenin temel çelişkisi belirginleşmektedir: Küresel modernite, sınırları bir yandan aşındırırken, diğer yandan onları yeniden tahkim etmektedir. Zayıflayan unsur devletin kendisi ya da ulus kavramı değil; devlet ile ulusun mekânsal olarak birebir örtüştüğü klasik ulus-devlet modelidir. Devlet, giderek yalnızca ulusun siyasal temsilcisi olmaktan çıkmakta; küresel ve ulus-ötesi güçlerin yarattığı çelişkileri yöneten karmaşık bir yönetsel aygıta dönüşmektedir. Bu dönüşüm, devletin idari ve güvenlik kapasitesini güçlendirebilirken, ulusla kurduğu temsil ilişkisini daha kırılgan ve tartışmalı hâle getirmektedir[922].

Sermayenin ve üretim ilişkilerinin küreselleşmesine rağmen ulus-devletin ortadan kalktığına ya da geçici bir örgütlenme biçimi olduğuna dair ikna edici bir kanıt bulunmamaktadır. Ulus-devlet, devletin tarihsel biçimlerinden yalnızca biridir; dönüşmesi, devletin sona ereceği anlamına gelmemekte, aksine egemenliğin yeni ölçekler ve araçlar üzerinden yeniden örgütlenebileceğine işaret etmektedir. Benzer biçimde ulusçuluk da iki yüzyıllık geçmişine rağmen, küresel ve yerel siyasal süreçleri etkileyen güçlü bir aidiyet ve meşruiyet kaynağı olmaya devam etmektedir[923].

Bu bağlamda günümüzdeki asıl sorun, ulus-devletin çöküşü değil; devletin ulusu temsil etme iddiasının zayıflamasıdır[924]. Modern demokrasilerin kurucu ilkelerinden biri olan yöneten-yönetilen özdeşliği, ulus-devletin mekânsal bütünlüğüne dayanır. Ancak karar alma merkezlerinin giderek ulus-aşırı ölçekte örgütlenmesi, bu özdeşliği

[922] Dirlik, *Küreselleşmenin Sonu Mu?,* s.60.
[923] Dirlik, *Küreselleşmenin Sonu Mu?,* s.76-77.
[924] Kalkınma ve küresel rekabet gerekçeleriyle devletin belirli çıkar gruplarıyla özdeşleşmesi, toplumsal temsil krizini derinleştirmektedir. Devletin bu krize verdiği yanıt ise, gözetim ve denetimin artırılması, temel haklarının daraltılması gibi baskıcı uygulamaların yoğunlaşması olmuştur. Sonuçta vatandaşlığın zayıflaması, demokrasinin doğrudan tehlikeye girmesine yol açmaktadır. Dirlik, *Küreselleşmenin Sonu Mu?,* s.123-124.

aşındırmakta; çok uluslu şirketler, küresel finans merkezleri ve çok taraflı yönetişim yapıları, yerel halkın siyasal denetiminin dışında işleyerek temsil krizini derinleştirmektedir[925].

Sonuç olarak küreselleşme, ulus-devleti ortadan kaldıran bir süreçten ziyade, onun mekânsal ve siyasal mantığını dönüştüren bir dinamik olarak değerlendirilmelidir. Ülkesel sınırlar anlamını yitirmemekte; ancak egemenliği tek başına açıklamaya yetmeyen bir çerçeve hâline gelmektedir. Egemenlik, artık yalnızca toprak merkezli bir ilişki olarak değil; farklı mekânsal ölçekler, akışlar ve etkileşim biçimleri üzerinden yeniden düşünülmek zorundadır. Bir sonraki bölümde ele alınacak olan dijitalleşme olgusu, bu dönüşümün en ileri ve en zorlayıcı aşamasını oluşturarak, post-territoryal tartışmayı yeni bir düzleme taşımaktadır.

C. Dijitalleşmenin Egemenliğin Mekânsal Temelini Dönüştürmesi

Dijitalleşme, modern devletin egemenliğini somutlaştıran ülke unsurunu ortadan kaldırmamakta; ancak egemenliğin tarihsel olarak dayandığı analog ve toprak merkezli mekânsallığı dolaylı biçimde aşındırmaktadır. Devlet, varlığını sürdürebilmek için hâlen sınırları belirli bir toprak parçasına ihtiyaç duysa da dijital teknolojiler, egemenliğin yalnızca fizikî mekân üzerinden açıklanmasını giderek yetersiz hâle getirmektedir. Bu nedenle dijitalleşme, ülke unsurunu işlevsizleştiren değil; onu yeni, hibrit ve çok katmanlı bir egemenlik zemini içinde dönüştüren bir süreç olarak değerlendirilmelidir.

Ulus-devlet, egemenliğini vatan olarak kavramsallaştırılan muayyen bir toprak parçası üzerinde kurarken, dijital platformlar fizikî sınırlara bağlı olmaksızın faaliyet göstermektedir. Bu durum, klasik ülkesellik ilkesinin pratik belirleyiciliğini zayıflatmakta ve dijital faaliyetlerin hangi hukuk düzenine tâbi olacağı sorununu sürekli ve yapısal hâle getirmektedir. Böylece dijitalleşme, modern devletin mekânsal temelini doğrudan hedef almadan, analog egemenlik kurgusunu dolaylı yoldan aşındırmaktadır.

---

[925] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.82.

Toprak temelli egemenlik; ölçek ve savunulabilirlik gibi coğrafi sınırlamalara tabidir. İnsanlar, kaynaklar ve siyasal iktidar, doğal engellerle bölünmüş fizikî alanlar üzerinde dağılmıştır. Buna karşılık dijital mekân, yoğunlaşmış ve sınır tanımaz bir etkileşim alanı sunarak coğrafi ayrımları büyük ölçüde anlamsızlaştırmaktadır. İnternet altyapısı, bulut bilişim sistemleri, veri merkezleri ve ağ mimarileri, devletlerin doğrudan denetim kurmakta zorlandığı yeni bir dijital uzam yaratmakta; bu uzam, klasik anlamda sınır çizilebilen mekân anlayışını belirsizleştirmektedir[926].

İnternet ve ona bağlı teknolojiler, ulus-devletlerin kendi ülke sınırları içinde bilgi ve haber akışını denetleme kapasitesini önceki iletişim teknolojilerine kıyasla çok daha derin biçimde aşındırmaktadır. Dijital içerikler, belirli bir ülke toprağına bağlı olmaksızın anında küresel dolaşıma girebilmekte; böylece bilgi akışı, ülke unsuru üzerinden kurulan geleneksel denetim ilişkilerinden büyük ölçüde kopmaktadır[927]. Bu kopuş, egemenliğin yalnızca nerede kullanıldığı değil, nasıl tesis edildiği sorusunu da merkeze taşımaktadır.

Dijital alandaki bu durum sıklıkla "Vahşi Batı" metaforuyla açıklansa[928] da daha isabetli bir benzetme, toplum sözleşmesi öncesi doğa durumudur. Çünkü dijital ortam tek bir bütünsel sistem içerisinde olmadığından hem koruyucu otorite belirsizdir hem de denetleyen aktörler çoğu zaman denetlenememekte olduğundan düzen öncesi ontolojik bir kaos bulunmaktadır. Siber saldırılar, dezenformasyon, deepfake içerikler ve çevrim içi taciz gibi olgular, bireyleri dijital alanda sistematik hak ihlallerine açık hâle getirmektedir. Bu tablo, dijital güvenliğin kolektif bir düzenleyici otorite olmaksızın sağlanamayacağını göstermektedir.

Bu noktada Hobbes'un doğa durumu tasviri açıklayıcıdır: Güvenliğin yokluğu, bireyleri haklarını devrederek koruyucu bir egemenlik düzeni kurmaya sevk eder[929]. Spinoza'nın yaklaşımı ise dijital bağlamda hak ile güç arasındaki ilişkiyi görünür kılar[930]. Dijital ortamda hak, çoğu zaman kullanıcının teknik, bilişsel ve erişim kapasitesiyle

[926] Lehdonvirta, s.128.
[927] Akdenizli, s.42.
[928] Bu metafor; özellikle bir platformdan kaldırılan içeriğin başka bir platformda kolaylıkla yeniden dolaşıma girebilmesinin yaygınlığı üzerinden somutlaşmaktadır. Işık, s.33.
[929] Akad, Dinçkol ve Bulut, s.106-108.
[930] Kriegel, s.40-45, 71.

sınırlı kalmakta; güçlü aktörler zayıflar üzerinde fiilî bir tahakküm kurabilmektedir. Bu nedenle sorun, dijital alanda kendiliğinden bir egemenliğin ortaya çıkmasını beklemek değil; bu alanın hangi aktörler tarafından, hangi araçlarla ve hangi meşruiyet zemininde düzenleneceğinin belirlenmesidir[931].

Bu bağlamda ülke unsuru, klasik anlamıyla ortadan kalkmamakta; dijital alanı da kapsayan hibrit bir egemenlik zeminine dönüşmektedir[932]. Bilgi akışının denetlenmesi, veri trafiğinin izlenmesi ve içerik erişiminin sınırlandırılması gibi uygulamalar, dijital mekânı devletin güvenlik ve egemenlik politikalarının merkezine yerleştirmektedir. Böylece egemenliğin mekânsal boyutu, fizikî ülkenin ötesine taşarak dijital uzama doğru genişlemektedir. Dijitalleşme, devlete yalnızca sınır aşındıran bir süreç sunmamış; aynı zamanda dijital alanlarda yeni sınırlar inşa etme imkânı da tanımıştır. Gourley'e göre devlet, egemenliğini iki ilkeye dayandırır: sınırları içindeki ve sınırlarını aşan işlemler üzerinde denetim hakkı (toprak esaslılık) ile dışarıda gerçekleşip ülke içinde etkisi olan olaylara müdahale hakkı (etki ilkesi). Dijital alan fiziksel bir yer olmasa da altyapısının gerçek mekânlara bağlı olması nedeniyle bu alandaki unsurlar da bulundukları ülkenin hukukuna tâbidir. Bu yaklaşım, siber uzayın da egemenlik alanının bir parçası olarak görülmesini mümkün kılmaktadır[933].

Postmodern bağlamda dijitalleşme, devletin coğrafi tabanını kaydırmakta; ülke unsurunu sanal biçimde yeniden üretmektedir. Fransa Anayasa Konseyi'nin WebGroup/Xnxx[934] ve Coyote System[935] kararları, dijitalleşmenin ülke unsuru

---

[931] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.75.

[932] Benjamin H. Bratton, **The Stack: On Software and Sovereignty,** Massachusetts: The MIT Press Direct, 2016, s.111.

[933] Stephen K. Gourley, "Cyber Sovereignty", Panayotis A. Yannakogeorgos ve Adam B. Lowther (Ed.), **Conflict and Cooperation in Cyberspace: The Challenge to National Security** içinde (277-290), Florida: Taylor & Francis, 2014, s.279.

[934] WebGroup/Xnxx davasında Fransa, çocukları müstehcen içeriklerden korumak amacıyla, Çekya merkezli bir dijital platforma kendi ceza yasalarını uygulamaya çalışmıştır. Ancak bu girişim, Avrupa Birliği'nin E-Ticaret Direktifi'nde yer alan 'orijin ülke' ilkesine aykırıdır. Fransa, çocukların korunması ve kamu düzeni gerekçesiyle bu ilkeye istisna getirilmesini savunmuştur. Bu durum, egemenliğin yalnızca fizikî toprakla değil, dijital erişimin etkilediği kullanıcı kitlesiyle de tanımlanması gerektiğini göstermektedir.

[935] Conseil d'État, Coyotte System; Société Webgroup Czech Republic et autre, Décision n° 453763 (jonction des N°s 461193 et 461195), 4e chambre jugeant seule, séance du 7 février 2024, décision du 6 mars 2024, ECLI: FR:CECHR:2024:453763, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-03-06/453763 (2 Şubat 2026). Coyote System davasında Fransa, karayolu güvenliği amacıyla, navigasyon uygulamalarının polis kontrol noktalarını

üzerindeki dönüştürücü etkisini açık biçimde ortaya koymaktadır. Bu davalar, egemenliğin yalnızca fizikî toprakla değil, dijital hizmetlerin etkilediği kullanıcı kitlesiyle de tanımlandığını göstermektedir. Devletlerin dijital platformları düzenleme çabaları, egemenliğin klasik sınırların ötesine geçerek dijital alanda yeniden tanımlandığını ortaya koymaktadır.

Dijital alanın fizikî mekânın bir uzantısı olarak ele alınması, devletin etki alanını genişleterek dijital ilişkiler üzerinde egemenlik kurmasına imkân tanımaktadır[936]. Devletler, bilgi akışını denetleyerek, erişimi kontrol ederek ve dijital düzenleme araçları geliştirerek bu yeni alanda egemenliklerini yeniden inşa etmektedir[937]. Güvenlik duvarları, veri yerelleştirme yükümlülükleri, ulusal ağ altyapıları ve internet kesintileri, devletin ülkesi üzerindeki dijital egemenliğin araçsal yeni görünümleridir.

Bu dönüşümün en somut görünümlerinden biri, internetin ulusal sınırlar temelinde yeniden yapılandırılmasıdır. "Splinternet/internetin balkanlaşması/parçalanması" olarak adlandırılan bu süreç, dijital alanın küresel ve sınırsız doğasına karşılık, devletlerin kendi normatif düzenlerine uygun dijital sınırlar inşa etmesini ifade eder[938]. Coğrafi erişim engellemeleri (geo-blocking), veri yerelleştirme yükümlülükleri ve ulusal ağ altyapıları, dijital ülkeselliğin dijital teknik araçları hâline gelmiştir.

---

bildirmesini yasaklamıştır. Bu kez hizmet sağlayıcısı Fransa'da faaliyet gösterdiği için, klasik ülke unsuru doğrudan geçerli olmuştur. Ancak bu düzenleme, dijital hizmetlerin iletişim özgürlüğü gibi temel haklar ile çelişebileceğini de ortaya koymuştur.

[936] Carwyn Morris, Andy Hanlun Li ve Lotus Ruan, "Covid origins, nationalism, and diasporic heterogeneity: China, Chineseness, and Covid-19", Michael Butter ve Peter Knight (Ed.), **Covid Conspiracy Theories in Global Perspective**, içinde (43-57), London: Routledge, 2023, s.43.

[937] Küzeci, s.437.

[938] Küzeci, s.447, 448.

Çin'in küresel platformlara erişimi tamamen kapatması[939] BAE'nin VoIP hizmetlerini sınırlaması[940] Türkiye'nin belirli içeriklere yurtdışından erişimi engellemesi[941] ve Tayvan[942] ile Avustralya'nın güvenlik gerekçeli coğrafi filtreleri[943] bu eğilimin farklı politik amaçlarla nasıl kullanıldığını gösterir. Bu uygulamalar, bilgiye erişim ve ifade özgürlüğü açısından ciddi sorunlar doğurmakla birlikte, yeni bir kamusal idare alanı ortaya çıkararak egemenliğin dijital boyutunun giderek güçlendiğini de göstermektedir. Fakat küresel internetin açık yapısının zayıflamasına ve parçalanmasına da katkı sunduğundan, uluslararası hukuk düzenlemelerine duyulan ihtiyacı ortaya koymaktadır[944].

Işık'a göre, var olan bu olguyu "parçalanma" olarak algılamak hatalı bir yaklaşımdır. Çünkü internet kelime anlamı ile ağlar arası anlamına gelir ve bilgisayarların birine bağlanmasını ifade eder. Oysa ağlar arası bağlantı sona erdiğinde bir fragmentasyon ya da parçalanma değil birbirinden bağımsız ağlar ortaya çıkar. Bağlantılı bilgisayar sayısı azalacağından oluşan durum aslında bilinen internetin ulusal sınırlar ölçeğinde küçülerek bir Siber Vestfalya'nın yani birden fazla internetin ortaya

---

[939] Çin'in Great Firewall mekanizması kapsamında, Facebook, Twitter ve Google gibi uluslararası dijital platformlara ülke içinde erişim tamamen engellenmesi bireylerin ifade özgürlüğü ve serbest bilgi akışı haklarını doğrudan sınırlamaktadır. Paul Roberts, "China's Great Firewall Being Turned Against Facebook, Google, and Twitter," Threatpost, 18 Kasım 2011, https://threatpost.com/chinas-great-firewall-being-turned-against-facebook-google-and-twitter-111811/75912/ (E.T.: 1 Şubat 2026).

[940] Birleşik Arap Emirlikleri'nin ulusal telekomünikasyon sektörünü koruma gerekçesiyle Skype ve WhatsApp gibi VoIP hizmetlerine erişimi sınırlandırması dijital hizmet sağlayıcılar arasında ticari ayrımcılığa ve rekabetin kısıtlanmasına yol açabilmektedir. Wired.me, "UAE alternatives to banned Skype calls," https://wired.me/technology/uae-alternatives-banned-skype-calls/ (E.T.: 1 Şubat 2026).

[941] Human Rights Watch (HRW), "Questions and Answers: Turkey's Control of the Internet and Upcoming Election," 10 Mayıs 2023, https://www.hrw.org/news/2023/05/10/questions-and-answers-turkeys-control-internet-and-upcoming-election (E.T.: 1 Şubat 2026). Coğrafi erişim engellemeleri hem yurtiçi hem de yurtdışında bulunan bireylerin bilgi edinme hakkını sınırlayabilmektedir. Örneğin, Türkiye'de TRT ve Tabii gibi devlete ait dijital platformlara ve bazı kamu kurumlarının hizmetlerine yurt dışından erişim sınırlandırılmaktadır. Bu durum, yurtdışındaki vatandaşlar açısından anayasal düzeyde korunan iletişim ve bilgi edinme özgürlüğü ile çelişebilme potansiyeli taşımaktadır.

[942] Tayvan, Çin kaynaklı dijital içeriklere karşı coğrafi kısıtlamalar uygulayarak propaganda faaliyetlerine karşı önlem almaktadır. Deutsche Welle, "How Taiwan is countering Chinese disinformation," 25 Ağustos 2022, https://www.dw.com/en/how-taiwan-is-countering-chinese-disinformation/a-62931086 (E.T.: 1 Şubat 2026).

[943] Avustralya, özellikle çocukların zararlı içeriklere erişimini engellemek amacıyla kumar ve medya sitelerine coğrafi erişim kısıtlamaları getirmektedir. eSafety Commissioner (Australia), "eSafety Statement: National age restrictions for digital platforms," https://www.esafety.gov.au/newsroom/media-releases/esafety-statement-national-age-restrictions-for-digital-platforms (E.T.: 1 Şubat 2026).

[944] Alkan Altaş, "Özgürlük ve Egemenlik Arasında 'Bölünmüş İnternet'", (**Yüksek Lisans Tezi,** İstanbul Medeniyet Üniversitesi Lisansüstü Eğitim Enstitüsü, 2024), s. 38.

çıkmasıdır[945]. Çin ve Rusya örneklerinde görüldüğü üzere, dijital alanın millîleştirilmesi yönündeki uygulamalar, devletlerin dijital ülke unsuru üzerindeki egemenlik iddialarını güçlendirmektedir[946]. Bu çerçevede dijital vatandaşlık, ulusal pasaport vb. erişim izinleri ve içerik kontrol mekanizmaları ile desteklenerek, dijital ülke unsuru üzerindeki egemenlik pekiştirilmektedir.

Ancak bu dönüşüm, dijital egemenliğin tam anlamıyla tesis edildiği anlamına gelmemektedir. Dijitalleşme, yalnızca teknolojik bir ilerleme değil; aynı zamanda kültürel, toplumsal ve siyasal yapıları yeniden biçimlendiren kapsamlı bir dönüşümdür. Bu yeni düzende egemenliğin klasik mekânsal temelleri aşındıkça, devletin hem içsel hem de dışsal egemenlik iddiası zayıflamakta; kamu gücü giderek daha fazla dijital ağlara ve bu ağları kontrol eden devlet dışı aktörlere bağımlı hâle gelmektedir[947]. Böylece egemenlik, sabit bir ülke üzerinde kullanılan mutlak bir yetki olmaktan uzaklaşarak akışkan ve dağınık açık bir nitelik kazanmaktadır. Bu bağlamda post-territorial dönüşümün en kritik sonucu, egemenliğin artık yalnızca devletler arasında değil; devletler, küresel teknoloji şirketleri ve algoritmik sistemler arasında paylaşılan bir güç ilişkisine dönüşmesidir. Dijital imparatorluklar, klasik meşruiyet mekanizmalarına dayanmaksızın veri ve davranış denetimi üzerinden fiilî iktidar kurmaktadır.

Dijital alan her ne kadar maddesel olmasa da sunucular, kablolar ve enerji kaynakları gibi fiziksel altyapılara dayanır. Bulut bilişim gibi çok merkezli yapılar, verilerin farklı ülkelerde tutulmasına neden olarak toprak esaslı egemenlik anlayışıyla çelişmekte ve veri egemenliği sorununu gündeme getirmektedir. Kritik kamu verilerinin ulusal sınırlar içinde tutulması yönündeki eğilim, egemenliğin dijital bağlamda yeniden tanımlandığını göstermektedir[948]. Verilerin başka bir ülkenin yargı yetkisine girmesi hukuki sorunlar doğurmaktadır. Her ne kadar teknoloji şirketleri faaliyetlerini sürdürebilmek ve uyuşmazlıkları çözmek için devletin hukuk sistemine başvurmak

[945] Işık, s.51.
[946] Roberts ve Diğerleri, s.13.
[947] Kristina Irion ve Diğerleri, "Governing 'European values' inside data flows: Interdisciplinary perspectives", **Internet Policy Review,** Vol.10, No.3, (2023), s.3.
[948] Irion, *"Government Cloud Computing and National Data Sovereignty",* s.65.

zorunda olsa da bu alanda siber ilişkileri ve uluslararası dijital ticareti düzenleyecek yeni bir hukuki çerçeveye ihtiyaç duyulmaktadır[949].

Uluslararası hukukta gerekli özen (due diligence) ilkesi, devletlerin kendi yetki alanları içindeki faaliyetlerin başka devletlere zarar vermesini önleme yükümlülüğünü ifade eder[950]. Bu ilkenin siber uzaya uygulanması; devletlerin kendi dijital altyapılarının ve ülkelerinde faaliyet gösteren platformların sınır aşan zararlı etkiler doğurmasını engelleme sorumluluğunu gündeme getirmektedir. BM Açık Uçlu Çalışma Grubu 2023 Nihai Raporu; bilgi ve iletişim teknolojilerinin kötü niyetli kullanımının barış, güvenlik ve insan hakları için ciddi tehdit oluşturduğunu belirtmiş; devletlere, devlet egemenliği temelinde küresel kritik altyapıyı korumaya yönelik önleyici tedbirler alma yükümlülüğü tavsiye etmiştir[951]. NATO Uzmanlar Grubu'nca 2017'de yayınlanan Tallinn El Kitabı 2.0'de yer verilen 6. ve 7. Kurallar kapsamında, siber alanda normların azlığının hukuki bir boşluk olduğu anlamına gelmediğini belirtmiş; gerekli özen (due diligence) ilkesini siber uzaya uyarlayarak, devletlerin kendi toprakları veya kontrol ettikleri siber altyapının başka devletlere zarar veren siber operasyonlarda kullanılmasını önleme yükümlülüğü bulunduğunu kabul etmiştir[952].

Bu yaklaşım, devletlerin ve özel şirketlerin birlikte aktör hâline geldiği dijital alanlarda da güncelliğini ve önemini korumaktadır. Dijital altyapıların, veri akışlarının ve çevrim içi platformların büyük ölçüde özel şirketlerin kontrolünde bulunmasına rağmen,

---

[949] Gourley, s.280.

[950] Nergiz Emir, "Siber Operasyonlar ve Özen Yükümlülüğünün İhlalinden Devletin Sorumluluğu", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (61-74), İstanbul: Adalet, 2021, s.64. Uluslararası Adalet Divanı (UAD), Korfu Boğazı Davası'nda her devletin kendi topraklarını diğer devletlerin haklarına aykırı eylemler için kullanmasına bilerek izin vermeme yükümlülüğü altında olduğunu ifade etmiştir. International Court of Justice (ICJ), Judgment of 9 April 1949 Corfu Channel Case (Merits), https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf (E.T.: 1 Şubat 2026) s.22.

[951] United Nations General Assembly, A/RES/78/237 Developments in the field of information and telecommunications in the context of international security, 78th Sess., 22 December 2023, https://docs.un.org/en/a/res/78/237 (E.T.: 1 Şubat 2026), s.4.

[952] Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence General Editor Michael N. Schmitt Managing Editor Liis Vihul, Cambridge University Press 2017, https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf

bu alanların devlet egemenliği, kamu düzeni ve temel haklar üzerinde doğrudan etkiler üretmesi, gerekli özen yükümlülüğünün kapsamının yeniden değerlendirilmesini zorunlu kılmaktadır. Bu çerçevede devletler, kendi yetki alanları içinde faaliyet gösteren dijital platformların ve teknoloji şirketlerinin, başka devletlerin haklarını ihlal eden siber faaliyetler, veri ihlalleri veya insan haklarına aykırı uygulamalar bakımından zararlı etkiler doğurmasını önlemek için makul ve öngörülebilir tedbirleri almakla yükümlüdür. Aynı zamanda şirketler açısından da gerekli özen, yalnızca iç hukuk kaynaklı bir yükümlülük olmaktan çıkarak, insan haklarına saygı, veri koruma ve siber güvenlik alanlarında uluslararası normatif beklentilerle şekillenen bir sorumluluk hâline gelmektedir. Bu durum, dijital alanlarda devletlerin düzenleyici ve denetleyici rolü ile şirketlerin operasyonel ve teknik kapasitesi arasında paylaşılan, çok aktörlü bir gerekli özen anlayışının ortaya çıktığını göstermektedir.

Sonuç olarak dijitalleşme, modern devletin ülke unsurunu ortadan kaldıran değil; onu post-territorial bir bağlamda yeniden tanımlayan bir dönüşüm sürecidir. Ülke, artık yalnızca haritalar üzerinde çizilmiş fizikî sınırlarla değil; veri, erişim ve denetim ilişkileri üzerinden kurulan dijital sınırlarla da şekillenmektedir. Egemenliğin ölçütü, toprağın nerede bulunduğundan ziyade, dijital mimarinin kim tarafından tasarlandığı ve kontrol edildiği sorusuna kaymaktadır[953]. Bu durum, ulus-devletin fizikî vatan anlayışını, dijital çağda sınırları koruyacak yeni egemenlik araçları geliştirme zorunluluğuyla karşı karşıya bırakmaktadır. Nitekim dijital çağda iktidar, klasik anlamda rıza ve zorun toplamına dayalı olmaktan çıkarak, mekânsız dijital alanlarda zihinler üzerinde kurulan yeni bir otorite biçimine evrilmektedir. Bu durum, adeta dijital imparatorlukların ortaya çıkışına işaret ettiğinden; ulus-devletin fiziksel vatan anlayışı, dijital çağda sınırları koruyacak dijital altyapılar üzerinden üniter bir dijital egemenlik kurma zorunluluğuna dönüşmektedir[954].

[953] Timmers, *"Sovereignty in the Digital Age",* s.582.
[954] Erözden, s.147-148.

IV. EGEMENLİK 2.0: EGEMENİN DİJİTAL YÜZÜ

A. Dijital Egemenlik ve Dijital Egemen

Dijitalleşme, devlet-hukuk-siyaset ilişkisini yalnızca teknik düzeyde değil, aynı zamanda meşruiyet, iktidar ve norm koyma biçimleri bakımından da köklü biçimde dönüştürmektedir[955]. Dijital çağda devletin dönüşen rolünü anlamak, yalnızca dijital egemenlik kavramına odaklanmayı değil; bu egemenliğin kim tarafından, hangi araçlarla ve hangi meşruiyet zemininde kullanıldığını da analiz etmeyi zorunlu kılar. Bu nedenle dijital egemenlik ile dijital egemen kavramları arasında teorik ve işlevsel bir ayrım yapılması gerekmektedir.

1. Dijital Egemenin Meşruiyet Krizi: Toplumsal Sözleşme Kuramlarının Aşılması

Modern siyasal düşüncede meşruiyet, yasa ile uygulama arasındaki ilişkinin kurulma biçimi üzerinden tanımlanır. Bu ilişki, modern toplumda egemenlik kavramı etrafında şekillenmiş ve devletli toplumu ayırt eden temel ölçüt hâline gelmiştir[956]. Klasik egemenlik kuramında egemen, yasayı koyan, değiştiren ve uygulayan tekil otoritedir; bu yetkinin bölünmesi ya da paylaşılması siyasal düzenin çözülmesi anlamına gelir[957]. Bu nedenle egemenliğin mutlak, sürekli ve bölünemez oluşu, modern devlet düşüncesinin kurucu kabullerinden biridir.

Toplumsal sözleşme[958] kuramları, modern egemenliği bireylerin rızasına dayalı bir siyasal, mantıksal ve kuramsal kurgu olarak temellendirir[959]. Hobbes'ta egemenlik, bireylerin güvenlik karşılığında iradelerini devrettikleri yapay siyasal bedenin iradesi olarak yasada somutlaşır. Devlet, daha iyi bir yaşam için aklın tasarladığı yapay bir beden,

---

[955] Küzeci, s.302.

[956] Akal, *Devlet, Yasa, Hakimiyet*, s.22.

[957] Abdurrahman Saygılı, "Jean Bodin'in Egemenlik Anlayışı Çerçevesinde Kralın İki Bedeni Kuramına Kısa Bir Bakış", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.63, Sayı.1, (2014), s.190-191; Uygun, s.211.

[958] Toplumsal sözleşme kuramı modern öncesi dönemde de ileri sürülmüştür: Antik Yunan'da Epiküros, devletin kökenini insanları ortak tehlikeleri önlemek ve daha fazla haz/mutluluk sağlamak için bir araya getiren bir sözleşmeye dayandırır. Şenel, s.179.

[959] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.217.

egemenlik ise bu bedenin ruhudur[960]. Rousseau'da ise yasa, genel iradenin ifadesi olarak aşkın bir meşruiyet düzeyine ulaşır[961]. Her iki yaklaşımda da egemenliğin kaynağı, kolektif rıza ve ortak akıldır[962]. Toplum sözleşmesi kurgusunun içerdiği ortak onay gereklidir, ama siyasal bedeni tam anlamıyla oluşturmaya yeterli değildir. Her birey, kendi iradesini egemenin iradesine bağlı kılmalı; egemenin iradesini kendi iradesi olarak tanımalıdır[963].

Bu kuramsal zeminde modern egemenlik, halk iradesi ve hukuk düzeni üzerine inşa edilmiş bir siyasal örgütlenme biçimi olarak ortaya çıkmıştır. Devlet, meşruiyetini hukuktan ve toplumsal rızadan alır; iktidarını ulus adına kullandığını iddia ederek kendini temellendirir[964]. Salt güç tek başına iktidar oluşturmaz; iktidar, zorlamanın rıza ile kabul edilmesiyle kurulan bir ilişkidir. Baskı, muhatabın bunu meşru ve yararlı görmesiyle tamamlanır. Bu anlamda iktidar, en basitinden en karmaşığına kadar tüm ilişkilerde, zor ile rızanın birleşmesine dayanır[965]. İktidarın sürekliliği, iktidar ilişkisinin baskı ve onay unsurlarını aynı anda içermesin bağlıdır: iktidar ilişkisinin bir tarafı gerekli gördüğünde baskı ve zor kullanır diğer tarafı da buna rıza ve onay gösterir. Baskı salt kaba güç olarak kalmaz, yönetilenler bu gücü çoğunlukla onaylarsa meşru ve sürekli bir iktidardan söz edilir. Gayri meşru siyasal iktidar ancak baskı uygulayan bir güçtür ve kendisine boyun eğilmesini sağlayabildiği sürece var olabilir[966].

Ulus-devlet modelinde bu meşruiyet, "egemenlik ulusundur" ilkesiyle kurumsallaşmıştır: egemenlik; ulus adına kullanılan ve hukuk düzeniyle sınırlandırılmış bir iktidar biçimidir. Akal'a göre, sözleşmeci kuramlar, modern ulus-devlet mantığını kurarak yeni siyasal-hukuki düşünceyi ve onun pozitivist karakterini belirlemiştir. Bu kuramlar, ulusu soyut bir bütün olarak düşünmeyi ve egemenlik kavramını sözleşme mülahazasıyla tamamlayarak ulus-devleti sistemli bir yapı hâline getirmeyi sağlamıştır.

---

[960] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk,* s.25-26.
[961] Drucker, s.23.
[962] Modern siyaset felsefesinde egemenlik, Hobbes ve Rousseau'da halkın rızasına dayalı meşru bir otorite olarak temellendirilir: Hobbes'ta egemenliğin iradesi yasa olurken, Rousseau'da yasa, genel iradenin ifadesidir.
[963] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.217.
[964] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.19.
[965] Akal, *Devlet, Yasa, Hakimiyet*, s.45.
[966] Uygun, s.8.

Böylece insanlar, uymakla yükümlü oldukları düzenin ve yasaların aynı zamanda yaratıcısı olarak kavranmıştır; egemenlik kavramı gerçek anlamını bu sözleşme düşüncesiyle kazanmıştır[967]. Günümüzde toplum sözleşmesi temelli meşruluk anlayışı hala geçerliliğini korumaktadır[968].

Devlet, içerde meşru zor kullanma tekeline, dışarda ise bağımsızlığa sahip "tek" siyasal otorite olarak konumlanır. Egemenliğe sahip olan devlet, toplum içindeki tüm iktidar ilişkilerinin üzerinde yer alır ve kendi ülkesinde rakip kabul etmez. Yasa koyma, para basma, savaş ve barışa karar verme gibi iç egemenlik yetkileri yalnızca egemene aittir; dış egemenliği sayesinde de diğer devletler karşısında bağımsızdır[969]. Sınırlarını ülke unsurunun tayin ettiği bu yetkiler; halkın rızasıyla ve ulus adına meşrulaştırılır[970]. İdeolojik aygıtlar aracılığıyla bireyin bedeni ve düşünce dünyası üzerinde etkili olan bu iktidar biçimi, yurttaşın iradesini devletin kurucu çerçevesi içinde yeniden üretir.

Ancak dijital çağ, bu yerleşik meşruiyet yapısında tarihsel bir kırılma yaratmıştır. Yukarıda gösterildiği üzere ulus, mekân ve yurttaşlık gibi modern egemenliğin temel dayanakları bu süreçte yeniden tartışmaya açılmıştır. Dijital platformlar; kullanıcı sözleşmeleri, algoritmik karar mekanizmaları ve içerik denetimi yoluyla norm koyma, uygulama ve yaptırım benzeri yetkiler kullanmaya başlamıştır. Böylece yasa ile uygulama arasındaki ilişki, devlet dışı aktörler tarafından fiilen yeniden kurulmakta; egemenliğin klasik sınırları aşınmaktadır.

Bu dönüşüm, egemenliğin bölünmezliği ilkesini fiilen zayıflatırken, dijital alanda ortaya çıkan iktidarın meşruiyetini de tartışmalı hâle getirmektedir. Big Tech; kamusal iktidara özgü düzenleyici ve yargısal işlevleri demokratik yetkilendirme ve hesap verebilirlik mekanizmalarından yoksun biçimde üstlenmektedir. Ortaya çıkan bu dijital egemen(!) ne halk iradesine ne de toplumsal sözleşme kuramlarının öngördüğü kurucu rıza ve siyasal eşitlik ilkelerine dayanmaktadır.

---

[967] Akal, *Devlet, Yasa, Hakimiyet*, s.27-29.
[968] Uygun, s.218.
[969] Akad, Dinçkol ve Bulut, s.126.
[970] Cemil Caca Arslan, s.260.

Bu noktada bazı yazarlarca ileri sürülen dijital platformların kullanıcı sözleşmeleri aracılığıyla meşruiyet ürettiği iddiası sorunludur[971]. Çünkü toplumsal sözleşme eşit özneler arasında kurulur, kamusal niteliklidir ve siyasal topluluğun varlığını mümkün kılan kurucu bir mutabakattır[972]. Buna karşılık platform sözleşmeleri, tek taraflı olarak belirlenen, müzakereye kapalı ve özel hukuk ilişkisi doğuran metinlerdir. Bu tür sözleşmelerin dijital bir toplum sözleşmesi olarak nitelendirilmesi, klasik toplum sözleşmesi kuramının dayandığı kurucu irade, siyasal eşitlik ve kolektif bağlayıcılık unsurlarını göz ardı etmektedir.

Toplum sözleşmesi kuramı, geliştiği özgün tarihsel zemin içerisinde aklın buyruğu ile sivil barışı sağlamak için herkesin üzerinde uzlaştığı bir sözleşme olup bireyin toplum karşısında özgürlüğünü savunmayı içerir[973]. Hobbes'ın ileri sürdüğü sivil yurttaşlık sözleşmesi, doğal durumdaki sürekli savaş hâlinden (*homo homini lupus*) kaçmak için doğal hakların bireyler tarafından egemene (Leviathan) devrederek egemenin mutlak gücünü tanımasıyla ortaya çıkmıştı. Devlet, yasal şiddet tekelini elinde tutarak güvenliği sağlar ve bu da insan haklarının ilki ve temeli olan güvenlik hakkını doğurur[974]. Günümüzde, devlet ortadan kalkmadığına göre bu görüş ya en fazla platformların biriktirdikleri gücü meşrulaştırmaya ya da platformları yeni egemenler olarak devletin yerini aldıklarına ikna etmeye çalışır. Fakat insanın ve toplumun

[971] Tarleton Gillespie, göre bu denli büyük ve etkili hâle gelen sosyal medya platformları, kamusal söylem üzerindeki güçlü etkileri sebebiyle kullanıcıların onayladığı sözleşmelerin ötesine geçen örtük bir toplumsal sözleşmenin tarafı konumuna geldiğini ve topluma karşı fiilî bir sorumluluk üstlendiği iddia etmiştir. Tarleton Gillespie, **Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media,** Connecticut: Yale University Press, 2018, s.208. Benzer görüşte bkz: Işık, s.27.

[972] Toplum sözleşmesi kuramı, devletin ve egemenliğin kaynağını bireylerin aklı ve kolektif rızasında temellendirir. Bu çerçevede önce siyasal topluluğu kuran sosyal sözleşme, ardından egemenliğin kullanımını düzenleyen siyasal sözleşme yapılır. Okandan, *"Devletin Tarihi Menşeini Mukaveleye İstinat Ettiren Muhtelif Görüşler",* s.121-122. Suárez, toplum halinde yaşamanın insan tabiatından doğan siyasal bir zorunluluk olduğunu ve bu zorunluluğun bireylerin özgür iradeleriyle yaptıkları kurucu bir anlaşmaya dayandığını vurgular; bu anlaşma, topluluğu ortak yarara yönelen siyasal-ahlaki bir bütün hâline getirir. Akal, *Modern Düşüncenin Doğuşu: İspanyol Altın Çağı,* s.254. Akkaya ise siyasal bağlılığın geçici çıkarlara değil, siyasal sistemin sürekliliğine içkin ilkelere dayanması gerektiğini savunur. Rukiye Akkaya, "J. J. Rousseau'nun 'Sosyal Sözleşme' Eserinin Osmanlı Türkçesine İlk Tercümeleri II", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.26, Sayı.2, *(Aralık 2020)*, s.535.

[973] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.91.

[974] Kriegel, s.40-45, 71.

doğasında ve kodlarında var olan siyasal iktidar ile doğal bağları ve ilişkileri ve bunun yanı sıra bilinen yöneten-yönetilen ilişkisi değişmemiştir.

Bu sözleşmeler siyasal bir topluluk yaratmadığı gibi, bireyi yurttaş olmaktan çıkararak tüketici statüsüne indirger. Veri üreten yeni nesil serfler olarak bireyler (tüketiciler), teknolojik güçler bünyesinde bir siyasal bütünleşme[975] yaratmadığından dijital şirketler toplum sözleşmesinin tarafı olarak nitelendirilemez. Post modern küresel kapitalist düzeni tanımlamak için ortaya atılan "çokluk/İmparatorluk" kavramı da tekil bir iktidara indirgenemeyen, birliğe dönüşmeyen ve bu nedenle egemenlik kuramayan dağınık bir toplumsal yapıya işaret etmişti[976].

Dijital platformların anayasa benzeri kurallar, iç denetim mekanizmaları ve sözde uyuşmazlık çözüm yolları geliştirmesi ise hukukun üstünlüğünü tesis etmekten ziyade, onun meşruiyet sembollerini taklit eden sahte normatif yapılar üretmektedir. Bu yapılar, demokratik hukuk düzenine tabi olmaksızın kamusal otorite görüntüsü yaratmakta; egemenliğin hukuki ve ahlaki temelini daha da muğlaklaştırmaktadır[977].

Kullanıcı sözleşmeleri şirket çıkarını esas aldığından devlet egemenliği, hak ve birey merkezli düzenlenmez. Platform-kullanıcı sözleşmeleri ve gizlilik politikaları şeffaflıktan uzak algoritmalar karşısında bireyi değil platformu koruyan hukuki kalkan görevi görmektedir[978]. Kullanıcı sözleşmelerindeki onay, siyasal toplum oluşturmayan bölük pörçük rızalar olduğundan meşruiyet kaynağı sayılamaz.

Ulus-devlet, kendi egemenlik sahasında gerçek ve tüzel kişiler üzerinde tek meşru otorite olduğunu iddia eder; bu iddianın temelinde de yalnızca bir kimlik değil, egemenliğin kavramsal ve ideolojik temeli olan ulus adına hareket etme söylemi yer

---

[975] Erözden, s.174.

[976] Negri, siyaset teorisi geleneğinin ortak varsayımı olan yalnızca "bir" yönetebilir anlayışın karşısına küreselleşmiş kapitalist düzenin bir niteliği olan "çokluk" kavramını koymuştur. Çokluk birliğe indirgenemez, bir'in iktidarına boyun eğmez ve egemenlik kuramaz. Bu nedenle toplumsal bir beden olarak düşünülemez. Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.345. Kapitalizm tarafından yönlendirilen küreselleşme artık bir süreç değil, gerçekleşmiş bir durumdur. Ortaya çıkan yapı, Hardt & Negri'nin "imparatorluk" dediği, çelişkilerle dolu ve alternatif güç odaklarının yükselmesine imkân tanıyan bir düzen üretir. Dirlik, *Küresel Modernite: Küresel Kapitalizm Çağında Modernite,* s.109.

[977] Coroado, s.5.

[978] Uluk, s.105.

alır[979]. Bu nedenle platformların toplumsal sözleşmenin tarafı olabilecekleri, kamusal bir fonksiyona sahip olabilecekleri ve kamusal işleri bürokrasi olmadan halledebileceği iddiası küreselleşmenin sınır aşan etkisinin derinleştirilerek egemene paralel yapılar oluşturmanın çabalarıdır. Devlet dışı aktörlerin bu yeni toplum mühendisliği kapasitesi, yüzeyde Rousseau'nun genel iradesini andıran kişiler-üstü bir yönlendirme pratiği üretse de özgürlüğü ve hakları korumayı değil; kâr ve kontrolü merkeze alan bu güç biçimi meşru bir egemenlik olarak değerlendirilemez[980]. Bu nedenle mevcut toplumsal sözleşme modelleri aşılmış; egemenliğin yeniden tanımlanması ve dijital çağın koşullarına uygun yeni bir toplumsal sözleşme arayışı zorunlu hâle gelmiştir.

Toplumsal sözleşme kuramları, Hobbes, Locke ve Rousseau'da modern devlet egemenliğini açıklamakta işlevsel olsa da dijital çağda ortaya çıkan teknoloji şirketlerinin iktidarını kavramakta yetersiz kalmaktadır. Bu aktörler halk iradesiyle yetkilendirilmemiş, yasama gücüne sahip olmayan ve etkili biçimde denetlenemeyen yapılardır. Hukuktan kaynaklanmayan bir güç, bu anlamda iktidar niteliği taşıyamaz[981]. Dijitalleşme öncesinde egemenlik daha çok toplumsal ve sınıfsal modeller üzerinden işlerken, algoritmik kişiselleştirme her bireyi ayrı bir model hâline getirmekte; toplumsal bağları çözmekte ve atomizasyonu hızlandırmaktadır[982]. Böylece dijital iktidar, toplumsal sözleşmenin kolektif yapısını aşındıran bireysel düzeyde bir tahakküm üretmektedir.

Sonuç olarak dijital alanda ortaya çıkan güç, devletler ve devlet dışı aktörler arasında paylaşılmaktadır. Bu çok aktörlü ve sınır aşan yapı, klasik egemenlik modellerini aşındırmakta; devletlerin dijital alan üzerindeki kontrol iddialarını yalnızca meşru otorite savına dayandırmasını hem teknik hem de demokratik denetim açısından zayıflatmaktadır. Meşruiyetin gücün kurala bağlanmasıyla mümkün olduğu dikkate alındığında[983] dijital platformların ticari rasyonaliteye dayalı, belirsiz ve kuralsız güç kullanımı ciddi bir meşruiyet krizi üretmektedir[984]. Bu kriz, dijital çağda ortaya çıkan bu

[979] Erözden, s.70.
[980] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.50.
[981] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.21-24.
[982] Çalgan, s.67.
[983] Uygun, s.8.
[984] Akdenizli, s.43.

iktidar biçiminin, modern toplumsal sözleşme kuramlarıyla açıklanamamasından kaynaklanır. Devlet dışı aktörlerin fiilî egemenlik benzeri yetkiler kullanması, egemenliğin kaynağı, sınırları ve meşruiyetinin yeniden düşünülmesini zorunlu kılmaktadır. Bu bağlamda mevcut sözleşmeci modeller aşılmış; dijital çağın koşullarına uygun, kamusal rızayı ve demokratik denetimi merkeze alan yeni bir egemenlik ve meşruiyet tartışması, egemenliğin içsel dönüşümü açısından kaçınılmaz hâle gelmiştir. Dijital alanın denetimsiz bırakılmasının temel haklar açısından ciddi riskler doğuracağı gerçeği ile yüz yüze iken; bu riske çözüm, bize göre, ne uluslararası insan hakları mekanizmalarından sonuç beklemek ne de platformlara kamusal aktör niteliği atfetmektir. Platformları haklar karşısında zorlayacak ve hesap verebilir kılacak güç devlet dışı aktörlerde bulunmadığı gibi uluslararası düzenlemeler de ulusal düzeyde etkili koruma sağlayamamaktadır. Bu nedenle dijital çağda temel hakların korunmasında devlet, sosyal sözleşmenin yegâne tarafı ve asli aktör olarak kabul edilmelidir. Platformların kamusal fonksiyonu olduğu varsayımı yerine, platformların devlete karşı sorumlu tutulması esası benimsenmelidir; aksi yaklaşım modern kamu hukuku anlayışıyla bağdaşmaz ve kullanıcıları belirsizlik içinde bırakır.

2. Yeni Güç Biçimi Olarak Dijital Egemen ve Çok Katmanlı Formu

Toplumsal düzen; kurallar ve bu kurallara uyma yükümlülüğü üzerine kuruludur. Kurallara uyumun meşruiyet inancıyla birleştiği durumda otorite ortaya çıkar; meşruiyet kazanmış iktidar, otorite niteliği taşır. İtaat; korku ya da alışkanlıktan değil, emirlerin haklı ve geçerli olduğuna inanıldığı için gerçekleşiyorsa, bu ilişki iktidar değil otorite olarak tanımlanır; meşruiyetten yoksun güç kullanımları ise siyasal nitelik taşımaz[985]. Bu bağlamda siyasal iktidar, toplumun bütününü kapsayan ve toplumsal düzenin devamı için zorunlu olan iktidar türüdür[986]. En basit toplumsal yapılarda dahi mevcut olmakla birlikte, örgütleniş ve işleyiş biçimi tarihsel, ekonomik ve kültürel

[985] Yahya Kazım Zabunoğlu ve Diğerleri, **Devletin Genel Kuramı Dersleri: Cilt I**, Ankara: Yetkin Yayınları, 2021. s.26.
[986] Uygun, s.6-7.

koşullara göre değişir[987]. Bu nedenle siyasal iktidarı yalnızca devletle özdeşleştirmek, devlet dışındaki güç ilişkilerini açıklamakta yetersizdir[988].

Siyasal iktidarı diğer iktidar biçimlerinden ayıran başlıca özellikler; toplumun tamamı üzerinde geçerlilik iddiası taşıması, diğer güç odaklarına üstünlüğü, genel yetki iddiası ve meşru fiziksel zor kullanma kapasitesidir[989]. Toplumdaki diğer iktidar odakları egemenden kaynaklanır: onun izniyle onun izin verdiği ölçü ve süre için vardırlar. Klasik egemenlik öğretisinde bu nitelikler mutlaklık, süreklilik ve bölünmezlik ilkeleriyle tamamlanır. Bodin egemeni egemenlikle sınırlar: egemen olan bu üstün erki bir başka kişiye ya da kuruma devredemez; egemen kararlarında başka bir iradeye bağlı değildir[990]. Bu anlayış modern devlet egemenliğinin teorik temelini oluşturmuştur.

Bununla birlikte siyasal iktidar biçimleri, zaman, mekân, üretim ilişkileri, iletişim teknolojileri ve hukuk düzenleri gibi değişkenlere bağlı olarak dönüşmektedir. Toplumsal değişimi yalnızca soyut bir ilerleme fikri olarak değil, kurumların ve örgütlenme biçimlerinin dönüşümü olarak ele almak gerekir. İlkel toplumdan kent toplumuna, feodal yapılardan ulus-devlete uzanan tarihsel süreçte siyasal iktidar, her aşamada farklı bir düzen kurma modeli üretmiştir[991]. Modern devlet, yöneten-yönetilen ayrımına dayanan, kural koyan ve uygulayan uzmanlaşmış kurumsal bir yapıdır; meşruiyetini kendi koyduğu ve uyguladığı hukuk kurallarına uygun davranmasından alır. Tarihsel olarak bu iktidar, ilkel toplumdan sonra ortaya çıkan kent toplumunda (polis/site devleti) şekillenmiş; ardından feodal devlet ve ulus-devlet biçimlerine dönüşerek evrilmiştir[992].

Dijitalleşme olgusu, bu tarihsel süreklilik içinde niteliksel bir kırılma noktası yaratmaktadır. İletişim ve bilişim teknolojileri, artık yalnızca iktidarın kullandığı araçlar değil, bizzat iktidar üretme kapasitesine sahip bağımsız güç odakları hâline gelmiştir[993].

---

[987] Akal, *Devlet, Yasa, Hakimiyet*, s.48.
[988] Akad ve Diğerleri, s.17.
[989] Uygun, s.7.
[990] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.27-32.
[991] Uygun, s.5.
[992] Uygun, s.8-9.
[993] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.76.

Bu durum; devlet, ülke unsuru ve egemenlik gibi klasik kavramların aynı anlam içeriğiyle kullanılmasını tartışmalı kılmaktadır. Dijital alan, egemenliğin mekânsal sabitliğini aşındırarak, sınırların geçirgenleştiği ve yetki alanlarının iç içe geçtiği yeni bir iktidar düzlemi yaratmaktadır.

Bu tartışmayı derinleştiren bir nokta da sosyal bilimlerde "sabit yasalar" fikrinin sınırlılığıdır. Doğa bilimlerinde aynı koşullar aynı sonuçları üretirken; tarihsel ve toplumsal süreçler; bağlam, aktörlerin eylemleri ve güç ilişkileri tarafından şekillenir[994]. Bu nedenle hukuk da çoğu zaman önceden kurulmuş güç ilişkilerini tanımlayan ve meşrulaştıran bir işlev görür. Günümüzde dijital alan bakımından benzer bir eşik yaşanmakla birlikte, temel fark şudur: Egemen devlet fiziksel mekânda hâlihazırda varlığını sürdürmekte ve dijital alana da kapasitesi ölçüsünde nüfuz edebilmektedir. Bu nedenle dijital alanda tekil ve mutlak bir "dijital egemen"in doğduğunu peşinen varsaymak yerine, devletler ile küresel teknoloji şirketleri arasında henüz istikrara kavuşmamış güç ilişkilerini dikkate alan bir analiz gereklidir.

Modern devlet, egemenliği hukuken belirlenmiş sınırlar içinde eşit ve mutlak işleyen bir yetki olarak[995] kurgulamışken; dijital çağda bu mekânsal kurgu zayıflamaktadır. Coğrafi merkezler yerini ağlara, veri akışlarına ve teknik altyapılara bırakmaktadır[996]. Bu yeni düzlemde dijital platformlar, fiziksel sınırların ötesinde faaliyet göstererek devletin düzenleme kapasitesini ve yurttaş üzerindeki otoritesini zorlamaktadır. Büyük teknoloji şirketleri, veri, algoritma ve bilgi akışı üzerindeki denetimleri sayesinde demokratik karar alma süreçlerini dolaylı biçimde etkileyebilmekte; bireylerin kanaat oluşturma özgürlüğü üzerinde baskı kurabilmektedir. Bu etki, yalnızca bireysel hak ihlalleriyle sınırlı olmayıp, devletin iç egemenliğinin fiilî olarak aşınması riskini de beraberinde getirmektedir[997].

---

[994] İsmail Bahadır Turan, "Devlet Öğretisi Metodolojisi-Georg Jellinek (Allgemeine Staatslehre)", **Kamu Hukuk ve Yönetim,** Cilt.1, Sayı.1, (Temmuz 2024), s.53-54.
[995] Anderson, s.33.
[996] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.517.
[997] Cemil Caca Arslan, s.261.

Buna karşın dijital platformların sınır aşan niteliği, onları bütünüyle hukuk-dışı aktörler hâline getirmez. Çoğu platform, hukuken merkezlerinin bulunduğu devletin hukukuna tâbidir. Ancak tekil bir ulusal hukuk düzenine bağlı olup çok sayıda ulusal düzen üzerinde etkili olan bu yapılar, kaçınılmaz olarak norm çatışmaları ve uyumsuzluklar üretmektedir. Kullanıcı sözleşmeleri ile ulusal kamu düzenleri arasındaki gerilim, devletler ile küresel platformlar arasındaki uyuşmazlıkların temelini oluşturmaktadır[998].

Dijital alanın teknik özellikleri de klasik egemenlik anlayışını zorlayan unsurlar arasındadır. AYM'nin bir kararında belirttiği üzere, internetin yaygın ve ademimerkeziyetçi ağ yapısı, içeriklerin dünyanın herhangi bir yerinden anında dolaşıma girmesine imkân tanırken; kimliğin gizlenebilmesi hukuka aykırı içeriklerin küresel ölçekte yayılmasını kolaylaştırmaktadır. Bu durum, ulusal sınır temelli denetim mekanizmalarının etkinliğini azaltmakta ve devletin geleneksel kontrol kapasitesini zayıflatmaktadır[999]. NFT, blokzincir ve Metaverse gibi yeni teknolojiler ise yetki, yargı yeri ve uygulanacak hukuk sorunlarını daha da karmaşık hâle getirmektedir[1000].

Dijitalleşme, ekonomik faaliyetleri de fiziksel mekândan büyük ölçüde koparmıştır. Devletler, bilgi işlem ve veri işleme kapasitelerinin önemli bir bölümünü özel şirketlere devrederken; büyük teknoloji platformları bu kapasiteyi kendi bünyelerinde yoğunlaştırarak ticaret, emek piyasası, uyuşmazlık çözümü ve iletişim alanlarında güçlü düzenleyici aktörler hâline gelmiştir. Büyük veri ve algoritmik karar alma süreçleri, klasik bürokrasi ve kamu yönetiminin dijital karşılıkları olarak işlev görmektedir. Big Tech şirketleri ulusal sınırları tamamen ortadan kaldırmasa da onları fiilen aşarak, ekonomik gücün yanında siyasal ve kültürel etki üreten yarı-devlet(!) niteliğinde aktörlere dönüşmüştür[1001]. Veri ve iletişim altyapıları üzerindeki hâkimiyetleri

---

[998] Cemil Caca Arslan, s.259-260.

[999] AYM, 15/11/2017, E. 2015/76, K. 2017/153, Karşı Oy Gerekçesi, par. no. 12, https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/153

[1000] Sökmen Güler, s.196. Örneğin Barbados'un Decentraland gibi bir metaverse platformunda dijital elçilik açma girişimi, egemenliğin dijital ortamlarda sembolik yeniden üretiminin ilk örneklerindendir. Ancak bu tür hamleler, egemenliğin maddi altyapılara olan bağımlılığı nedeniyle çoğunlukla sembolik kalmakta ve fiilî kontrol gücü başka aktörlerin (şirketler, platform sağlayıcıları) elinde bulunmaktadır. Dikmengil s.176-178.

[1001] Lehdonvirta, s.210-214.

ve artan ekonomik güçleriyle siyasal ve toplumsal alanlara müdahale edebilen, iç politika ve uluslararası ilişkilerde etkili, hatta bazı yönleriyle devlet otoritesiyle yarışan ve insan hakları üzerinde ciddi etkiler yaratabilmektedirler[1002]. Devasa veri setleri aracılığıyla bireyleri öngörebilmekte, yönlendirebilmekte; iletişim altyapısı ve veri akışları üzerindeki fiilî hâkimiyetleriyle devletin düzenleyici kapasitesini zayıflatmakta; sınır aşan veri hareketliliği ise ulus-devletin coğrafi egemenlik modelini aşındırmaktadır. Bu süreç, verinin stratejik bir kaynak hâline geldiği dijital kapitalizm/dijital kolonyalizm biçimini doğurmakta; merkez ülkeler güçlerini pekiştirirken çevre ülkeler dijital bağımlılık ve kırılganlıkla karşı karşıya kalmaktadır[1003].

Böylece devletin egemenlik yetkilerini toprak paradigması üzerinden sürdürmesi güçleşmiş; devlet dışı aktörler (özellikle büyük teknoloji şirketleri) veri, altyapı ve algoritmik yönlendirme gücüyle egemenliğe benzer etkiler üretmeye başlamış[1004] ve egemen devletlerle sınırlı dünya düşüncesinin aşınmasına neden olmuştur. Bu tablo, egemenlik iddialarının fiilî kontrol, altyapı sahipliği ve veri yönetimi gibi unsurlarla birlikte değerlendirilmesini zorunlu kılar. Ancak meşru bir yetki kaynağı olmaksızın kendi kendilerini egemen ilan eden küresel teknoloji tiranlarına ayrıcalık tanıyan bu düzen, henüz ne meşruluk kriterini aşabilmiştir ne de kalıcı bir egemenlik benzeri form üretebilmiştir. Bu durum, dijital platformların hukuken egemen aktörler hâline geldiği anlamına da gelmez; daha isabetli bir değerlendirme, devlet ile platformlar arasında egemenlikten ziyade iktidar ve meşruiyet eksenli bir mücadelenin yaşandığıdır.

Bu çerçevede dijital egemenlik, devletin dijital alana klasik egemenlik mantığını uyarlama çabasını ifade eder. Dijital altyapı, veri ve teknolojik sistemler üzerinde dış müdahaleye kapalı biçimde karar alma ve düzenleme yetkisi, bu anlayışın merkezinde yer alır. Dijital vatandaşlık, dijital kamu hizmetleri ve dijital haklar gibi kavramların ortaya çıkışı, egemenliğin bu yeni biçiminin doğal sonuçlarıdır. Ulusal veri merkezleri, platform düzenlemeleri, siber güvenlik stratejileri ve sınır ötesi veri transferlerinin denetimi, dijital egemenlik politikalarının başlıca araçlarıdır. Ancak dijital alan, aynı

[1002] Coroado, s.4-5.
[1003] Sala, s.376-379, 382-385.
[1004] Işık, s.25.

zamanda devlet dışı aktörlerin yoğunlaştığı bir iktidar düzlemidir; bu durum egemenliğin tek bir özne üzerinde toplanmadığı, çok merkezli ve çok katmanlı bir yapının ortaya çıktığını göstermektedir.

Bu bağlamda dijital egemen kavramı, egemenlik yetkilerini dijital alanda fiilen kullanan aktörleri tanımlamak üzere kullanılmaktadır. Devletler, büyük teknoloji şirketleri, algoritmalar, yapay zekâ sistemleri ve teknik standartları belirleyen ağ yapıları, bu yeni güç alanının aktörleri arasında yer almaktadır. Egemenlik yetkilerinin bu aktörler arasında dağılması, klasik egemenlik öğretisiyle çelişmekte; hukuki sorumluluk ve hesap verebilirlik sorunlarını derinleştirmektedir[1005]. Dijital çağda ortaya çıkan bu çok katmanlı iktidar yapısı, egemenliğin yalnızca hukukla değil; veri, altyapı ve bilgi kontrolüyle birlikte yeniden düşünülmesini zorunlu kılmaktadır.

Günümüzde devlet egemenliği, hukuk devleti ilkesi, insan hakları rejimi ve uluslararası normlarla sınırlandırılmış bir yetki alanı içinde kullanılmaktadır[1006]. Buna karşılık dijital platformlar, bu sınırlayıcı çerçevelere tabi olmaksızın sınır aşan, fiilî ve büyük ölçüde denetimsiz bir güç alanı üretmektedir. Bu asimetri, egemenliğin tek merkezli ve hiyerarşik bir yapıdan uzaklaşarak merkezsiz, ağ temelli ve parçalı bir iktidar düzenine evrilmesine yol açmaktadır. Dijital alan, bu yönüyle yalnızca yeni bir teknik ortam değil; kültürel hegemonya, yapay rıza üretimi ve davranış yönlendirmesi yoluyla işleyen yeni bir iktidar biçiminin taşıyıcısıdır.

Dijital iktidarın ayırt edici özelliği, yurttaşı hak sahibi bir siyasal özne olmaktan ziyade veri üreten ve öngörülebilir bir nesneye indirgemesidir[1007]. Algoritmik karar alma süreçleri, bireysel tercihleri yönlendiren ve davranışları şekillendiren bir tahakküm mekanizması üretmektedir. Bu bağlamda "kim biliyor, kim karar veriyor ve kimin karar vereceğine kim karar veriyor?" soruları, giderek siyasal kurumların dışına taşarak şirketlerin veri mimarileri ve algoritmik altyapıları içinde yanıt bulmaktadır[1008].

[1005] Max Tretter, "Sovereignty in the Digital and Contact Tracing Apps". **Digital Society: Ethics, Socio-Legal and Governance of Digital Technology,** Vol.2, (2023), s.1-2.
[1006] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.20.
[1007] Shoshana Zuboff, **The Age of Surveillance Capitalism**, New York: Public Affairs, 2019, s. 16 vd.
[1008] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.230-231.

Çevrimiçi deneyim, kullanıcının yalnızca ne yaptığına değil, kim olduğuna, ne istediğine ve kim olması gerektiğine dair normatif bir çerçeve sunduğundan, özgürlük kavramının da yeniden düşünülmesini zorunlu kılmaktadır[1009].

Bu gelişmeler, dijital çağda ortaya çıkan iktidar biçiminin ne Sanayi Devrimi'nin üretim ilişkileriyle ne de Soğuk Savaş'ın devlet-merkezli güç dengeleriyle açıklanabileceğini göstermektedir. Dijital çağ, algoritmik yönlendirme, davranışsal yönetim ve yapay zekâ temelli karar süreçlerine dayanan, siyasal nitelikli yeni bir iktidar potansiyeli üretmiştir. Bu nedenle dijital egemenlik, insan özerkliği ile teknoloji-iktidar ilişkisi üzerinden yeniden kavramsallaştırılmalıdır[1010].

Bu noktada egemenliğin dönüşümü, yalnızca yetki alanlarının genişlemesi ya da daralmasıyla değil, bu yetkiyi fiilen kullanan öznenin niteliğinin değişmesiyle açıklanmalıdır. Dijitalleşme, iktidarın görünüm biçimlerinden birinin devlet merkezli yapıdan kısmen koparak devlet dışı aktörlere yönelmesini zorunlu kılmıştır. Dijital egemen, bu bağlamda klasik anlamda hukuki yetkiyle donatılmış tekil bir otorite değil; dijital altyapıların kontrolü, veri işleme kapasitesi ve algoritmik düzenleme gücü sayesinde fiilî bir yapabilme kudreti kullanan çok katmanlı bir özne olarak ortaya çıkmaktadır. Devletler, platform şirketleri, teknik standartları belirleyen ağ yapıları ve kullanıcı toplulukları arasında dağılan bu güç, hukuki egemenliğin yanında işleyen, fakat onunla örtüşmeyen özgül bir dijital iktidar rejiminin oluşmasına zemin hazırlamaktadır.

Bu dönüşümün hak boyutu da belirleyicidir. Devletler dijital egemenlik politikalarıyla kontrol kapasitelerini artırmaya yönelirken; ifade özgürlüğü, mahremiyet ve dijital özerklik gibi temel haklar üzerinde yeni baskı alanları oluşabilmektedir. Buna karşılık dijital şirketlerin modern devletin yerini alması, özellikle sosyal ve ekonomik haklar bakımından yapısal olarak mümkün değildir. Zira çağdaş anayasal düzende hakların gerçekleşmesi, yalnızca müdahalesizlik değil, aynı zamanda aktif düzenleme ve kamu hizmeti yükümlülüklerini de gerektirir. Bu nedenle mesele, devletin ortadan

[1009] John Cheney-Lippold, "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control: Soft Biopolitics and the Modulation of Control", **Theory, Culture & Society,** Vol.28, No.6, (2011), s.177.
[1010] Timmers, *"Sovereignty in the Digital Age",* s.584.

kalkmasından ziyade, dijital çağda iktidarın taşıyıcılarının çeşitlenmesiyle ortaya çıkan yeni bir iktidar rejiminin hukuki ve siyasal olarak nasıl denetleneceği sorunudur.

Modern devlet, iktidarını ülkesindeki tüm kişi ve kurumların üzerinde yer alan merkezi ve üstün bir güç olarak kurar. Bu üstünlük egemenlik kavramıyla ifade edilir[1011]. Bununla birlikte siyasal iktidar biçimleri arasında mutlak bir hiyerarşi bulunmadığı; farklılıkların, yasa ile uygulama arasındaki ilişkinin nasıl kurulduğundan kaynaklandığı da açıktır. En basit toplumsal yapılarda dahi sosyal düzen, norm ile fiil arasındaki bağ üzerinden kurulmuş; sosyallik, siyasilik ve hukuksallık tarihsel olarak iç içe gelişmiştir[1012].

Bununla birlikte, dijital şirketlerin modern devletin yerini alması özellikle sosyal ve ekonomik haklar yönünden mümkün değildir. Çünkü, günümüzde çağdaş anayasalarda devlet artık sadece müdahale etmeyen "pasif" bir yapı değildir; temel hak ve özgürlüklerin gerçekleşmesi için aktif görevler üstlenir. Kişinin onuruna yaraşır koşullarda yaşayabilmesi, devletin engelleri kaldırması ve maddî-manevî gelişim için somut imkânlar sağlamasına bağlıdır. Anayasal düzende bir yandan dokunulmaz kişisel özgürlükler devletten korunurken, diğer yandan sosyal hakların gerçekleşmesi devletin aktif düzenleme ve hizmet sunma yükümlülüğüne bağlanmıştır[1013].

Bu çerçevede devlet ile büyük teknoloji şirketleri arasındaki ilişki, bir egemenlik devrinden ziyade, insan unsuru üzerinde yürütülen bir iktidar ve meşruiyet mücadelesi olarak okunmalıdır. Dijital platformlar, devletin yurttaşla kurduğu meşru iktidar ilişkisine eklemlenen ve onu aşındıran paralel yapılar üretmektedir. Bununla birlikte dijital alandaki iktidarın nihai kaynağının kullanıcılar olduğu da gözden kaçırılmamalıdır; kullanıcı kitlesi ortadan kalktığında dijital iktidarın da varlık zemini çöker. Buna rağmen günümüz koşullarında devletlerin toplumu bütünüyle dijital alanın dışına çıkarması ya da

---

[1011] Başgil, *"Devlet Nedir?: Realist Bir Tarif Denemesi",* s.990.
[1012] Akal, *Devlet, Yasa, Hakimiyet*, s.24.
[1013] İlhan Akın ve Mehmet Akad, "Cumhuriyetin Ellinci Yılında Temel Hak ve Özgürlükler", **İstanbul Üniversitesi Hukuk Fakültesinin 50. Yıl Armağanı: Cumhuriyet Döneminde Hukuk,** İstanbul: İstanbul Üniversitesi Yayınları, Yayın No: 1888, 1973, s.24.

platform egemenliğini tamamen bertaraf etmesi fiilen zorlu bir süreç olarak görünmektedir.

Metaforik anlatımla, küresel teknoloji şirketleri devletin egemenlik alanına sırtlan gibi saldırmakta, onun üzerinde parçalayıcı ve kuşatıcı bir baskı kurmaktadır. Bu baskı doğrudan zor kullanma biçiminde değil, ama algı yönetimi, altyapı kontrolü ve bilgi erişimi tekeli yoluyla yürütülür. Bu durum, özellikle zayıf dijital altyapıya sahip devletler için egemenlik boşlukları yaratır. Devlet dışı aktörlere (özellikle büyük teknoloji şirketlerine) toplum mühendisliği, yani birey ve toplumu yönlendirme kapasitesi vermekte; kişiler-üstü bir tasarım ve yönlendirme pratiği doğurmaktadır.

Sonuç olarak dijitalleşme, egemenliği yalnızca yetki alanlarının genişlemesi bağlamında değil, bu yetkiyi fiilen kullanan öznenin niteliğinin dönüşmesi bakımından da köklü biçimde değiştirmektedir. Dijital egemen, klasik anlamda hukuki yetkiyle donatılmış tekil bir otorite olmaktan ziyade; dijital altyapıların kontrolü, veri işleme kapasitesi ve algoritmik düzenleme gücü sayesinde fiilî iktidar kullanan çok katmanlı bir yapı olarak ortaya çıkmaktadır. Bu yeni iktidar formu, devlet merkezli egemenlik anlayışını aşındırırken hukuk devleti ilkesi, meşruiyet ve temel haklar açısından yeni sorular ve yapısal kriz alanları üretmektedir.

Küresel teknoloji şirketleri hukuken egemen aktörler olmamakla birlikte, fiilen egemenliğe benzer bir güç inşa etmiş durumdadır. Bu güç, meşruiyetini halk iradesinden ya da hukuki yetkilendirmeden değil; piyasa sözleşmelerinden, teknik bağımlılıklardan ve altyapı üzerindeki fiilî kontrolden almaktadır. Bu nedenle dijital çağda egemenliği yalnızca hukuki kategorilerle açıklamak yetersiz kalmakta; veri, altyapı ve bilgi kontrolünü merkeze alan bütüncül bir analiz zorunlu hâle gelmektedir. Dijital egemenlik kavramıyla yetinmeyip dijital egemeni, onun araçlarını ve yurttaş üzerindeki etkilerini incelemek, kamu hukuku ve siyaset teorisi açısından kaçınılmazdır.

Bu perspektif, temel hakların dijital çağda yalnızca korunması gereken normatif değerler olarak değil, aynı zamanda görünmez güç ilişkilerini açığa çıkaran eleştirel bir analiz zemini olarak yeniden yorumlanmasına imkân tanır. Akkaya'nın tespit ettiği üzere, devletin geleneksel kurumsal yapısı hem dışsal tehditleri bertaraf etmekte hem de içeride

olgunlaşan toplumsal taleplere tatmin edici yanıtlar üretmekte yetersiz kaldığında, iktidar örüntüsünün yeniden düşünülmesi kaçınılmaz hâle gelir[1014]. Bununla birlikte devletlerin dijital aktörler olarak egemenliklerini sürdürme mücadelesi ivme kazanarak devam ettiğinden, bu mücadelenin galibini şimdiden belirlemek ya da devletin yerini bütünüyle yeni bir siyasal iktidar formunun alıp almadığını kesin biçimde yanıtlamak mümkün görünmemektedir. Mevcut aşamada yapılabilecek olan, dijital çağın ürettiği bu dönüşümü zamansal bağlamı içinde izlemek ve eleştirel bir dikkatle çözümlemektir.

3. Leviathan 2.0: Veri-Tanrı ve Dijital Teoloji

Egemenliğin toplumun üzerinde, aşkın bir konumda tahayyül edilmesi, siyasal iktidarın tarihsel olarak teolojik bir kökene dayandığını göstermektedir. Egemen, kendisinden üstün bir merci tanımayan ve norm koyma yetkisini tek başına elinde bulunduran otorite olarak tanımlanır[1015]. Bu bağlamda Thomas Hobbes'un Leviathan kavramsallaştırması, modern siyasal düşüncede egemenliğin en güçlü metaforlarından birini oluşturur. Hobbes'un yapay insan olarak kurguladığı Leviathan, bireylerin rızasıyla inşa edilen seküler bir Tanrı figürüdür: bedeni halktan, iradesi ise egemenden oluşur[1016]. Leviathan'ın temel işlevi kaosu önlemek, güvenliği tesis etmek ve toplumsal düzeni sürdürülebilir kılmaktır.

Hobbes'un siyasal teorisinde eşitlik, insanların birbirlerini öldürebilme kapasitesine dayalıdır. Bu nedenle doğa durumu barışçıl bir eşitlik alanı değil, herkesin herkesle savaşıdır. Ölüm korkusu ve aklın yönlendirici etkisi, bireyleri özgürlüklerinin bir kısmından feragat ederek merkezi bir egemen otorite kurmaya sevk eder. Sivil durumda barış, bireyler arası eşitlikten değil; egemen ile uyruklar arasındaki yapısal eşitsizlikten doğar. Devlet, bu çerçevede güvenlik, refah ve düzen arayışının kurumsal

[1014] Akkaya, *"J.B. Bossuet: 'Devlet Sizsiniz Majesteleri'!",* s.850.
[1015] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.346.
[1016] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.218.

karşılığıdır[1017] ve güçlü bir egemenlik olmaksızın barışın mümkün olmadığı varsayımına dayanır.

Modern siyasal düşüncede egemenlik anlayışının özgünlüğü, dünyevi iktidarın ruhani iktidardan ayrılmasıyla yaşanan düşünsel kopuşta aranmalıdır. Bu kopuş göz ardı edildiğinde, laik ulus-devlet kuramının niteliği eksik kalır[1018]. Duguit'nin işaret ettiği üzere, modern ulusal egemenlik kuramı, kralın tanrısal hakkının yerini halkın ya da ulusun tanrısal hakkının almasıyla teolojik bir süreklilik barındırır. Böylece teokrasi ortadan kalkmamış, yalnızca öznesi değişmiştir[1019].

Dijital çağda bu egemenlik modeli niteliksel bir dönüşüm geçirmektedir. Artık bireyler devleti besleyerek tekil ve merkezi bir Leviathan yaratmak yerine, gündelik veri üretimleri aracılığıyla dağınık, ağsal ve görünmez bir egemenlik yapısı inşa etmektedir. Bu yeni Leviathan'ın bedeni veri setleri, algoritmalar, yapay zekâ sistemleri ve dijital altyapılardan oluşur[1020]. Ama işlevi değişmemiştir: davranışları düzenlemek, öngörmek ve denetlemek. Ancak egemenlik, bu kez görünür bir siyasal otorite yerine teknik ve algoritmik bir işleyiş üzerinden tesis edilmektedir. Tanrı ile birey arasındaki ilişki, kullanıcı ile algoritma arasındaki ilişkiye evrilmiş; teslimiyet biçimi değişmiş fakat görünmeyen otoriteye bağımlılık devam etmiştir.

Bu dönüşüm, modern-öncesi dönem ile post-modern dijital çağ arasında dikkat çekici bir yapısal benzerliği ortaya koyar. Orta Çağ boyunca Kilise, gücünü belirli bir toprak parçasına değil, fiziksel sınırları aşan manevi otoritesine dayandırarak yarı-devlet niteliğinde bir iktidar kurmuştur. Günümüzde ise büyük teknoloji şirketleri, dijital altyapılar sayesinde herhangi bir ulusal coğrafyaya yerleşmeden küresel ölçekte fiilî bir güç kullanmakta ve mekânsız bir egemenlik üretmektedir[1021]. Her iki durumda da

---

[1017] Nihat Bulut, "Ölümüne Rekabetten Barış İçinde Yarışa: Hobbes'un Eşitlik Anlayışı", Prof. Dr. Abuzer Kendigelen (ed.) **Prof. Dr. Ömer Teoman'a 55. Yaş Günü Armağanı,** içinde (1377-1397), İstanbul: Beta Yayınevi, 2002, s.1396-1397.

[1018] Akal, *Devlet, Yasa, Hakimiyet*, s.20-21.

[1019] Akal, *Devlet, Yasa, Hakimiyet*, s.28.

[1020] Tristan Thielmann, ve Christoph Borbach, "The Digital Leviathan: Medializing Sovereignty for Critical AI and Data Studies", **communication +1,** vol.11, no.2, (2025), s.1.

[1021] Coroado, s.4.

toprakla sınırlı olmayan bu iktidar biçimi, klasik egemenlik ve hukuki denetim mekanizmalarına yapısal bir meydan okuma oluşturmaktadır.

Teolojik egemenlik anlayışında iktidar, Tanrı'nın mutlak otoritesinden türetilir. Aziz Pavlus'un "Bütün iktidarlar Tanrı'dandır" önermesi, düzen kurma yetkisinin ilahi bir kaynağa dayandığını ifade eder: insanı, toplumu, evreni var eden ve yöneten Tanrı, insanların nasıl yaşayacağına ilişkin kuralları da belirler[1022]. Dijital çağda ise Tanrı'ya atfedilen her şeyi bilen (*omniscient*), her yerde hazır ve nazır olan (*omnipresent*) ve her şeye kadir olma (*omnipotent*) gibi temel sıfatların teknolojik karşılıklar bulduğu görülmektedir. Gözetim ve veri analitiği her şeyi bilme kapasitesini; sürekli bağlantı ve yaygın hesaplama her yerde olma durumunu; içerik filtreleme, sıralama ve erişim kısıtlamaları ise müdahale kudretini temsil eder[1023]. Bu anlamda teknoloji, seküler ve dijital bir Tanrı işlevi üstlenmekte ve insan davranışlarını bilme, öngörme ve yönlendirme kapasitesiyle teolojik egemenliğin dijital yeniden doğuşunu mümkün kılmaktadır.

Bu tablo, Hobbes'un güvenlik ile özgürlük arasındaki dengeye ilişkin temel sorusunu dijital çağda yeniden gündeme taşır. Egemenlik 2.0, yalnızca devletin dijitalleşmesi değil; egemenliğin teknoloji adına yeniden kutsallaştırılmasıdır. Hobbes'un Leviathan'ı açık bir siyasal özne ve hesap verilebilir bir iktidar modeli sunarken, algoritmik düzen aynı işlevi daha görünmez, daha yaygın ve daha az denetlenebilir biçimde yerine getirmektedir. Düzen kurma iddiası artık demokratik rızaya değil, teknik zorunluluk söylemine dayandırılmaktadır.

Bu bağlamda dijital egemenlik, teolojik otoritenin yerini alan bir teknik-otorite rejimi olarak okunabilir. AB, ABD ve Çin gibi farklı dijital yönetişim modelleri, Leviathan 2.0'ın çeşitli tezahürlerini temsil etmektedir. Ancak ortak nokta, egemenliğin artık yalnızca hukukçuların ve siyasetçilerin değil; veri bilimcilerin, mühendislerin ve etikçilerin de müdahil olduğu bir alan hâline gelmesidir[1024]. Leviathan 2.0, giderek Tanrı gibi her şeyi bilen, gören ve yöneten bir veri-Tanrıya dönüşmektedir. Bu dönüşüm,

---

[1022] Uygun, s.168.
[1023] Harari, s.403.
[1024] Ge Xin ve Yiting Wang, "The Algorithmic Leviathan and the Digital Polis: A Review of Global Digital Governance Dilemmas and Pathways", **Chinese Journal of International Review,** Vol.7, No.2, (2025), s.4-6.

kaçınılmaz olarak şu soruyu gündeme getirir: Bu dijital Tanrı'ya kim, nasıl ve hangi meşruiyetle sınır çizecektir?

Teolojide Tanrı, görünmeyen fakat mutlak bir otoritenin düzenleyici gücünü ifade eder. Seküler teoloji ise bu düzenleyici gücün Tanrı yerine devlet, yasa ya da soyut bir ilke tarafından temsil edilmesidir. Modern devlet kuramının temeli dünyevileştirilmiş ilahiyat kavramlarıyken[1025] dijital egemenlik, bu çizgide Tanrısal düzenin teknik bir formda yeniden vücut bulması olarak değerlendirilebilir. Teolojik egemenlikte itaat inançla, seküler egemenlikte yurttaşlıkla, dijital egemenlikte ise uyum (compliance) mekanizmalarıyla sağlanmaktadır[1026]. Egemenliğin dijital formu, eski teolojik mirası teknolojik bir zeminde yeniden üretmektedir. "Tanrı her şeyi görür" söyleminin yerini "veri her şeyi kaydeder", "Tanrı yargılar" ifadesinin yerini ise "algoritma sıralar ve engeller" almıştır. Egemenliğin tarihsel evrimi, Tanrı-devlet-algoritma hattında süreklilik gösterirken, biçimi değişse de temel işlevi olan insan davranışını tanımlamak, sınırlamak ve düzenlemek sabit kalmıştır. Tanrı, devlet ve veri sistemleri, farklı tarihsel bağlamlarda "görünmeyen fakat düzenleyici" güçler olarak işlev görmüştür. Bu tablo, egemenliğin biçim değiştirse de temel işlevinin (insan davranışını tanımlamak, sınırlamak ve düzenlemek) sabit kaldığını göstermektedir.

Son aşamada teknolojik gelişmeler, bu dönüşüm döngüsünün belirleyici unsuru hâline gelmiştir. Rönesans ve Aydınlanma, siyasal iktidarı ilahi referanslardan koparark akıl ve irade temelinde yeniden tanımlamış; modern devlet bu süreçte doğmuştur[1027]. Makyavelizm; iktidarın temelini erdem veya iyilikte değil, güç ve akılcı stratejide gören; siyasal mekanizmayı ahlaki süslemelerden arındırarak tarihsel gerçeklik ve saf mantık üzerinden okuyan özgün bir düşünce biçimi sunmuştur[1028]. Reformasyon, bireyi kilise otoritesinden kurtararak Tanrı ile doğrudan ilişki kurmasını sağlamış; Hobbes bu özgür bireyi kaostan korumak adına devlete teslim etmiş ve insanlar devleti yeryüzüne

[1025] Carl Schmitt, **Siyasi İlahiyat Egemenlik Kuramı Üzerine Dört Bölüm,** A. Emre Zeybekoğlu(çev.), Ankara: Dost Kitabevi, 2005, s.41-42.
[1026] Daria Gritsenko ve Matthew Wood "Algorithmic governance: A modes of governance approach", **Regulation & Governance,** Vol.16, (2022), s.45-46.
[1027] Şenel, s.307; Uygun, s.202-203.
[1028] Akkaya Kia, *"Post Modern Zamanlarda Machiavelli Okumak",* s.121.

indirmiştir[1029]. Bugün ise devletin düzenleyici rolü giderek veri sistemleri ve algoritmalar tarafından üstlenilmektedir. Disiplinin aracı artık din ya da yasa değil, kod ve otomatik denetim mekanizmalarıdır[1030]. Birey Tanrı'ya değil veriye hesap vermekte; yargı süreçleri yerini algoritmik sınıflandırmalara bırakmaktadır. Bu durum, dinsel, hukuksal ve teknolojik egemenlik biçimlerinin birleşerek daha incelmiş, daha görünmez ve daha kapsamlı bir disiplin rejimi oluşturduğunu göstermektedir.

B. Modus Disrupti[1031]: Dijitalleşmenin Egemenlik Üzerindeki Aşındırıcı Etkisi

1. Devletin Egemenlik Niteliği Açısından

a. Devletin; Hukuk, Yasa ve Zor Tekelinin Dijital Alanda Aşınması: Platformların Monist Hukuka Müdahalesi

Modern devlet bağlamında hukuk, yalnızca davranışları düzenleyen normatif bir sistem değil; egemen iktidarın toplumsal alanı kuran ve sürdüren asli aracıdır. Normların bağlayıcı nitelik kazanabilmesi, bu normları ihlal eden davranışları değerlendirecek ve yaptırım uygulayacak üstün bir iktidarın varlığını zorunlu kılar[1032]. Bu yönüyle hukuk, salt güç kullanımına indirgenemez; aksine, toplumsal ilişkileri öngörülebilirlik ve düzen içinde değerlendirmeyi mümkün kılan kurumsal bir iktidar biçimi olarak ortaya çıkar[1033]. Hukuk ile egemenlik arasındaki ilişki, bu nedenle tali değil, kurucu bir ilişkidir.

[1029] Akkaya, *Küreselleşme Olgusu Karşısında Ulus Sorunu*, s.54.

[1030] Antoinette Rouvroy ve Thomas Berns, "Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships?", **Réseaux**, Cilt.2013/1, No.177, (2013), s. X-XIII.

[1031] Latince'de modus kelimesi, düzenli bir işleyiş biçimini veya tarzı ifade ederken; disrupti kelimesi, "kopmuş, çözülmüş, dağılmış" anlamına gelir. **Online Latin Dictionary,** "modus", "disrupti" https://www.online-latin-dictionary.com/ (E.T.: 1 Şubat 2026. Bu nedenle modus disrupti, yalnızca bir farklı tarz değil, tarzın kendisinin işlevsizleşmesi, yani yöntemin yıkılmasıdır. Buradaki semantik vurgu, egemenliğin kendi işleyiş ilkesini kaybettiği ve var olan bütünselliğin bozulduğu anlamına gelir. Siyasal anlamda modus disrupti, devletin egemenlik iddiasının zayıfladığı alanları işaret eden anlamda kullanılmıştır. Bu, doğrudan bir egemenin yıkılması değil, egemenliğin işlevinin özünden başka gayrimeşru, belirsiz veya merkezi olmayan güçler tarafından ikame edilmesidir. Devlet otoritesinin hem zayıfladığı hem egemenliğinin parçalanarak yayıldığı bir izmihlal halidir.

[1032] Uygun, s.11; Doehring, s.1.

[1033] Mehmet Tevfik Özcan, "Hukuk Olgusunun Sosyolojik Elemanları", **Mahmut R. Belik'e Armağan,** İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Yayını, (1993), s.317.

Modern hukuk düzeninde norm ile yasa arasındaki ayrım giderek silikleşmiş; hukuk, soyut ilkeler bütününden çıkarak yazılı, genel ve bağlayıcı kurallar sistemine dönüşmüştür. Yasa, yalnızca teknik bir düzenleme değil; belirli bir toplumun tarihsel, kültürel ve sosyolojik birikimini yansıtan kurucu siyasal iradenin ürünüdür. Devlet, yasama, yürütme ve yargı erkleri aracılığıyla hukuku üretir ve uygular; zor kullanma tekeline sahip olması sayesinde bu normatif düzeni fiilen geçerli kılar. Bu bağlamda hukuk ve yasa, yalnızca normatif bir düzen değil, devlet egemenliğinin maddi dayanakları hâline gelir[1034].

Klasik egemenlik kuramına göre egemenlik tek, bölünmez ve süreklidir. Siyasal topluluk içinde farklı otoriteler bulunabilse de nihai karar verme yetkisi tek bir merkezde toplanır ve modern dönemde bu merkez devlettir[1035]. Egemenliğin asli sahibi olabilmek, meşru iktidar (*auctoritas*) ile zor kullanma yetkisinin (*potestas*) aynı bünyede birleşmesini gerektirir[1036]. Bu birliktelik devleti egemen konuma getireceğinden[1037] devlet için olmazsa olmaz şarttır (*conditio sine qua non*); devleti süreklilik taşıyan soyut fakat kurumsal bir varlık hâline getirir. Egemenin mutlaklığı en açık biçimde yasa ile kurduğu ilişkide görünür; yasa, egemenin tek taraflı buyruğudur ve muhatapların rızasına dayanmaz[1038].

Bu yaklaşım Hobbes'un kuramında teorik zirvesine ulaşır. Hobbes'a göre egemen, içte yasayla, dışta ise devletler arası doğa durumunda hareket eder. Yasayı koyan, değiştiren ve kaldıran tek otorite egemendir; kendisinden üstün bir güç tanımadığı için yaptığı yasalara dahi bağlı değildir[1039]. Bu anlayış üzerine inşa edilen modern hukuk düzeni, tek merkezli norm üretimine dayanan monist bir yapı sergiler. Hukukun kurucu öznesi devlettir; normlar tek merkezden üretilir ve hiyerarşik bir yapı içinde uygulanır.

[1034] Muharrem Kılıç, "Bilgi-İktidar İlişkisi Bağlamında Yasa Düşüncesi: İktidarın Yasa(l)laşması", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII, Sayı.1, (2014), s.175-176.
[1035] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.344.
[1036] Abdurrahman Saygılı, "Modern Devlet'in Beden İdeolojisi Üzerine Kısa Bir Deneme", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.54, Sayı.3, (2005), s.331.
[1037] Saygılı, *"Jean Bodin'in Egemenlik Anlayışı Çerçevesinde Kralın İki Bedeni Kuramına Kısa Bir Bakış",* s.194.
[1038] Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.27, 31.
[1039] Sevtap Metin, "Oyun Teorileri Işığında Thomas Hobbes'un Sosyal Sözleşme Kuramının Analiz ve Yorumu", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII Sayı.1, (2014), s.248.

Yargılama faaliyeti kamusal bir yetki olarak yalnızca devlete aittir ve egemenliğin en görünür tezahürlerinden birini oluşturur[1040]. Yasa koyma ve kaldırma yetkisi kimdeyse egemen de odur. Egemenin bu niteliklerine aykırı bir pozisyonun varlığı, onu yok etmekle birdir. Yasa, yalnızca egemenin varlığında ortaya çıkar[1041].

Modern döneme geçişle birlikte hukukun meşruiyet kaynağı giderek aşkın otoritelerden ayrışmış, dünyevileşmiş; egemenlik anlayışı ise monarşik kişilikten koparak ulusa atfedilmeye başlanmıştır[1042]. Böylece hukuk, toplumun kendi ihtiyaçları doğrultusunda insan aklının ürünü olarak kurgulanan bir düzen hâline gelmiştir[1043]. Bu dönüşüm, Orta Çağ'ın parçalı ve çoğul hukuk düzenlerinin yerini yazılı, genel, soyut ve öngörülebilir kurallara dayanan tekçi bir hukuk sistemine bırakmasını beraberinde getirmiştir. Hukukun rasyonelleşmesi, bir yandan kapitalist ekonomik düzenin ihtiyaçlarına cevap verirken, diğer yandan devletin egemenlik iddiasını kurumsal olarak pekiştirmiştir[1044].

Bu tarihsel bağlamda yasaların toplumsal temeli daha görünür hâle gelir. Montesquieu'nün ifadesiyle yasalar, belirli toplum-ülke-insan ilişkilerinin zorunlu bir sonucudur. Yasaların ruhu, bu ilişkiler bütününde konumlanır. Yasalar toplumu biçimlendirirken, toplum da yasaları biçimlendirir[1045]. Modern demokrasilerde egemenlik yetkisi ulusa ait olmakla birlikte, bu yetkinin kullanımı devlet aracılığıyla gerçekleşir. Böylece ulus, egemenliğe hukuki ve fiilî meşruiyet kazandıran özne hâline gelirken, siyasal otorite de dünyevî ve kurumsal bir nitelik kazanır[1046].

Bu gelişmelerle birlikte kamu hukukunun merkezîleşmesi, hukuku giderek bir "iktidar hukuku" hâline getirmiştir. Hukuk artık yalnızca pozitif normlar bütünü değil; siyasal iktidar tarafından üretilen ve zor kullanma yetkisiyle desteklenen kurumsal bir

---

[1040] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.31, 66, 99.
[1041] Akad, Dinçkol ve Bulut, s.108-110, 116.
[1042] Akal, *Devlet, Yasa, Hakimiyet*, s.20.
[1043] Uygun, s.8.
[1044] Akad, Dinçkol ve Bulut, s.91.
[1045] Akad, Dinçkol ve Bulut, s.142-143.
[1046] Akal, *Devlet, Yasa, Hakimiyet*, s.37.

sistemdir[1047]. Kelsen'in ifadesiyle devlet ve hukuk, aynı cebri düzenin iki farklı görünümüdür. Aynı sosyal topluluğun iki farklı sistem tarafından inşa edilmesi mümkün olmaması nedeniyle özdeştirler[1048]. Devlet, kurumsal yapı olarak; hukuk ise bu yapının normatif düzeni olarak varlık kazanır. Hukuku diğer normatif sistemlerden ayıran temel unsur, devlet gücüyle konulması ve korunmasıdır[1049]. Muallim Mithat Bey de bunu veciz ifadesi ile "*hukukun menşei devlettir*" olarak ifade etmiştir[1050]. Bu yaklaşımda adalet yasallıkla; hukuk yasayla; yasa ise devlet iradesiyle özdeşleştirilir. Hukuk dışındaki normlar ise ancak yargı kararlarıyla desteklenip uygulanınca hukuk kuralı niteliği kazanır[1051]. Bu nedenle modern devlet, ancak fiilen işleyen bir hukuk düzeniyle varlık kazanır[1052]. Bu sistem, tek hukuk kaynağı olarak halk iradesini; demokrasinin her durumda adaleti sağlayacağı varsayımına dayandığını kabul eder[1053].

Bu çerçevede modern devlet; hukuk, yasa ve meşru zor tekeli üzerinden tanımlanmış; egemenlik, norm üretimi, yargılama ve yaptırım yetkilerinin tek merkezde toplanmasıyla kurumsallaşmıştır. Monist hukuk mimarisi olarak adlandırılabilecek bu yapı, hukukun kaynağını devlette konumlandırmış ve yargılama faaliyetini kamusal bir yetki olarak yalnızca devlet organlarına atfetmiştir. Ancak bu teorik bütünlük, dijitalleşme süreciyle birlikte fiilî olarak zorlanmaya başlamıştır.

Dijital platformlar, hizmet şartları ve topluluk kuralları aracılığıyla kullanıcı davranışlarını değerlendirmekte; içerik kaldırma, hesap askıya alma ve erişim sınırlandırma gibi işlemler yoluyla yaptırıma benzer sonuçlar doğuran bir düzenlilik tesis

---

[1047] Akad, Dinçkol ve Bulut, s.121-122; Rukiye Akkaya, "Kamu Hukuku Eğitiminin Fransa'da Tarihsel Kökleri ve Kamu Hukuku Okulları Üzerine Notlar", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.VII, Sayı.3-4, (2003), s.143, 155.

[1048] Hans Kelsen, **Saf Hukuk Kuramı: Hukuk Kuramının Sorunlarına Giriş,** Ertuğrul Uzun (çev.), İstanbul: Nora Kitap, 2020, s.122-124.

[1049] Uygun, s.12.

[1050] Muallim Mithat Bey, "Hukuku Amme Dersleri", İÜHFM, Sene.VIII, Sayı.46, (Şubat 1930), s.6 Aktaran: Rukiye Akkaya Kia, "Darülfünun'dan 1933 Üniversite Reformuna; Hukuk-i Siyasiye-i Osmaniye Derslerinden, Hukuk-i Âmme Derslerine Dönüşüm ve Genel Kamu Hukuku Dersinin Geçmişine Dair Notlar II", **Journal of Istanbul University Law Faculty,** Cilt.70, No.1, (2012), s.690.

[1051] Mehmet Tevfik Özcan, "Hukuk Olgusunun Sosyolojik Elemanları", **Mahmut R. Belik'e Armağan,** İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Yayını, (1993), s.310–311.

[1052] Rukiye Akkaya Kia, "Ulusal Ekonomi ve Girişimcilik Üzerine 1329 (1913) Tarihli ve Yazarı Belli Olmayan Bir Risale", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.24, No.2, (Aralık 2018), s.519.

[1053] Akal, *Devlet, Yasa, Hakimiyet*, s.24.

etmektedir. Bu süreçte platformlar; norm koyma, normu yorumlama ve normu uygulama işlevlerini teknik ve organizasyonel düzenekler aracılığıyla yerine getirmekte; böylece devletin klasik olarak kendisine ait sayılan yargılama ve yaptırım işlevleri, dijital alanda yeniden üretilmektedir. Algoritmik denetim mekanizmaları; ifade özgürlüğü, özel hayatın gizliliği ve haberleşme hürriyeti gibi temel hak alanlarına doğrudan temas eden kararlar almakta ve bu kararları fiilen icra edebilmektedir[1054]. Big Tech şirketlerinin bu faaliyetleri, algoritmaların önceden belirlenmiş amaçlar doğrultusunda insan topluluklarının davranışlarını şekillendirmek, kısıtlamak ve koordine etmek ya da riskleri yönetmek üzere kullanıldığı algoritmik regülasyon olarak nitelendirilmektedir[1055].

Bu durum, monist hukuk anlayışı açısından yapısal bir gerilim yaratmaktadır. Platformlar hukuken egemen değildir; ancak fiilen egemenliğe özgü işlevler üstlenmektedir. Biçimsel olarak özel sözleşmelere dayanan bu kararlar, etkileri bakımından kamusal yaptırımlara benzer sonuçlar doğurmakta; böylece platformlar, devletin hukuk, yasa ve zor tekelini dijital alanda fiilen paylaşan aktörler hâline gelmektedir. Oysa yasa, karşılıklı rızaya dayalı özel hukuk sözleşmeleriyle değil; egemenin tek taraflı kamusal buyruğuna dayanır[1056]. Egemenliğin monist yapısı; yasa koyma iradesi, zorlayıcı gücü ve yargılama yetkisinin tek merkezde toplanması gerektiğini aksi halde kargaşa doğacağını savunduğundan[1057] bireylerin teknoloji şirketleriyle kurduğu sözleşmesel ilişkiler egemenliğin hukuki kaynağı olamaz. Bu nedenle platform sözleşmeleri, kamusal yetki ve meşru zor kullanma gücü üretmeye elverişli değildir.

[1054] Örneğin Hindistan'daki Bilgi Teknolojileri (Aracı Kurumlar) Kuralları'nın 12. maddesi, platformların içerik yönetimi için kendi denetim mekanizmalarını kurabilmesine izin verir, ancak bunun bazı şartlara bağlı olduğunu belirtir.

[1055] Erol, s.29.

[1056] Roma hukukunda lex, hükümran otorite tarafından konulan bağlayıcı buyruk anlamını taşır. Latince lex (kanun), ligere (bağlamak) sözcüğünden gelir Yasa, hükümran otoritenin tek taraflı buyruğu; sözleşme ise tarafları karşılıklı olarak bağlayan bir ilişkidir. Nasıl ki din adamlarının iddia ettiği üzere Papa'nın eli hiçbir zaman bağlı değilse, egemen hükümdar da dilediği anda güçsüz kılınamaz. Bu nedenle ferman ve emirnamelerin sonunda sıklıkla şu ifade yer alır: "Çünkü Biz Böyle İstiyoruz." Bu ibare, hükümdarın yasalarının her ne kadar iyi ve geçerli gerekçelere dayansa da nihayetinde onun mutlak ve açık iradesine tâbi olduğunu açıkça gösterir. Kriegel, s.21-24; Ağaoğulları ve Köker, *Kral-Devlet ya da Ölümlü Tanrı*, s.28.

[1057] Şenel, s.314; Kriegel, s.19-20.

Örneğin, ABD'li teknoloji şirketi eBay, satıcı ve alıcılar arasındaki anlaşmazlıkları çözmek için çevrimiçi bir arabuluculuk programı oluşturmuştur. Bu program, kullanıcıların sorunlarını hızlı ve etkili şekilde çözmesine yardımcı olur. Devlete ait olması gereken yetkilerin özel aktörler tarafından fiilen kullanılması egemenliğin aşındırılması hatta egemenliğin kaçırılması anlamına gelir ve bireyleri bu yapılar karşısında korunmasız bırakır. Rızaya değil güce dayalı olarak genişleyen bu fiilî egemenlik alanı, hukuki meşruiyet üretmez. Kamu hukuku disiplini, egemen iradenin onayına dayanmadıkça bu güçlerin egemen gibi davranmasını ne teorik ne de normatif olarak kabul eder. Egemenliğin üstün ve sürekli olma niteliği, devletin dijital alanlarda da meşru otoritesini sürdürmesini; veriler üzerinde denetim kurmasını ve sınır aşan veri akışının kontrolünde kendisinden güçlü bir dijital aktörün ortaya çıkmamasını gerektirir. Buna karşın büyük teknoloji şirketleri, kendilerini küresel hizmet sağlayıcılar ve dijital altyapı yöneticileri olarak konumlandırmakta; bu statü üzerinden kendilerine özgü bir düzenleme rejimi talep etmektedir. Bu durum, onları yalnızca ekonomik değil, aynı zamanda sosyo-politik kararlar alabilen fiilî dijital kamu otoritelerine dönüştürmekte; meşruiyet ve hesap verebilirlik sorunlarını derinleştirmektedir. Oysa kamu yararı şirketlerce tanımlanamaz; bu nedenle egemenliğin dijital düzlemde yeniden tanımlanması ve uluslararası iş birliğiyle güçlendirilmesi gereklidir[1058].

Yetki kullanımı ile egemenlik arasındaki ayrım bu noktada belirleyici hâle gelir. Güçleri ne kadar büyük olursa olsun, başka bir iradenin komutasına bağlı olan aktörler egemen sayılamaz. Teknik icra kabiliyeti, meşru zor kullanma hakkı değildir. Egemenlik, yalnızca zor ve buyruğa indirgenebilir bir iktidar biçimi değil; meşruiyet, rıza ve koruma ilişkisiyle birlikte işler[1059]. Egemen olmayan aktörlerin egemen gibi davranması ise bireyleri korumasız bırakmakta ve hukuk devleti ilkesini aşındırmaktadır.

Dijital platformların fiilî normatif rejimleri, anayasal ilkeleri görünüşte taklit etmekte; ancak içeriksel olarak bu ilkeleri boşaltmaktadır. Topluluk kuralları ve şirket içi denetim mekanizmaları, anayasa benzeri bir dil kullanarak meşruiyet üretmeye

[1058] Christakis, s.13.
[1059] Hardt ve Negri, *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,* s.347.

yönelmekte[1060] fakat yetkilerini demokratik bir iradeden değil, doğrudan kurumsal çıkar ilişkilerinden almaktadır. Kâr amacıyla hareket eden bu aktörlerin kamusal amaçlarla uyumlu ve kamu yararını önceleyen bir yönelim taşıyıp taşımadığı ise yapısal olarak her zaman tartışmaya açıktır[1061]. Nitekim milyarlarca kullanıcı için "uygun" ve "uygunsuz" davranışı belirleyen fiilî normatif rejim, kamusal denetime tabi olmaksızın anayasal dil ve kavramlarla cilalanabilmekte; insan hakları söylemi, toplumsal güç ilişkilerini dönüştüren bir araç olmaktan çıkarak marka itibarı, yatırımcı güveni ve piyasa konumu gibi ekonomik değerleri güçlendiren bir yönetişim retoriğine indirgenebilmektedir. Bu durumda anayasacılık, kamu yararı temelli kamusal denetimi güçlendirmek yerine, özel iktidarın yeniden üretildiği ve metalaştırıldığı bir meşruiyet mekanizmasına evrilir[1062]. Oysa anayasaların temel amacı ister devlet ister başka bir güç odağı olsun, iktidarı sınırlamak ve bireylerin özgürlüğünü güvence altına almaktır[1063]. Nitekim Anayasa Mahkemesi'nin haberleşme özgürlüğüne ilişkin bir kararında, hâkim onayı olmaksızın resen erişim engeli uygulanmasının Anayasa'nın öngördüğü koruma mekanizmalarıyla bağdaşmadığının vurgulanması, dijital alandaki müdahalelerin hangi aktör tarafından gerçekleştirilirse gerçekleştirilsin güçlü bir anayasal denetime tabi olması gerektiğini açıkça ortaya koymaktadır[1064]. Bu nedenle yargılama yetkisinin devlet dışı biçimlerce ikame edilmesi, yalnızca teknik bir yönetişim sorunu değil, egemenliğin niteliğine ilişkin doğrudan ve yapısal bir kırılma olarak değerlendirilmelidir.

Dijital platformların kararları hukuki anlamda yargılama değildir; fakat fiilî etkileri, bireylerin temel haklarını ciddi biçimde etkileyebilmektedir. Savunma hakkı, silahların eşitliği, gerekçelilik ve bağımsızlık gibi güvenceler bu süreçlerde çoğu zaman devre dışı kalmaktadır. Bu belirsizlik, kararların ekonomik çıkarlar veya dışsal siyasal talepler doğrultusunda şekillenebildiği kuşkusunu artırmakta; veri güvenliği ve dijital haklar açısından ciddi riskler doğurmaktadır[1065]. Bu nedenle öğretide, anayasal

[1060] Coroado, s.12-13.
[1061] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.32.
[1062] Engin Yıldırım, "Meta Gözetim Kurulu: Meta'nın 'Anayasa Yargısı' mı, Anayasacılığın Metalaşması mı?", **GSÜHFD**, Cilt.2025, No.2, (2025), s.1055-1057.
[1063] Akad, Dinçkol ve Bulut, s.183.
[1064] AYM Kararı, 15/11/2017, E.2015/76, K.2017/153, par. 27.
[1065] Hatipoğlu Aydın, s.105-106.

demokrasinin temel ilkelerinin özel sektöre taşınması ve kullanıcıların platform karar süreçlerinde söz sahibi olması gerektiği yönündeki yaklaşımlar güçlenmektedir[1066].

Öte yandan dijital alanda ortaya çıkan normatif yapı, hukuki birlik yerine parçalı ve öngörülemez bir düzen üretmektedir. Bir platformdan kaldırılan içeriğin başka bir platformda serbestçe dolaşıma girmesi, sorumluluğun belirlenmesini güçleştirmekte ve fiilî bir düzensizlik doğurmaktadır. Platformlar arası tutarsızlık, normatif bir dağınıklık yaratmakta; hangi davranışın hangi ölçütlere göre değerlendirileceği belirsizleşmektedir. Bu durum, tarihsel olarak feodal beylerin kendi topraklarında yargılama yetkisi kullandığı Orta Çağ'ın parçalı hukuk düzenlerini çağrıştırmakta; ancak bu kez anayasal güvencelerden ve kamusal denetimden yoksun bir dijital çoğulluk ortaya çıkmaktadır[1067].

Bu bağlamda dijital platformların self-regülasyonu tercih etmesi, kamu yararı ve temel hakların korunması açısından ciddi sorunlar doğurmaktadır. Dış denetimden kaçınma ve ticari çıkarları koruma amacıyla geliştirilen bu yaklaşım; şeffaflık, hesap verebilirlik ve hukuki kesinlikten yoksundur. GDPR sürecinde görüldüğü üzere, büyük teknoloji şirketlerinin bağlayıcı düzenlemelere karşı seçici ve isteksiz tutumu, self-regülasyonun sınırlarını açıkça ortaya koymuştur[1068]. Platformların düzenleyici çerçeveleri, hakların korunmasından ziyade şirket çıkarlarına göre şekillenmekte; bu durum kamusal düzenleme ihtiyacını daha da görünür kılmaktadır.

Sorun, egemenliğin ortadan kalkması değil; dijital bağlamda yeniden tanımlanması gereğidir. Ulusötesi teknoloji şirketleri; veri işleme gücü sayesinde temel hak ve özgürlükler üzerinde fiilî etki kurmakta; hukukun üstünlüğü ve demokratik düzen açısından devletlerle rekabet edebilen bir konuma yerleşmektedir. Bu süreçte platformlar, klasik ülkesel egemenlik yerine işlevsel bir egemenlik anlayışı inşa ederek, dijital alandaki hakların varlığını ve kullanım biçimlerini özerk biçimde belirleme iddiasında bulunmaktadır. Düzenleyici ve bağlayıcı bir hukuki çerçevenin eksikliği ise bu şirketlerin

---

[1066] Küzeci, s.232, 354.

[1067] Işık, s.10, 33; Uygun, s.165.

[1068] GDPR doğrultusunda, Microsoft küresel uyum yönünde adım atarken, Facebook korumayı AB ile sınırlayarak çok sayıda kullanıcıyı düzenleyici denetim dışında bırakmış; böylece hakların korunmasından ziyade kendi çıkarları doğrultusunda hareket ettiğini göstermiştir. Çelik ve Aydoğan, *"Sosyal Medyada Hukuku Yerleşik Kılma Çabaları",* s.307-308.

küresel ölçekte fiilî bir dijital hukuk üretmesine zemin hazırlamaktadır[1069]. Fakat dijital alan bütünüyle egemenlik dışı değildir; aksine, egemenlik iddialarının teknik ve hukuki düzlemde yeniden kurulduğu bir mücadele alanıdır. Dijital altyapıların maddi varlığı, veri merkezleri ve ağ yapıları büyük ölçüde devletlerin denetimi altındadır[1070]. Bu nedenle çözüm, egemenliği inkâr etmek değil; dijital alanda demokratik meşruiyet, hukuki denetim ve kamu yararı ekseninde yeniden kurmaktır.

Uluslararası hukukta Vestfalya'dan bu yana devletlerin ülkesel egemenliği ve hukuki eşitliği temel ilke olarak korunmuş; Birleşmiş Milletler çerçevesinde de devletlerin dijital altyapı ve yargı yetkisi üzerinden düzenleme iddiaları genel olarak kabul görmüştür[1071]. Bununla birlikte, dijital bilginin sınır aşan doğası ve özel sektör kontrolünün yoğunlaşması, klasik egemenlik anlayışının yetersizliğini de görünür kılmakta; demokratik meşruiyet ve hukuki denetimle uyumlu yeni bir dijital egemenlik anlayışını zorunlu hâle getirmektedir[1072].

Hukuk devletinde yargı erki anayasal düzenin amaçlarının üzerinde konumlanmış bir güç değildir. Anayasal kurumlar, görevlerini yerine getirirken özgürlükçü demokrasinin korunmasını esas almalı ve kendi fonksiyonel sınırları içinde kalmalıdır. Kurumların görev alanlarını aşarak siyasal tutum alır görünmesi, yalnızca erkler ayrılığını değil, devlet otoritesinin meşruiyetini de zayıflatır[1073]. Bu nedenle dijital alanda ortaya çıkan yeni güç merkezleri karşısında çözüm, yargısal veya idari yetkinin

---

[1069] Sezen Kama Işık, "Klasik Anayasacılıktan Dijital Anayasacılığa: Anayasa Hukukunun Dönüşümü", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (75-96), İstanbul: Adalet, 2021, s.88.

[1070] Gourley, s.279.

[1071] Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmeler Üzerine Hükümet Uzmanları Grubu, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015, https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf (15 Aralık 2024), s.2-3; Vestfalya sisteminin kuruluşundan bu yana devletler, ülke sınırları içinde yalnızca kendi egemenliklerini tanır. Uluslararası hukuk, modern devletlerin ülkesel sınırları üzerinde egemen eşitliğini ve toprak bütünlüğüne saygıyı temel ilke olarak benimser. Christakis, s.4-5.

[1072] Floridi, s.372.

[1073] Dönmezer, s.2.

genişletilmesi değil; egemenliğin demokratik meşruiyet, hukuki denetim ve kamu yararı ekseninde yeniden tanımlanmasıdır.

Buna karşın, AB Dijital Hizmetler Yasası'nın 20. maddesinde, platformların tıpkı bir yasama erki gibi kendi kurallarını oluşturması ve yürütme erki gibi bunların uygulanmasını sağlaması ve nihayet bu kurallara aykırılık tespit etmeleri halinde yargı erki benzeri müeyyideler uygulaması öngörülmektedir[1074]. Düzenleme, platformların kendi kurallarını oluşturmasını, bu kuralları uygulamasını ve ihlal hâlinde yargısal nitelik taşıyan müeyyideler öngörmesini kabul ederek, norm üretimini devlet tekelinin dışına taşımaktadır. Bu durum, küreselleşmenin daha önce başlattığı tek ülke-tek hukuk ilkesinin fiilî aşınmasının dijitalleşmeyle hızlandığını ve derinleştiğini göstermektedir[1075]. Böylece modern hukukun hiyerarşik norm piramidi yerini giderek yatay ilişkiler ağına bırakmakta; bağlayıcı "hard law" düzenlemelerin yanında esnek "soft law" mekanizmaları yaygınlaşmakta, normların kaynağı ve uygulanma alanı karmaşıklaşmaktadır[1076]. Big Tech şirketleri, hizmet şartları aracılığıyla kendi kurallarını koyarak fiilî bir "özel hukuk düzeni" tesis etmekte hem düzenlenen hem de düzenleyici aktör konumuna yerleşmektedir. Bu yapı, bireylerin devlet aracılığı olmaksızın doğrudan dijital şirketlerle karşı karşıya kalmasına, ulus-ötesi aktörler karşısında korunmasızlaşmasına ve küresel dijital gücün hukuk yoluyla nasıl ve ne ölçüde sınırlandırılacağına ilişkin belirsizliğin sürmesine yol açmaktadır.

Sonuç olarak dijitalleşme, devletin geleneksel otorite araçlarını ortadan kaldırmamış; fakat bunların dijital alandaki münhasırlığını zayıflatmıştır. Dijital platformlar hukuken egemen değildir; ancak fiilen egemenliğe özgü işlevler üstlenmektedir. Bu durum, monist hukuk varsayımını kırılgan hâle getirmektedir. Bununla birlikte, dijital alanda bireysel haklar üzerindeki fiilî etki artık yalnızca devletin yargı, kolluk ve idari organlarıyla sınırlı değildir; platform işletmecileri de bu alanda asli aktörler hâline gelmiştir. Ne var ki bu yetkinin, demokratik meşruiyet, kuvvetler ayrılığı

[1074] Mesut Serdar Çekin, "Dijital Çağda Anayasa Yargısı: Özel Hukuk Perspektifinden Bir. İnceleme", **Anayasa Yargısı,** Cilt.42, Sayı.1, (2025), s.597.
[1075] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.98-101.
[1076] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.117-124.

ve denge-denetim mekanizmalarına tabi olmayan özel aktörler tarafından kullanılması, kaçınılmaz olarak anti-demokratik sonuçlar doğurmaktadır[1077]. Bu nedenle, hukukun geleceği, egemenliği inkâr ederek değil; dijital alanda yeniden kurarak, temel hak güvencelerini ve kamusal denetimi güçlendiren yeni bir normatif mimariyle güvence altına alınabilir.

b. Bilgi Üzerindeki Egemenliğin Aşınması

Egemenliğin tekilliği, modern devlette yalnızca meşru zor kullanma tekelini değil; aynı zamanda bilgi, iletişim, kültür ve eğitim alanlarında norm koyma ve yönlendirme kapasitesini de içerir. Egemenlik, devredilemez ve parçalanamaz bir nitelik taşır; yalnızca belirli yetkilerin kullanımının görev, süre ve kapsam bakımından devri mümkündür. Egemenliğin kendisinin devri ise, hukuki anlamda yeni bir egemenin ortaya çıkması anlamına gelir. Bu nedenle bilgi üzerindeki denetim, egemenliğin tali bir unsuru değil, onun kurucu bileşenlerinden biridir.

Modern devletin toplumsal hayatı düzenleme ve yönlendirme iddiası, bilgi ve iletişim alanını da kaçınılmaz biçimde siyasal iktidarın müdahale sahasına dâhil etmiştir[1078]. Hukuk, örf ve kurumlar yoluyla toplumsallığı kuran devlet, aynı zamanda bilginin üretimi, dolaşımı ve meşrulaştırılması süreçlerini de kuşatmıştır[1079]. Analog dönemde bu denetim; istihbarat faaliyetleri, kamu kayıtları, eğitim politikaları ve kitle iletişim araçları üzerinden tesis edilmiştir. Devlet, hükmettiği uzamda bilgiye hâkim olmayı, yönetim kapasitesinin zorunlu bir koşulu olarak görmüştür. Bu yönüyle devlet, toplumsal ilişkileri gördüklerimizin dışında görmediklerimiz üzerinden de biçimlendiren sayısız kılcal damarlardan oluşan bir kas yığınına benzetilmektedir[1080].

[1077] Zeynep Ardıç, "Sosyal Medyaya İnsan Hakları Perspektifinden Bakış: İfade Özgürlüğünün Sınırlandırılması", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (251-268), İstanbul: Adalet, 2021, s.263-264.

[1078] Akal, *Modern Düşüncenin Doğuşu: İspanyol Altın Çağı,* s.231.
[1079] Kılıç, s.174.
[1080] Abdurrahman Saygılı, **Kutsal Canavar Devlet,** Ankara: Yetkin Yayınları, 2021, s.33.

Dijitalleşme, bu yerleşik dengeyi yapısal biçimde sarsmıştır. İnternetin merkezsiz mimarisi, düşük maliyetli içerik üretimi ve sınır aşan dolaşım kapasitesi, bilginin ulusal sınırlar içinde tutulmasını güçleştirmiştir[1081]. Telefon, radyo ve televizyon gibi klasik iletişim araçlarının aksine internet, siyasal denetimleri büyük ölçüde aşabilen bir iletişim alanı sunar. Bu dönüşüm, bireysel mahremiyet tartışmalarını aşan bir nitelik taşımakta; bilginin, bilmenin ve dolayısıyla iktidarın doğasını köklü biçimde dönüştürmektedir[1082].

Dijital teknolojilerin yaygınlaşmasıyla birlikte siyasal gücün yalnızca devlet kurumlarında değil, özel sektör aktörleri ve ağlar içinde örgütlenen platformlarda da yoğunlaştığı görülmektedir. Bu kayma, kamu-özel ayrımını bulanıklaştırmakta; temsilî demokrasinin dayandığı rasyonel müzakere zeminini aşındırmaktadır[1083]. İnternetin başlangıçta atfedilen demokratikleştirici potansiyeline karşın, algoritmalar tarafından şekillendirilen yankı odaları ve tepkisel kamusallık biçimleri, kamusal tartışmayı kırılgan hâle getirmiştir. Böylece teknolojinin, uygun denetim mekanizmaları olmaksızın demokrasiyi güçlendirmek yerine zayıflatabileceği yönündeki endişeler güç kazanmıştır.

Dijital çağda bilgiyle ilgili devlet kurumları idarenin ayrılmaz bir parçası hâline gelmiş olsa da ve bilgi, görünür şekilde devletin drije ettiği bir alan gibi ele alınsa da dijital alanın sınır tanımayan yapısı devletin bilgiye erişim ve bilgiyi denetleme kapasitesini paradoksal biçimde sınırlamaktadır. Bir yandan devlet, dijital veriye her zamankinden daha fazla ihtiyaç duymakta; diğer yandan sanal engeller, platform mimarileri ve sınır ötesi veri akışları nedeniyle bu veriye fiilen erişmekte zorlanmaktadır. Bu durum, bilginin görünürde devletin müdahale alanında olmasına karşın, pratikte devlet denetiminin dışında dolaşıma girebildiği bir gerilim alanı yaratmaktadır.

Enformasyonun giderek transnasyonal bir nitelik kazanması, bu gerilimi daha da derinleştirmiştir. Tarihsel olarak devletler haber akışını kontrol etmeye çalışmış olsa da

---

[1081] Akdenizli, s.34.

[1082] Marie-Pierre Granger ve Kristina Irion, "The right to protection of personal data: The new posterchild of European Union citizenship?", Sybe de Vries, Henri de Waele ve Marie Pierre Granger (Ed.) **Civil Rights and EU Citizenship: Challenges at the Crossroads of the European, National and Private Spheres** içinde (279-302), Cheltenham: Edward Elgar Publishing. 2018, s.302.

[1083] Shapiro, s.viii.

bilgi dolaşımı hiçbir dönemde bütünüyle durdurulamamıştır. Günümüzde ise enformasyon, yalnızca haberle sınırlı olmayıp popüler kültür ürünlerinden görsel tasarıma kadar geniş bir alana yayılmış; bu da devletlerin sınırlama kapasitesini yapısal olarak zayıflatmıştır. Enformasyonun sınır aşan karakteri, kapalı rejimlerde dahi bilgi tekellerini aşındırmış; kültür ve iletişim alanında ulusal egemenliğin etkinliğini azaltmıştır[1084].

İnternete dayalı iletişim, devletlerin enformasyonu denetleme kapasitesini teknik ve hukuki açıdan yeni bir eşiğe taşımıştır. Sınır ötesi veri akışı, sansür girişimlerini çoğu zaman etkisiz ve meşruiyet bakımından tartışmalı kılmaktadır. Arama motorları ve sosyal medya platformları, algoritmik filtreleme yoluyla kullanıcıların neyi görüp neyi görmeyeceğini belirlemekte[1085] bilginin kaynağı bilinse dahi yaptırım uygulanmasını güçleştirmektedir. Tüm bir ülkeyi ağdan koparmadan erişimi tam anlamıyla engellemek çoğu durumda mümkün değildir. Mahkemelerin geniş kapsamlı internet kısıtlamalarını ifade özgürlüğüyle bağdaşmaz bulması da bu durumu pekiştirmektedir[1086]. Bu yapısal sınır, bilginin devlet sınırları içinde tutulmasına dayanan klasik egemenlik anlayışını fiilen çözmektedir.

Bilgi egemenliğinin aşınmasında bulut bilişim sistemleri de belirleyici bir rol oynamaktadır. Bulut ortamında veri üzerindeki denetim, kullanıcı ile hizmet sağlayıcı arasında paylaşılan bir ilişkiye dönüşmekte; veri egemenliğinin doğası köklü biçimde değişmektedir[1087]. Devletin; ulusal güvenlik, kamu düzeni, kurumsal süreklilik ve bireylerin mahremiyetinin korunması gibi gerekçelerle tekeline aldığı kamu kayıtları ve kritik devlet verileri[1088] giderek sınır ötesi veri merkezlerinde depolanmakta; devletlerin bu verilere anlık ve doğrudan erişimi zorlaşmaktadır. Bu durum, yerleşik egemenlik kavramının mekânsal varsayımlarını geçersiz kılmakta ve devletlerin yönetim kapasitesini zayıflatmaktadır. Örneğin, Amazon Web Services (AWS) veya Microsoft Azure gibi şirketler aracılığıyla, kritik ulusal veriler ABD veya başka bir ülkedeki veri

---

[1084] Drucker, s.203-204; Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.204-205.
[1085] Işık, s.35.
[1086] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.405-406.
[1087] U.S. Department of Commerce National Institute of Standards and Technology, s.2.
[1088] Irion, *"Government Cloud Computing and National Data Sovereignty",* s.52.

merkezlerinde depolanabilir. Avrupa Komisyonu'nun 2018 yılındaki raporunda, elektronik delillerin suç soruşturmalarının yaklaşık %85'i için gerekli olduğu ve bu soruşturmaların üçte ikisindeki delillerin başka ülkenin yargı yetkisi alanında bulunan online hizmet sağlayıcıda depolandığı belirtilmesini gelinen vaziyeti ortaya koymaktadır[1089]. Küresel teknoloji pazarındaki tekelleşme, bağımlılık ilişkilerini derinleştirerek şeffaflık ve hesap verebilirlik sorunlarını büyütmektedir. Artan jeopolitik rekabet ve ulusal güvenlik kaygıları, teknik standartların stratejik bir mücadele alanına dönüşmesine yol açmıştır. Teknik standartlar yalnızca teknolojik uyumluluğu değil; ekonomik (lisans/patent gelirleri), hukuki (uluslararası ticaretin altyapısı), siyasal (siber güvenlik avantajı) ve ideolojik (etik tercihler ve toplumsal değerler) boyutları da taşır. Bu nedenle standartların kim tarafından belirlendiği sorusu, dijital çağın güç mücadelesinde merkezi bir yere yerleşmiştir[1090].

Öte yandan, bilgi üzerindeki egemenliğin aşınması yalnızca devletin güç kaybıyla sınırlı olarak okunamaz. Boşalan alan, büyük ölçüde dijital platformlar tarafından doldurulmuştur. Sosyal medya ve veri temelli hizmetler, büyük veri analitiği yoluyla toplumsal eğilimleri çözümleyebilen ve davranışları yönlendirebilen bir altyapı kurmuştur. Öyle ki, bu verilerle bir toplumsal kriz çıkarmak istenirse, bunun için en uygun gün ve saat bile tespit edilebilir. Algoritmalar, hangi bilginin ne zaman, kime ve hangi bağlamda sunulacağını belirleyerek kamusal algıyı şekillendirebilmekte; bazı içerikleri görünür kılarken bazılarını sistematik biçimde bastırabilmektedir. Bu kapasite, toplumsal manipülasyon, siyasal süreçlere müdahale ve kolektif davranışların yönlendirilmesi gibi ciddi riskleri beraberinde getirmektedir[1091].

[1089] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN (14 Aralık 2024), s.14.

[1090] Tim Rühlig, "China: A Technical Standardisation Power?", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State,** içinde (103-122), Maryland: Rowman & Littlefield Publishers., 2023, s.108-109.

[1091] Cambridge Analytica'nın 2015'te birçok Facebook kullanıcısının verisini izinsiz toplaması ve bu bilgileri seçim kampanyalarında kullanması ile 2016 ABD Başkanlık Seçimlerine sosyal medya üzerinden yapılan müdahaleler, devletlerin karşılaştığı dijital sosyal mühendislik ve ulusal güvenlik tehditlerine örnektir.

Bu noktada dijital alanın yalnızca bilgiye değil, kolektif bilinç süreçlerine de etki ettiği görülmektedir. Bilinç, salt bilgi birikiminden ibaret olmayıp anlama, ilişkilendirme ve yaratıcı sentez üretme yetisini içerir[1092]. Dijital çağda bireysel ve toplumsal zihinsellik, veri ve algoritmalar aracılığıyla biçimlenmekte; kolektif bilinçdışı, teknik olarak işlenebilir bir alana dönüşmektedir. Büyük veri teknolojileri, insan davranışlarını çözümlemede güçlü araçlar sunarken, aynı zamanda bilinç süreçlerinin kapitalist sömürüye açılmasını mümkün kılar[1093].

Bu dönüşüm, yalnızca bireysel psikolojiyi değil; eğitim, üretkenlik, istihdam, toplumsal katılım ve siyasal yönelim gibi yapısal alanları da etkiler. Dijital okuryazarlığı bireysel bir beceri olmaktan çıkararak ulusal egemenlik ve toplumsal direnç meselesine dönüştürmektedir. Devletin rolü, yalnızca dijital altyapı kurmakla sınırlı değildir; aynı zamanda eleştirel düşünebilen, bilgiyi ayırt edebilen ve bilinçli yurttaşlar yetiştirecek bir kamusal kapasiteyi sürdürmeyi gerektirir[1094]. Aksi hâlde dijitalleşme, gerçek bilgiye erişimi kolaylaştırmak yerine, ilgisizlik, yüzeysellik ve bilgi düşmanlığı üreten bir zemine dönüşebilir.

Sonuç olarak dijitalleşme, bilgi üzerindeki egemenliği ortadan kaldırmamış; ancak bu egemenliğin geleneksel devlet merkezli biçimini derinden sarsmıştır. Enformasyonun transnasyonal dolaşımı ve platformların veri temelli iktidarı, devletin bilgi denetimini yapısal olarak sınırlamaktadır. Bu durum, bilginin serbestleşmesi ile yeni bir özel tahakküm biçiminin ortaya çıkması arasındaki gerilimi görünür kılmaktadır. Devletin kamusal iletişim alanından çekilmesi, her zaman özgürlüğün artması anlamına gelmemekte; çoğu zaman düzenlenmemiş özel güçlerin bir iktidar boşluğu doğurmasına ve bu boşluğu piyasa temelli bir tahakkümle doldurmasına yol açmaktadır. Dolayısıyla enformasyon kontrolü bakımından kritik soru şudur: Devletin geri çekilmesi gerçekten özgürlük mü üretir, yoksa yeni bir piyasa-egemen düzen mi kurar? Dijital çağın en çıplak gerilimi burada görünür hâle gelir: Devlet müdahalesinin azalması, otomatik olarak

[1092] Çalgan, s.205, 209-210.
[1093] Drucker, s.272.
[1094] Drucker, s.276-280.

özgürlüğün artması değildir; tersine, düzenlenmemiş özel güçlerin yeni bir egemenlik biçimi kurmasına zemin hazırlayabilir.

Devletler açısından, toplumsal sorunların çözümünde çoğu zaman karşıt çıkarlar arasında kalıcı bir uzlaşı değil, geçici ve pratik bir *modus vivendi* sağlanır; taraflar tüm farklılıkları ortadan kaldıramaz, yalnızca çatışmayı yönetilebilir düzeyde tutarak birlikte var olmanın yolunu bulur[1095]. Demokrasi ideal olarak savunulabilir olsa da özellikle aciliyet ve tehdit içeren durumlarda demokratik yöntemlerle hareket etmek her zaman mümkün değildir[1096]. Nitekim ABD'nin Huawei'ye yönelik yaptırımları gibi teknoloji şirketleri üzerinden kurduğu küresel etki, Çin'in katı veri yerelleştirme rejimi[1097] ve birçok ülkenin veri akışını sınırlayan tedbirlerinin yanı sıra UNCTAD'ın gelişmekte olan ülkelere sınır ötesi veri akışlarını sınırlama önerisi[1098] bu mücadelenin örnekleri olup devletlerin veri üzerinde egemenliğini koruma yönündeki eğilimlerini ortaya koymaktadır[1099]. Bu süreç veri egemenliğini, ulusal egemenliğin çağdaş ve tamamlayıcı bir boyutu hâline getirmiştir[1100]. Devletin veri akışını sansürleyerek veya sınırlandırarak kontrol etmesi, bu geleneksel koruma reflekslerinin dijital çağda da sürdüğünü gösterir.

c. Dijital Çağda Egemenliğin Koruyucu Niteliğinin Aşınması: Siber Tehditler, Hibrit Savaş ve Veri Güvenliği

Dijitalleşme, ulusal sınır tanımayan siber suç ve siber saldırı biçimlerinin hızla yaygınlaştığı; bireylerin temel haklarını ve devletlerin egemenlik yetkilerini doğrudan

---

[1095] Walter Lippmann, **Hayalet Kamu,** Cem Evrim Aslan (çev.), İstanbul: Kabalcı Yayınevi, 2024, s.63.

[1096] Tehlikenin varlığında, hızlı ve uyumlu eylemin gerekli olduğu durumlarda, demokrasinin yöntemleri kullanılamaz. Lippmann, s.116-117.

[1097] Veri egemenliğinin öncülerinden olan Çin, dijital içeriği ve veriyi kontrol etme hakkının devlete ait olduğunu savunmakta ve katı veri yerelleştirme kuralları benimsemektedir. Bu doğrultuda veri transferini neredeyse engelleyen 2017 Siber Güvenlik Yasası gibi verilerin ülke içinde saklanmasını ve yurt dışına aktarılmadan önce devlet onayı alınmasını zorunlu kılan yasal düzenlemeler getirmiştir. Dorwart, s.123-124.

[1098] UNCTAD, Digital Economy Report 2019, 'Value Creation and Capture: Implications for Developing Countries', 2019, s.89.

[1099] World Economic Forum, Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows, 2021, https://www.weforum.org/publications/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows/ (14 Aralık 2024). Uygulamalı açıdan bakıldığında, Çin, dijital egemenlik politikası çerçevesinde Alibaba Cloud'un kullanım alanları ulusal güvenlik gerekçesiyle sınırlandırmıştır. ABD ve Çin merkezli bulut hizmetlerine alternatif olması ve dijital egemenlik açısından AB, Gaia-X Projesi'ni geliştirmektedir: bkz. https://www.data-infrastructure.eu.).

[1100] Irion, *"Government Cloud Computing and National Data Sovereignty",* s.42.

etkileyen yeni bir güvenlik ortamı yaratmıştır. Bu ortamda hem geleneksel suç tipleri dijital araçlarla işlenebilir hâle gelmiş hem de dijital teknolojilere özgü yeni suç ve tehdit biçimleri ortaya çıkmıştır. Sosyal mühendislik, oltalama, zararlı yazılımlar ve dijital şantaj gibi yöntemler, suçun icra biçimini dönüştürmüş[1101] özellikle sosyal medya platformları; dijital şiddet ve siber taciz pratiklerinin yoğunlaştığı alanlara dönüşmüştür[1102]. Israrlı takibin dijitalleşmesiyle birlikte bireylerin konum, iletişim ve kişisel verileri teknolojik araçlarla izlenebilir hâle gelmiş[1103] bu durum egemenliğin bireyi koruma kapasitesini yeni bir sınamayla karşı karşıya bırakmıştır.

Dijital dönüşümün kriminal boyutu, finansal sistemler ve yeni ödeme araçları üzerinden daha da derinleşmektedir. Kripto varlıkların sağladığı görece anonimlik ve iz sürmeyi zorlaştıran teknik özellikler, dolandırıcılık, kara para aklama ve terörün finansmanı gibi suçlar bakımından elverişli bir zemin yaratmaktadır[1104]. Blokzincir teknolojisinde işlem kayıtlarının izlenebilir yapısına rağmen, suç failleri farklı protokoller ve teknik ara katmanlar kullanarak izlerini gizleyebilmekte; bu durum soruşturma ve yaptırım süreçlerini hem teknik hem de hukuki açıdan karmaşıklaştırmaktadır[1105].

Bu gelişmeler, savaş ve güvenlik anlayışındaki dönüşümle birleşerek egemenliğin koruyucu niteliğini doğrudan etkilemektedir. Konvansiyonel savaşların yerini giderek hibrit ve asimetrik tehditler almakta; devlet destekli siber saldırılar, terör örgütleri, organize suç ağları ve bireysel hacker grupları enerji, finans, sağlık ve iletişim gibi kritik altyapıları hedef almaktadır. Siber saldırıların devlet politikalarının bir aracı

[1101] Türkiye'de bilişim suçları ilk kez 1991'de düzenlenmiş, 2022'de ısrarlı takip Türk Ceza Kanunu'na eklenmiştir (m.123/4-3). Bu düzenleme, özellikle kadınlar ve aile içi şiddet mağdurlarının güvenliğini korumayı hedeflemektedir. Aynı yıl, halkı yanıltıcı bilgi yayma suçu (m.217/A) da ceza hukukuna girmiştir; kamu düzeni ve sağlık gibi alanlarda panik yaratmayı amaçlayan yalan bilgi yayanlar cezalandırılmaktadır.

[1102] Tuğçe Özen, "Dijital Çağın Yarattığı Yeni Bir Fenomen: Dijital Şiddetin Türü Olarak Israrlı Takip", **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.111, 113.

[1103] Özen, s.109.

[1104] Bu eylemler, Türk Ceza Kanunu m. 158/1-f'de düzenlenen nitelikli dolandırıcılık suçu kapsamına girer. Ayrıca TCK m. 244/4'e göre bilişim yoluyla haksız kazanç sağlama suçu da oluşabilir. Ancak, fiil dolandırıcılık suçunu oluşturuyorsa esas olarak TCK m. 158/1-f uygulanmalıdır. Uğur Aşkın, "Bilişim Sistemleri Aracılığıyla İşlenen Kripto Para Dolandırıcılığı", **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.77-78.

[1105] Örneğin, Ethereum blokzincirinde çalışan "Tornado Cash" adlı kripto karıştırıcı, 2022'de ABD Hazine Bakanlığı tarafından yaptırıma uğramış; iki gün sonra Hollanda'da geliştiricisi Alexey Pertsev, suçtan kaynaklanan malvarlığı aklama şüphesiyle tutuklanmıştır. Polat, s. 52.

hâline gelmesi, savaş ile barış arasındaki sınırları belirsizleştirmiş; doğrudan askerî müdahale yerine düşük maliyetli ancak yüksek etkili operasyonlar, bazı aktörler açısından tercih edilen bir stratejiye dönüşmüştür. Özellikle tedarik zincirlerine yönelik saldırılar, dijital tehditlerin yalnızca tekil sistemleri değil, bütüncül toplumsal ve ekonomik düzeni hedef aldığını göstermektedir[1106].

Bu noktada modern egemenliğin kurucu işlevi yeniden gündeme gelir. Siyasal iktidarın temel meşruiyet kaynağı, egemenliği altındaki bireyleri koruma kapasitesidir. Hobbesçu gelenekte devletin varlık nedeni, güvenlik sağlama yükümlülüğüyle doğrudan ilişkilidir. Bu yükümlülük, yalnızca haklara saygı gösterme değil; üçüncü kişilerden gelebilecek tehditlere karşı koruma sağlama ve hakların fiilen kullanılabilmesini temin etme sorumluluğunu da içerir. Dijitalleşmeyle birlikte ortaya çıkan siber saldırılar, veri güvenliği açıkları ve hibrit savaş yöntemleri, devletin bu koruma ödevini dijital alanda da yerine getirmesini zorunlu kılmaktadır. Dolayısıyla dijital alana müdahale, egemenlik bakımından isteğe bağlı bir tercih değil; ulusal güvenlik ve kamu düzeni açısından yapısal bir zorunluluktur.

Siber saldırılar; insan onurunu ve temel hakları tehdit eden dijital risklerin merkezinde yer almaktadır[1107]. Bilişim sistemlerinin ve bu sistemlerde işlenen verilerin gizliliğini, bütünlüğünü veya erişilebilirliğini hedef alan bu saldırılar, yalnızca askerî sistemleri değil; hastaneler, enerji hatları, su altyapıları ve iletişim ağları gibi sivil ve kritik kamu altyapılarını da savunmasız bırakmaktadır[1108]. Siber suçlar ve casusluk faaliyetleri ekonomik istikrarı tehdit ederken, kişisel verilere izinsiz erişim bireylerin

---

[1106] Türkiye Büyük Millet Meclisi, Siber Güvenlik Kanunu Gerekçesi, Genel Gerekçe, s. 13, https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf?TSPD_101_R0=08ffcef486ab200056d52ad6f4103bc36409bacef68647464825ac8890b8c3bee400cfcfcf3cb37908ff8bf8ca143000f29b9816db340591384478f34e790f5076326c1ba3655e89c917854199f4e1779408741a3b9055db77539d39c3a13816 (E.T.: 1 Şubat 2026).

[1107] Siber saldırı, siber uzaydaki bilişim sistemlerinin ve bu sistemlerce işlenen verinin gizliliğini, bütünlüğünü veya erişilebilirliğini ortadan kaldırmaya yönelik kasıtlı eylemleri ifade eder. Siber Güvenlik Kanunu Gerekçesi, m. 3/1(ğ)., https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf?TSPD_101_R0=08ffcef486ab200056d52ad6f4103bc36409bacef68647464825ac8890b8c3bee400cfcfcf3cb37908ff8bf8ca143000f29b9816db340591384478f34e790f5076326c1ba3655e89c917854199f4e1779408741a3b9055db77539d39c3a13816 (E.T.: 1 Şubat 2026).

[1108] Aydınlı, s. 3.

itibarına ve mahremiyetine ciddi zararlar vermektedir[1109]. Bu nedenle siber güvenlik, teknik bir bilişim meselesi olmaktan çıkarak doğrudan ulusal güvenlik sorunu hâline gelmiştir[1110]. Bilişim sistemlerinin kesintisiz işleyişi, verilerin gizliliği ve bütünlüğü ile yetkisiz erişimin engellenmesi stratejik öncelik kazanmıştır[1111].

Dijital çağda ortaya çıkan tehditler, klasik siber suç kavramının ötesine geçmektedir. Siber terör, algoritmik manipülasyon ve hibrit savaş stratejileri, devletin vatandaşını koruma sorumluluğunu hedef alan çok boyutlu riskler üretmektedir. Dijital alan artık yalnızca bir iletişim mecrası değil; modern savaşın tamamlayıcı ve kimi zaman belirleyici bir bileşenidir. Geleneksel kışlalı orduların yanında; otonom silah sistemleri[1112] yapay zekâ destekli karar mekanizmaları ve uzaktan kontrol edilen araçlar saldırıların etkisini öngörülemez hâle getirmekte; dijital müdahaleler sivilleri de etkileyen fizikî yıkım ve can kaybı gibi sonuçlar doğurabilmektedir[1113]. Egemenliğin koruyucu niteliğini yeniden tanımlamayı zorunlu kılan yapısal bir meydan okumaya işaret eden bu tür saldırılar, sivillerin doğrudan etkilenmesi ve çatışmanın niteliği nedeniyle uluslararası

[1109] Kaliforniya'da yaşlı bir adam, yapay zekâ ile oğlunun sesinin taklit edilmesi sonucu manipüle edilmiş; oğlunun korkunç bir kazaya karıştığını ve hapisten kefaletle çıkmak için paraya ihtiyacı olduğunu düşünerek dolandırıcılara 25.000 dolar kaptırmıştır. Telefonda duyduğu sesin, oğlunun sesiyle tamamen aynı olduğunu iddia eden adam, panikle harekete geçerek dolandırıcıların taleplerini yerine getirmiştir. New York Post, "Scammers swindle elderly California man out of $25K by using AI voice technology to claim his son was in horrible accident, needed money for bail," 18 Ekim 2024, https://nypost.com/2024/10/18/us-news/scammers-swindle-elderly-california-man-out-of-25k-by-using-ai-voice-technology-to-claim-his-son-was-in-horrible-accident-needed-money-for-bail-absolutely-his-voice/ (E.T.: 1 Şubat 2026).

[1110] Avrupa Birliği, Amerika Birleşik Devletleri, Rusya ve Çin gibi başlıca küresel aktörler, bilgisayar virüsleri, veri ihlalleri ve kimlik hırsızlığı gibi siber tehditleri ulusal güvenlik riski olarak değerlendirmekte; kamu ve özel sektör düzeyinde bu tehditlere karşı yüksek bütçeli siber güvenlik önlemleri geliştirmektedir. Bkz. Avrupa Birliği Başkanlığı, Ocak 2022 Bülteni, https://www.ab.gov.tr/siteimages/birimler/mib/programlama/bulten/pdf/ocak_2022.pdf; The White House, 2024 Report on the Cybersecurity Posture of the United States, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf; Federal Budget IQ, DoD's FY24 Cyber Budget, https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/ (E.T.: 1 Şubat 2026).

[1111] Aydınlı, s.3.

[1112] Küzeci, s.303.

[1113] İsrail'in 1972 ve 1996 yıllarında FKÖ'nün Paris Temsilciliğine yönelik ev telefonu bombalı suikastleri ile 2010'da İran'ın enerji altyapısına, 2016'da Ukrayna'nın elektrik şebekesine ve 2024'te Lübnan'da Hizbullah'a ait çağrı cihazlarına yönelik siber saldırılar; ciddi can kayıplarına, fizikî yıkıma ve temel hizmetlerde geniş çaplı kesintilere yol açmıştır. Özellikle 17 Eylül 2024'te Lübnan'da Hizbullah'ın binlerce çağrı cihazının eş zamanlı patlatılması, siber saldırıların yalnızca dijital sistemleri değil, doğrudan insanın fizikî varlığını da hedef alabileceğini açıkça göstermiştir. Bu tür saldırılar, bireyin dijital kırılganlıklarının fizikî teröre dönüşebildiğini; siber terör, dijital savaş ve hibrit tehdit gibi yeni savaş biçimlerinin ortaya çıktığını ortaya koymaktadır. Böylece dijital alan, algoritmalar üzerinden işleyen ve geleneksel silah sistemleriyle birlikte çalışan yeni bir savaş cephesine dönüşmüştür. Geçmişte devletler güvenliği sağlamak için sürekli hazır kışlalı ordulara ihtiyaç duyarken, günümüzde sınırlı ölçekli dijital müdahalelerle dahi başka bir devletin stratejik altyapısı ve insan gücü hedef alınabilmektedir.

nitelikte silahlı çatışma bağlamında ele alınmalı; hukuka uygunluk da uluslararası insancıl hukukun askeri gereklilik, ayrım gözetme, orantılılık ve gereksiz acı yasağı ilkeleri ışığında değerlendirilmelidir[1114].

Egemenliğin koruma fonksiyonunun aşınması, veri güvenliği alanında daha da görünür hâle gelmektedir. Büyük ölçekli veri tabanlarında toplanan kişisel veriler üzerinde devletin yeterli denetim kuramaması, ciddi güvenlik riskleri yaratmaktadır. Sosyal medya platformlarının veri toplama ve işleme kapasitesi, veri ifşalarına ve bireylerin çevrimiçi ve çevrimdışı şiddet risklerine maruz kalmasına yol açabilmektedir. Gazeteciler, aktivistler ve insan hakları savunucuları gibi grupların platformlar aracılığıyla fişlenebilmesi, ifade özgürlüğü ve mahremiyet hakkı bakımından yapısal tehditler doğurmaktadır[1115]. Üstelik verilerin çoğu zaman ulusal sınırlar dışında depolanması, devletlerin acil durumlarda etkili müdahale kapasitesini sınırlamakta; bir ulusal güvenlik meselesi olan veri egemenliğini zayıflatmaktadır[1116].

Bu noktada egemenlik ile itaat arasındaki klasik bağ yeniden belirginleşir. Bireylerin egemene itaat yükümlülüğü, egemenin onları koruyabildiği ölçüde meşruiyet kazanır. Devlet siber saldırılara karşı yurttaşlarını koruyamaz, veri güvenliğini sağlayamaz ve kritik altyapıların sürekliliğini teminat altına alamazsa, egemenliğin koruyucu temeli aşınır. Bu aşınma, yalnızca güvenlik açığı değil; egemenliğin ahlaki ve siyasal meşruiyetinin zayıflaması anlamına gelir[1117]. Dolayısıyla siber güvenlik ve veri güvenliği, teknik bir politika alanı değil, egemenliğin sürdürülmesi bakımından varlık-yokluk düzeyinde bir mesele hâline gelmektedir[1118]. Nitekim, Almanya eski Şansölyesi Angela Merkel, birçok Avrupa şirketinin veri paylaşımı konusunda ABD'li teknoloji şirketlerine bağımlı hale geldiğini vurgulayarak bu durumun dijital egemenlik açısından ciddi bir kısırdöngü yarattığını belirtmiştir[1119]. Benzer şekilde, Trump yönetimi Clean

---

[1114] Hacer Gizem Karataş, "Mossad'ın Çağrı Cihazı Operasyonunun Silahlı Çatışma Hukukunun Temel İlkeleri Bakımından Değerlendirilmesi", **GSÜHFD,** Cilt.2025, No.2, (2025), s.1426-1428.
[1115] All Tech Is Human, s.34.
[1116] Demir ve Özbuğday, s.15.
[1117] Göze, s. 163.
[1118] Christakis, s.42.
[1119] Bu zorunluluk doğrultusunda, günümüzde devletler siber güvenlik politikaları geliştirmekte ve siber güvenliği ulusal güvenlik stratejilerinin merkezine yerleştirmektedir. Guy Chazan, "Angela Merkel urges EU to seize control of

Network Programı ile, vatandaşların gizliliği ve şirketlerin hassas verilerini Çin gibi aktörlerin tehditlerine karşı korumayı hedeflemiştir[1120].

Bu nedenle çözüm, egemenliğin dijital çağdaki koruyucu niteliğinin yeniden inşa edilmesini gerektirir. Bilgi ve iletişim teknolojilerinin yarattığı yeni risklere karşı, bireylerin dijital haklarının güçlendirilmesi ve devletin bu hakları etkin biçimde koruyabilmesi zorunludur[1121]. Teknoloji şirketlerinin temel hak ve özgürlükleri ihlal ettiği durumlarda, devletin hızlı ve etkili biçimde müdahale edebilmesi, toplumsal huzur ve kamu düzeni açısından kaçınılmazdır[1122].

Bu müdahalenin stratejik boyutu, dijital alanda teknolojik bağımsızlığın güçlendirilmesidir. Siber güvenliğin sağlanması, devletin dijital altyapı üzerindeki kontrolünü yitirmemesini ve dışa bağımlılığın egemenliği aşındıracak düzeye ulaşmamasını gerektirir. Küresel teknoloji pazarında kritik altyapıların sınırlı sayıda tedarikçinin kontrolünde olması, devletleri karar alma ve uygulama kapasitesi bakımından kırılgan hâle getirmektedir. Deniz altı kabloları, 5G ve bulut altyapıları, yapay zekâ sistemleri ve yarı iletken teknolojiler gibi stratejik bileşenlerde ortaya çıkan bağımlılık ilişkileri, dijital çağda egemenliğin korunmasını doğrudan etkileyen yapısal riskler üretmektedir[1123].

---

data from US tech titans," Financial Times, 12 Kasım 2019, https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca, (E.T.: 1 Şubat 2026).

[1120] Güvenilirlik niteliğini temel alan bu program operatör, uygulama mağazası, uygulamalar, bulut, iletişim kabloları, veri iletim yolu olmak üzere 6 temel politikadan (clean carrier, clean store, clean apps, clean cloud ve clean path) oluşmaktadır. US Department of State, The Clean Network, 2020, https://2017-2021.state.gov/the-clean-network/ (15 Aralık 2024).

[1121] Uygun, s. 607.

[1122] Hobbes'un Leviathan'ı, herkesin herkese karşı olduğu savaşta güvenliği sağlamak için vardır; günümüzde değişen, bu savaş alanının ulusal sınırlar içinden küresel dijital/siber alana taşınmış olmasıdır. Bu nedenle devletin koruma görevi, vatandaşların verileri üzerinde denetim, dijital güvenliğin sağlanması, teknolojik rekabet gücü ve dijital alanda kural koyma ve uygulama yeteneğini gerektirir; başka bir deyişle dijital egemenliğin tesisini zorunlu kılar. Öğretide de verilerin büyük ölçüde ulusal sınırlar dışında yönetildiği ve devlet denetiminin zayıfladığı bir ortamda dijital egemenliğin öneminin arttığı vurgulanmaktadır. (All Tech Is Human, s.4; European Parliamentary Research Service, *Digital Sovereignty for Europe,* s.1.

[1123] 2023'te sadece Amerikalı Apple firmasının değeri 3,1 trilyon dolara ulaşmış; bu rakam, Fransa'daki tüm şirketlerin toplam değerine neredeyse eşittir. Subrat Patnaik ve Michael Msika, "iPhone maker Apple's market value approaches that of French stock market," Business Standard, 14 Aralık 2023, https://www.business-standard.com/world-news/iphone-maker-apple-s-market-value-approaches-that-of-french-stock-market-123121400586_1.html (E.T.: 1 Şubat 2026). Yapay zekâ ilişkili patent başvurularının %45'i ABD'de, %40'ı Çin'de yapılmaktadır ve küresel yapay

Dijital bağımlılığın ekonomik sonuçlarının ötesinde sosyal ve siyasal etkileri de vardır: Teknolojik bileşenlere erişimin kesilmesi, dijital manda benzeri bir bağımlılık rejimine dönüşebilecek ölçüde egemenliği tehdit edebilir. Bu nedenle özellikle üretim kapasitesi sınırlı ülkelerde yerli girişimlerin desteklenmesi, dijital bağımsızlık stratejisinin bir aracı olarak öne çıkmaktadır. Ancak bu tür uygulamalar Airbus örneğinde olduğu gibi, tekel karşıtı serbest piyasa rekabet politikasını ikircikli bir duruma sokmaktadır[1124].

Sonuç olarak dijital çağ, egemenliğin koruyucu niteliğini ortadan kaldırmamış; ancak bu niteliğin geleneksel araçlarla sürdürülemeyeceğini açıkça ortaya koymuştur. Siber tehditler, hibrit savaş yöntemleri ve veri güvenliği sorunları, egemenliğin dijital düzlemde yeniden tanımlanmasını zorunlu kılmaktadır. Bu yeniden tanımlama, güvenlik ile özgürlük arasındaki dengeyi gözeten; demokratik meşruiyet, hukuki denetim ve teknolojik kapasiteyi birlikte ele alan bütüncül bir egemenlik anlayışını gerektirir.

d. Sermayesiz Kapitalizmi Vergilendirme Sorunu

Egemenliğin klasik kuramsal çerçevesinde vergi, yalnızca mali bir teknik değil; devletin siyasal varlığını sürdürebilmesinin kurucu araçlarından biridir. Vergilendirme yetkisi, egemenliğin maddi zemininin somutlaştığı başlıca alanlardan biri olarak, siyasal iktidarın sürekliliğini ve kurumsal kapasitesini doğrudan belirler. Bu bağlamda erken modern egemenlik teorilerinde mali alan, mutlak iktidar iddiasına rağmen belirli sınırlara tabi kılınmıştır. Bodin'in egemenlik kuramında vurgulanan ahde vefa ve mülke saygı ilkeleri, egemenliğin mutlaklığı ile özel mülkiyet düzeni arasında kurulan hassas dengeyi yansıtır. Egemen, vergilendirme yetkisine sahip olsa da bu yetkinin meşruiyeti, mülkiyet hakkını bütünüyle ihlal etmeyecek bir çerçevede düşünülmüştür[1125]. Böylece mali

---

zekâ piyasasının %25'i sadece dört tane ABD firmasının elindedir. Tipper ve Krishnamurthy, s.2. ABD küresel dijital platformların %73'üne Çin %18'ine sahiptir. The Economist, "The EU wants to set the rules for the world of technology," 20 Şubat 2020, https://www.economist.com/business/2020/02/20/the-eu-wants-to-set-the-rules-for-the-world-of-technology (E.T.: 1 Şubat 2026).

[1124] Yerel girişimleri desteklemek amacı doğrultusunda, AB Komisyonu, New Competition Tool ve Digital Services Act'ın bir bölümünü Digital Market Act altında tek bir dokümanda birleştirmiştir. Christakis, s.90.

[1125] Şenel, s.316-317.

egemenlik, özel mülkiyetle çatışmadan kurulan bir siyasal düzenin parçası hâline gelmiştir.

Bu tarihsel arka plan, modern devletin inşasında vergilendirmenin neden merkezi bir rol oynadığını da açıklar. Düzenli ve öngörülebilir vergi gelirleri, modern devleti feodal ve patrimonyal yapılardan ayıran temel unsurlardan biridir. Özellikle savaşların finansmanı, vergi aygıtının kurumsallaşmasında belirleyici olmuş; artan askerî harcamalar, kaynakların sistematik biçimde toplanmasını zorunlu kılmıştır. Süreklileşen gelir ihtiyacı, genişleyen bir devlet aygıtını; genişleyen aygıt ise daha yüksek mali kapasiteyi gerektirmiştir[1126]. Bu döngü içinde vergi, yalnızca gelir elde etme aracı değil; ekonomik davranışları yönlendiren, teşvik eden veya caydıran bir yönetim tekniği olarak da işlev görmüştür.

Ne var ki dijitalleşmeyle birlikte ortaya çıkan yapısal dönüşüm, bu klasik mali-egemenlik mimarisini derinden sarsmaktadır. Maddi olmayan yatırımların (bilgi üretimi, yazılım geliştirme, organizasyonel kapasite ve veri temelli değer yaratımının) maddi yatırımların önüne geçmesi, fizikî sermayeye sahip olmadan yüksek gelir elde edebilen aktörlerin yaygınlaşmasına yol açmıştır. Bu yeni ekonomik yapı, "sermayesiz kapitalizm" olarak adlandırılmakta; değerin üretim araçlarının mülkiyetinden ziyade dijital aracılık, veri işleme ve algoritmik görünürlük üzerinden yaratıldığı bir düzeni ifade etmektedir[1127]. Sosyal medya, çevrim içi reklam ve platform ekonomileri, bu dönüşümün en belirgin taşıyıcılarıdır.

Sermayesiz kapitalizmin tipik örnekleri, fizikî varlığa sahip olmaksızın küresel ölçekte ekonomik değer üreten platformlarda somutlaşmaktadır. Örneğin Uber'in taksisiz taksi şirketi, Facebook'un içeriksiz medya şirketi, Aliexpress'in stoksuz perakendecilik,

---

[1126] Pierson, s. 49. Savaşların finansmanı, modern vergilendirme sisteminin ve merkezî devlet aygıtının oluşumunda belirleyici olmuştur. Düzenli vergiler ve zorunlu askerlik, bürokratik ve askerî yapıyı büyütmüş; bu büyüme ise devletin daha fazla mali kaynak üretme ihtiyacını doğurmuştur. Böylece egemenlik ile mali kapasite arasında karşılıklı beslenen bir döngü oluşmuş; daha fazla kaynak daha büyük bir devlet aygıtını, daha büyük bir devlet aygıtı ise daha fazla kaynak toplama zorunluluğunu beraberinde getirmiştir. Küzeci, s.299.

[1127] Jonathan Haskel ve Stian Westlake, **Capitalism Without Capital: The Rise of the Intangible Economy,** Princeton: Princeton University Press, 2017, s.4-5.

Airbnb'nin gayrimenkulsüz konaklama kapasitesi[1128] gibi. Dijital platformlar, üretim ve dağıtım zincirlerini aracısızlaştırarak değeri mal üretiminden ziyade erişimi düzenleme, kullanıcı etkileşimini yönetme ve veriyi işleme kapasitesi üzerinden üretmektedir. Bu modelde belirleyici olan unsur, üretim araçlarının klasik anlamda mülkiyeti değil; dijital altyapının, algoritmik sıralamanın ve platform mimarisinin kontrolüdür. Böylece ekonomik güç, maddi sermayeden çok dijital konumlanma üzerinden yoğunlaşmaktadır.

Bu dönüşüm, vergilendirmenin klasik mekânsal varsayımlarını geçersiz kılmaktadır. Vergi hukukunun temel ilkeleri, çoğu zaman vergiyi doğuran olayın belirli bir ülke sınırı içinde gerçekleşmesine ve faaliyetin o ülke ile fizikî bir bağ kurmasına dayanır. Oysa dijital hizmetlerde ekonomik faaliyetin icrası, sınırları aşan teknik işlemler zinciri içinde gerçekleşmekte; hizmet ifası mekândan koparak sanal ortamda vuku bulmaktadır. Sermayesiz kapitalizmin temel sorunu da burada ortaya çıkar: Küresel platformlar, faaliyetlerinin ekonomik etkisini yoğun biçimde belirli ülkelerde doğururken, bu ülkelerde vergilendirme dışı kalabilmektedir. Bu durum, ulus-devletlerin mali egemenliğini zayıflatmakta ve kamusal gelirlerin sürdürülebilirliğini kırılgan hâle getirmektedir.

Dijital ekonomide yaratılan değerin coğrafi sınırlarının belirsizliği, vergilendirme yetkisinin hangi devlete ait olduğunun tespitini güçleştirmektedir. Geleneksel işyeri, daimî temsilcilik ve mukimlik kavramları, dijital hizmetlerin sınır aşan niteliği karşısında işlevsizleşmektedir. Bu nedenle dijital reklamcılık ve veri temelli hizmetlerden elde edilen gelirler, çoğu zaman ulusal vergi sistemlerinin dışında kalmakta[1129] devletler, ekonomik faaliyetin sonuçlarına katlanırken mali karşılığını tahsil edememektedir.

[1128] Tom Goodwin, **Digital Darwinism: Surviving the new age of business disruption,** 2nd edition, London: Kogan Page Inspire, 2022, s.9. Shapiro'ya göre Amazon ve Virtual Vineyards gibi dijital platformlar, doğrudan üretim yapmasalar da internet aracılığıyla üretici ile tüketiciyi küresel ölçekte buluşturan aracı yapılardır. Bu platformlar, çevrim içi yatırımlar sayesinde bireylere zaman, mekân ve maliyet avantajı sunarken, etkileşim gibi dijital özellikler yoluyla tüketiciye daha fazla seçenek ve deneyim sağlamaktadır. Böylece dijital ekonomi, üretimden çok erişim, aracılık ve etkileşim üzerinden yeni fırsatlar yaratmaktadır. Shapiro, s.56.

[1129] Emine Sevcan Artun, "İnternet Ortamında Reklam Verenlerin Vergi Kesintisi Yapma Yükümlülükleri", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (513-530), İstanbul: Adalet, 2021, s.513.

Bu bağlamda klasik uluslararası vergi araçları da dijital ekonomide paradoksal sonuçlar üretmektedir. Çifte vergilendirmeyi önleme anlaşmaları, geleneksel ekonomide vergi adaletini sağlamayı amaçlarken, dijital ekonomide kimi zaman vergiden kaçınma için elverişli bir zemin oluşturmaktadır. Küresel ölçekte faaliyet gösteren platformların, belirli ülkelerde yüksek gelir elde etmelerine rağmen fizikî işyeri veya daimî temsil kriterlerini karşılamadıkları gerekçesiyle gelir vergisi yükümlülüğünden kaçınabilmesi[1130] vergilendirme yetkisinin mekânsal egemenliği (mülkîliğini) fiilen zayıflatmaktadır[1131]. Bu durum, mali güce göre vergilendirme ilkesini tersyüz ederek vergi adaleti bakımından ciddi eşitsizlikler yaratmaktadır.

Vergi adaleti açısından ortaya çıkan sorun, yalnızca mali değil, aynı zamanda siyasal bir nitelik taşır. Benzer ekonomik faaliyetlerden benzer vergi yükünün doğması gerekirken, yerli aktörler vergisel yükümlülük altındayken küresel platformların fiilen vergiden muaf kalması hem yatay hem de dikey eşitliği zedelemektedir. Bu eşitsizlik, rekabet koşullarını bozmakta ve kamusal meşruiyeti aşındırmaktadır[1132]. Dolayısıyla dijital ekonominin vergilendirilmesi, yalnızca gelir toplama meselesi değil; egemenliğin mali ayağının korunması, vergi adaletinin sağlanması ve piyasa düzeninin eşit koşullarda işletilmesi sorunudur.

Bu nedenle dijital ekonomide vergilendirme tartışması, doğrudan egemenliğin sınırlarıyla ilişkilidir. Tek taraflı vergisel düzenlemeler, uluslararası uzlaşı eksikliği nedeniyle ticari gerilim ve misilleme riskini artırabilmektedir[1133]. Dijital reklam gelirlerinin vergilendirilmesi, uluslararası bir altyapı kurulmasını gerektirdiğinden yalnızca iç hukuk düzenlemeleriyle yapılacak vergilendirme, uluslararası anlaşmalara

---

[1130] Özellikle reklam pazarında büyük oranda hâkimiyet kurmuş olan Google ve Facebook gibi şirketler, Türkiye'de önemli gelirler elde etmelerine rağmen -dijital hizmet vergisi dışında- vergi yükümlülüğünden muaf tutulmaktadır. Fatih Kaplanhan, "Türkiye'de Sosyal Medyanın Vergilendiril(eme)mesi ve Çözüm Önerileri: Google, Facebook, Twitter Örneği", **Turkish Journal of Police Studies/Polis Bilimleri Dergisi,** Vol.18, Sayı.3, 2016, s.51-54.

[1131] Kaplanhan, *"Dijitalleşme, Vergi ve Egemenlik Sorunu",* s.181-187.

[1132] Kaplanhan, *"Dijitalleşme, Vergi ve Egemenlik Sorunu",* s.189.

[1133] Fransa'nın 2019'da yürürlüğe koyduğu %3 Dijital Hizmet Vergisi, uluslararası uzlaşı eksikliğini görünür kılmış; özellikle ABD merkezli şirketlerin yoğunluğu nedeniyle, ABD ile ticari gerilim doğurmuştur. Bu örnek, tek taraflı vergisel hamlelerin misilleme riskini büyüttüğünü; karşılıklı yaptırımların, ticaret savaşlarının ve vergisel kaosun ihtimal dâhilinde olduğunu göstermektedir. Christakis, s.30-31.

aykırılık ve devletlerarası sorumluluk riski doğurmaktadır[1134]. Dijital hizmet vergileri etrafında yaşanan uluslararası tartışmalar, mali egemenliğin artık yalnızca iç hukuk meselesi olmadığını; küresel güç ilişkilerinin bir parçası hâline geldiğini göstermektedir. Vergilendirme alanındaki bu kırılganlık, sermayesiz kapitalizmin devletlerin mali kapasitesi üzerindeki aşındırıcı etkisini görünür kılmaktadır.

e. Ademimerkeziyetçi Dijital Paralar ve Parasal Egemenliğin Daralması

Paranın tarihsel gelişimi çoğu zaman somuttan soyuta doğru ilerleyen doğrusal bir evrim olarak anlatılsa[1135] da tarihsel deneyim paranın özünün formundan ziyade işlevinde yattığını göstermektedir. Dijital çağdan çok önce de para, fizikî varlıktan bağımsız, kayıt, borç ve hesap ilişkileri üzerinden işleyen sanal bir düzenleme tekniği olarak var olmuştur. Antik toplumlarda muhasebe sistemleri, yalnızca maddi malların miktarını değil, geleceğe dönük borç ilişkilerini de kayda geçirerek paranın temel mantığını oluşturmuştur. Bu nedenle bugün dijital teknolojilerin mümkün kıldığı sanal ödemeler ve dijital değer transferleri, paranın tarihsel doğasıyla radikal bir kopuş değil; onun kayıt, ölçüm ve borç yönetimine dayalı mantığının yeni bir teknik düzlemde sürdürülmesidir[1136].

Bu süreklilik, paranın işlevsel temelinde güvenin yer aldığını ortaya koyar. Nitekim kredi sözcüğünün kökeni Latincede inanmak anlamına gelen *credere*'ye dayanır. Para, değerini maddi karşılığından değil, onun toplumsal olarak kabul edileceğine dair kolektif inançtan alır. Tarihsel olarak bu güven, bireyler arası ilişkilere değil; daha güçlü ve süreklilik arz eden bir otoriteye, yani egemene dayanmıştır[1137]. Borç senetlerinin ve itibari paranın toplumsal dolaşıma girebilmesi, bu senetlerin arkasında onları garanti eden siyasal bir gücün bulunduğu inancıyla mümkün olmuştur. Böylece para, yalnızca

---

[1134] Artun, *"İnternet Ortamında Reklam Verenlerin Vergi Kesintisi Yapma Yükümlülükleri",* s.526.

[1135] Paranın insanlık tarihinde somuttan soyuta doğru ilerleyen çizgisel bir evrim izlediği fikri yaygındır: takastan kıymetli metale, kâğıt paraya ve nihayet dijital formlara geçiş. Necmeddin Güney ve Ömer Faruk Tekdoğan, "Merkez Bankası Dijital Paralarının (Mbdp) İslam Hukuku Açısından Değerlendirilmesi", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.222-223.

[1136] Varoufakis, *Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,* s.21.

[1137] Varoufakis, *Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,* s.20.

ekonomik bir değişim aracı değil; artık değerin yönetimi üzerinden otorite üreten siyasal bir mekanizma hâline gelmiştir.

Yunancada sikke (*nomisma*) ile düşünmek (*nomizo*) ve kanun (*nomos*) arasındaki yakınlık da tesadüf değildir: Madeni ve kâğıt paraya değer kazandıran şey, onun ülke çapında kabulünün hukukî ve siyasal bir zorunluluk hâline getirilmesi ve bu değerin sürdürüleceğine dair kolektif inançtır. Paranın işlenmesini sağlayan temel unsur bu nedenle güvendir[1138].

Bu bağlamda parasal güvenin siyasal formu egemenliktir. Klasik egemenlik doktrininde para basma, ölçü ve tartıları düzenleme ve dolaşımdaki paranın değerini belirleme yetkileri egemenliğin merkezî unsurları arasında yer alır. Para, ekonomik hayatın ortak ölçüsü olarak, hukuk düzeniyle benzer bir düzenleme gücü taşır. Bu nedenle parasal yetki, tarihsel olarak siyasal üstünlüğün sembollerinden biri olmuştur[1139]. Egemenliğe sahip olan devlet, paranın değerini ve dolaşım koşullarını belirleyerek toplumsal hayatın en kritik koordinasyon alanlarından birini kontrol eder. Parasal egemenlik, bu anlamda devlet egemenliğinin ekonomik temelini oluşturur[1140].

Ne var ki küreselleşme ve finansal entegrasyon, parasal egemenliği dijitalleşmeden önce de aşındırmaya başlamıştır. Sermaye hareketlerinin sınır aşan bir nitelik kazanması, merkez bankalarının para akışını doğrudan kontrol etmekten ziyade yönlendirmeye çalıştığı bir dönemi beraberinde getirmiştir[1141]. Ulusal para politikaları, küresel finans piyasalarının gerçek zamanlı tepkileriyle sürekli etkileşim hâlinde şekillenmekte; faiz, kur ve bütçe politikaları arasındaki bağlar sıkılaştıkça devletlerin ekonomik karar alanı daralmaktadır[1142]. Bu süreç, ulus-devletin ortadan kalktığını değil;

[1138] Varoufakis, *Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi,* s.123-126.

[1139] Roma İmparatorluğu'nun altın para basma hakkını merkezde tutması, vilayetlere bakır ve gümüşte sınırlı izin verirken altını yasaklaması da parasal yetkinin siyasal bir üstünlük işareti olduğuna dair tarihsel bir örnektir. Bodin, Egemenlik Üzerine, s. 114-117.

[1140] Akad, Dinçkol ve Bulut, s.126.

[1141] Drucker, s.202.

[1142] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.387-389.

küresel ağlara dâhil olmanın bedelinin egemenlik alanlarının daralması olduğunu göstermektedir[1143].

Ademimerkeziyetçi dijital paralar, bu aşınmayı yeni bir eşiğe taşımaktadır. Kripto varlıklar ve dağıtık defter teknolojilerine dayalı ödeme sistemleri, devlet denetiminin dışında işleyen mimarileriyle para basma ve dolaşımı düzenleme kapasitesini zayıflatmaktadır. Bu sistemler, klasik parasal egemenlik araçlarının (vergi toplama, sermaye hareketlerini izleme, kara para aklama ve finansal suçlarla mücadele) etkinliğini azaltan bir etki üretmektedir[1144]. Sınır aşan ve merkezsiz işlem yapıları, parasal düzenlemenin mekânsal varsayımlarını geçersiz kılmakta; devletin para üzerindeki münhasır yetkisini fiilen paylaşılır hâle getirmektedir.

Kripto varlıkların sağladığı anonimlik veya iz sürmeyi güçleştiren teknik özellikler, bu etkiyi daha da derinleştirmektedir. İşlemlerin merkezi bir otorite tarafından doğrulanmaması, finansal gözetim ve denetim mekanizmalarının dışında kalan yeni risk alanları yaratmaktadır. Bu durum, finansal istikrarı ve kamu düzenini ilgilendiren sorunların giderek daha belirgin biçimde ulusal güvenlik meselesi hâline gelmesine yol açmaktadır[1145]. Parasal egemenlik, artık yalnızca ekonomik değil; aynı zamanda güvenlik boyutu olan bir siyasal sorun olarak ortaya çıkmaktadır.

Bununla birlikte ademimerkeziyetçi dijital paraların egemenlik üzerindeki etkisi tek yönlü değildir. Bu sistemler, devlet müdahalesine kapalı yapıları nedeniyle, siyasal saiklerle yapılan parasal müdahalelere karşı bir koruma alanı olarak da görülmektedir. Geleneksel para rejimlerinde devletin kriz dönemlerinde piyasaya müdahale edebilme kapasitesi, istikrarı yeniden tesis etme imkânı sunarken; bu müdahaleler zaman zaman enflasyon gibi toplumsal maliyetler de üretmiştir. Kripto varlıkların tasarım gereği

---

[1143] Uluslararası kurumların ve uluslar üstü konsorsiyumların dünya politikasında oynadıkları rolün giderek büyümesi, ulus-devletin çöküşüyle bir tutulamaz. Ama ulus-devletlerin devlet ağları oluşturarak ayakta kalmak için ödedikleri bedel, egemenliklerinin giderek azalmasıdır. Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.420.

[1144] Robby Houben ve Alexander Snyers, "Crypto-assets: Key developments, regulatory concerns and responses", European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, 2020, s.13.

[1145] Douglas W. Arner, Jànos Barberis ve Ross P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", **Northwestern Journal of International Law & Business,** Vol.37, No.3, (2017), s.400.

müdahaleye kapalı mimarisi, bazı aktörler açısından bu tür maliyetlere karşı bir güvence olarak algılanmaktadır. Ancak aynı özellik, kriz anlarında kamusal müdahale kapasitesinin yokluğunu da beraberinde getirerek şokların derinleşmesi ve bireysel kayıpların artması riskini doğurur.

Bu ikili doğa, ademimerkeziyetçi dijital paraların parasal egemenliği yalnızca zayıflatmadığını; aynı zamanda egemenliğin ekonomik araçlarının meşruiyeti üzerine yeni tartışmalar ürettiğini göstermektedir. Paranın devlet tekeline dayalı olarak düzenlenmesi, bir yandan kamusal denetim ve istikrar sağlarken, diğer yandan siyasal müdahale riskini barındırır. Buna karşılık merkezsiz dijital paralar, müdahaleye kapalı yapılarıyla bireysel özerklik alanı açarken, kamusal koruma mekanizmalarını zayıflatır. Bu gerilim, parasal egemenliğin dijital çağda yeniden düşünülmesini zorunlu kılmaktadır.

Sonuç olarak ademimerkeziyetçi dijital paralar, parasal egemenliğin sınırlarını bulanıklaştırmakta ve egemenlik kavramının dijital çağda yeni bir kriz hattı yaşadığını ortaya koymaktadır. Bu kriz, yalnızca paranın formuna ilişkin değildir; para üzerinden vergi, finansal gözetim, suçla mücadele, sermaye hareketleri ve kamusal istikrar araçlarının tamamı yeniden tanımlanmaktadır. Devletler açısından mesele, dijital finansal dönüşümü bütünüyle dışlamak değil; bu alanı düzenleyerek parasal istikrarı, kamusal denetimi ve egemenliğin ekonomik temelini dijital koşullara uyumlu biçimde yeniden kurmaktır. Parasal egemenlik tartışması bu yönüyle teknik bir protokol meselesi değil; finansal altyapının hangi aktörler tarafından, hangi amaçlarla ve hangi denetim rejimi altında yönetileceğine ilişkin siyasal bir mücadele alanıdır.

2. Dijital Çağda Temel Hak ve Özgürlükler: Demokratik Toplum Düzeninde Erozyon

Dijital çağda temel hak ve özgürlükler, yalnızca hukuki düzenlemelerle güvence altına alınan soyut normlar olmaktan çıkarak; veri işleme süreçleri, algoritmik karar sistemleri ve otomatik sınıflandırma mekanizmaları tarafından fiilen yeniden tanımlanan alanlara dönüşmektedir. Bu dönüşüm, demokratik toplum düzeninin dayandığı eşitlik, ayrımcılık yasağı, ifade özgürlüğü, özel hayatın gizliliği ve masumiyet karinesi gibi temel

ilkelerin, görünmez ve denetlenmesi güç teknik süreçler aracılığıyla aşınmasına yol açmaktadır.

Bu aşınma, bireylerin gündelik yaşamlarında somut hak ihlalleri olarak ortaya çıkmaktadır. Örneğin, Sümeyye Selin'in aylarca aynı özgeçmişle yaptığı iş başvurularının yalnızca adını "S. Selin" olarak kısalttığında olumlu sonuçlanması, algoritmik işe alım sistemlerinin ayrımcılık yasağını dolaylı biçimde ihlal edebildiğini göstermektedir. Görünürde tarafsız olan veri temelli değerlendirmeler, isimler üzerinden etnik, dinsel veya toplumsal cinsiyet temelli önyargıları yeniden üretmekte; böylece eşit işe erişim hakkı teknik araçlar yoluyla zedelenmektedir.

Benzer biçimde, Berlin'de yaşayan Jonas'ın her gün algoritma tarafından daha güvenli olduğu gerekçesiyle önerilen güzergâhları kullanması, seyahat özgürlüğü ve kent hakkının kod aracılığıyla yeniden sınırlandırıldığını ortaya koymaktadır. Algoritmaların göçmen mahallelerini sistematik olarak dışarıda bırakması, mekânsal ayrımcılığı görünmez kılmakta ve bireyin farkında olmadan ayrımcı bir güvenlik mantığını içselleştirmesine neden olmaktadır. Bu bağlamda güvenlik, bireyin özgür hareket alanını daraltan teknik bir sınıflandırma kriterine dönüşmektedir.

Finansal alandaki dijitalleşme ise mülkiyet hakkı ve ekonomik özgürlükler bakımından yeni kırılganlıklar yaratmaktadır. Nairobi'de yaşayan Amina'nın kredi başvurusunun gelir durumu yerine sosyal medya faaliyetlerine dayalı bir güven skoruyla reddedilmesi, ekonomik haklara erişimin siyasal görüşler ve ifade biçimleriyle ilişkilendirilmesine yol açmaktadır. Bu durum, ifade özgürlüğü ile ekonomik özgürlükler arasında dolaylı ama etkili bir baskı mekanizması kurmaktadır.

Algoritmik sistemlerin etkisi yalnızca maddi haklarla sınırlı değildir; düşünce ve kanaat özgürlüğü de bu süreçten doğrudan etkilenmektedir. Toronto'da yaşayan Alex'in haber akışının algoritmalar tarafından tek tipleştirilmesi, bireyin farklı görüşlere erişim imkânını daraltmakta ve düşünce oluşum sürecini yönlendirmektedir. Böylece ifade özgürlüğünün ön koşulu olan çoğulcu kamusal alan, kişiselleştirilmiş veri akışları içinde parçalanmaktadır.

Gözetim teknolojilerinin yaygınlaşması ise özellikle özel hayatın gizliliği ve insan onuru açısından derin sorunlar doğurmaktadır. Şangay'da yaşayan 17 yaşındaki Lin'in sosyal kredi sistemi üzerinden disiplin puanıyla değerlendirilmesi ve bunun sosyal yaşama doğrudan etkide bulunması, çocuk hakları ve ölçülülük ilkesi bakımından ciddi ihlalleri gündeme getirmektedir. Gözetim, bu bağlamda istisnai bir güvenlik tedbiri olmaktan çıkarak, sürekli ve içkin bir denetim rejimine dönüşmektedir.

Bu örnekler birlikte değerlendirildiğinde, dijital çağda temel hak ve özgürlüklerin artık yalnızca hukuk normlarıyla değil, teknik mimarilerle belirlendiği görülmektedir. Algoritmalar, hakların kullanım koşullarını fiilen düzenleyen yeni normatif aktörler hâline gelmiş; bireyleri görünmez ölçütlerle sınıflandırarak eşitlik, özgürlük ve özerklik ilkelerini aşındırmıştır. Demokratik toplum düzeninin merkezinde yer alan yurttaş, bu süreçte hak öznesi olmaktan çıkarak davranışları öngörülen ve yönlendirilen bir veri profiline indirgenmektedir.

a. Temel Hak ve Özgürlükleri Koruma ve Yerine Getirme Yükümlülüğünde Zafiyet ve Dijital Anayasacılık

İnsan hakları, modern devletin insan onuruna yöneltebileceği tehditlere karşı bireyi korumak üzere geliştirilmiş, yargısal güvencelere dayanan özgün bir normatif alandır. Bu alan, insanın salt insan olmasından kaynaklanan ve evrensel kabul edilen bir özden hareket eder; bu özün merkezinde insan onuru kavramı yer alır[1146]. İnsan onuru, insanın kişi olarak en yüksek aklî ve ahlakî değerlerin dokunulmaz ve kaybedilmez sahibi olmasını ifade eden, ispata gerek duymayan varoluşsal bir gerçekliktir. Bu nedenle insan, başka bir gerekçeye ihtiyaç duyulmaksızın her koşulda saygıyı hak eden bir varlık olarak kabul edilir[1147].

İnsan hakları, insan onurunun korunmasına hizmet eden normatif araçlar olarak birey açısından bir talep ve yetki alanını; devlet, toplum ve diğer bireyler açısından ise ödev ve sorumluluk alanını ifade eder[1148]. Kaynağını yalnızca pozitif hukuk

[1146] Akkaya Kia, *Moderniteden Postmoderniteye Egemenlik ve Hukuk*, s.54.
[1147] Akad, Dinçkol ve Bulut, s.266-267. Uygun, s.506, 517.
[1148] Uygun, s.507.

düzenlemelerinden değil, aynı zamanda ahlakî bir zorunluluktan alan bu hakların temelinde insan onuru yer almakta; insan onuru, her türlü toplumsal, siyasal ve hukuksal müdahaleye karşı ileri sürülebilen kurucu bir ölçüt işlevi görmektedir. Bu anlayış modern anayasal düzenlerde devlete yalnızca haklara müdahale etmeme yükümlülüğü yüklemekle sınırlı kalmaz; haklara saygı gösterme, bireyleri üçüncü kişilerin ihlallerine karşı koruma ve hakların fiilen kullanılmasını sağlama yönünde pozitif yükümlülükler de yükler[1149]. Dolayısıyla insan hakları, demokratik rejimlerde sadece devlet iktidarını sınırlayan normlar değil, aynı zamanda devletin meşruiyet temelini ve varlık amacını belirleyen kurucu anayasal ilkelerdir[1150].

Hobbes'un güvenlik-hukuk ilişkisini merkeze alan sosyal sözleşme yaklaşımıyla da uyumlu biçimde, modern devletin temel varlık gerekçesi, bireylerin güvenliğini ve temel haklarını koruyarak kamu düzeni ve barışı sağlamaktır[1151]. Ancak temel hak ve özgürlüklerin korunması, yalnızca hukuk kurallarının varlığıyla değil, bu kuralların yönetenler, yargı ve toplum tarafından içselleştirilmesiyle mümkündür. Bu nedenle hukuk devleti; iktidarın sınırlandırılması, kuvvetler ayrılığı ve özellikle yargısal denetim mekanizmaları aracılığıyla temel hakların korunmasını güvence altına alan bir yönetim biçimi olarak şekillenmiştir. Klasik anayasal mimaride yargıya verilen yasama ve yürütme işlemlerini denetleme yetkisi, temel hak ve özgürlüklerin fiilen korunmasının asli güvencesi olarak kabul edilmiştir[1152].

Dijital teknolojilerin yaygınlaşması, devletin temel hak ve özgürlükleri korumaya yönelik klasik anayasal mimarisini köklü biçimde sarsmaktadır. Bilişim sistemleri, yapay zekâ uygulamaları ve küresel dijital ağlar; birey, devlet ve özel sektör arasındaki geleneksel sınırları bulanıklaştırarak, devletin hak koruma kapasitesini yeni ve karmaşık zafiyetlerle karşı karşıya bırakmaktadır. Verinin küresel ölçekte toplanması ve işlenmesi, birkaç büyük teknoloji şirketinin tekelinde yoğunlaşmakta; bu durum hem veri koruma rejimlerini zorlamakta hem de rekabet hukukunu ve veri minimizasyonu ilkesini

---

[1149] Akal, *Devlet, Yasa, Hakimiyet*, s.29.
[1150] Uygun, s.505.
[1151] Akkaya, *"J.B. Bossuet: 'Devlet Sizsiniz Majesteleri'!",* s.815.
[1152] Doğan Soyaslan, "Hukuk Devletin ve Güvenlik", **Prof. Dr. Sabih Arkan'a Armağan,** İstanbul: On İki Levha Yayıncılık, 2019, s.1025-1026.

temel haklar bakımından kritik hâle getirmektedir[1153]. Büyük Birader'in gizlilik istilaları için araç olarak kullanılabilen dijital aygıtlar, bir yandan kamu gücünün gözetim kapasitesini artırırken, diğer yandan şeffaflık eksikliği, hesap verilemeyen karar alma süreçleri ve profil çıkarmaya dayalı ayrımcılık riskleri nedeniyle özgürlük alanlarını daraltmaktadır[1154]. Algoritmik sistemlerin kasıtlı ya da kasıtsız biçimde ayrımcılığa yol açabilmesi, özellikle eşitlik ve kişi hakları bakımından yeni ihlal biçimlerini görünür kılmaktadır[1155].

Dijitalleşme, Sanayi Devrimi'nin devletin yapısını ve işleyişini dönüştürmesine benzer biçimde, egemenliğin somut yaşam pratiklerine nüfuz eden yeni biçimlerini ortaya çıkarmaktadır[1156]. Ancak bu dönüşüm küresel ölçekte eşitsiz gerçekleşmekte; dijital altyapıya, veri kaynaklarına ve algoritmik güce sahip ülkeler ile bu alanlarda bağımlı konumda kalan ülkeler arasında yeni bir hiyerarşi üretmektedir. Böylece klasik sömürgecilik ilişkileri, bu kez teknoloji ve veri ekseninde yeniden üretilmekte; sınır aşan veri akışları ve dijital platformlar aracılığıyla ulus-devletlerin egemenlik alanları aşınmaktadır. Dijitalleşme, bu yönüyle yalnızca egemenliği dönüştürmekle kalmamakta; hukuk devleti ilkesini de işlevsel bir krizle karşı karşıya bırakmaktadır[1157].

Dijital teknolojilerin toplumsal yaşama nüfuzu, devletin denetim kapasitesini özgürlük alanlarına doğru genişletirken, bu genişlemenin sınırları konusunda ciddi belirsizlikler yaratmaktadır. Gözetim araçlarının güçlenmesi bireysel mahremiyeti zayıflatırken, bireylerin de devlet faaliyetlerini kayda alıp küresel ölçekte görünür kılabilmesi çift yönlü bir gözetim ilişkisi doğurmaktadır[1158]. Ayrıca dijital platformların sunduğu anonimlik ve hız, yalnızca devletin değil, devlet dışı aktörlerin de hak ihlallerini

---

[1153] Elif Beyza Akkanat Öztürk, "Rekabet Hukuku ve Veri Minimizasyonu: Sömürücü 'Veri' Uygulamaları", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.386-387.

[1154] Papagianneas ve Knight, s.38, 39; Serkan Bulut, s.93.

[1155] Oostveen ve Irion, s.10-11; Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.6.

[1156] Küzeci, s.26.

[1157] Smuha, s.3.

[1158] Örneğin kamu görevlilerinin keyfi, usulsüz veya yasaya aykırı faaliyetleri bireyler tarafından fotoğraf veya video olarak kaydedilip anında tüm dünyaya duyurulabilmesi mümkündür. Uygun, s.607.

kolaylaştırmakta; anonim hesaplar ve teknik gizleme araçları üzerinden yürütülen tehdit, hakaret ve itibar saldırıları çoğu zaman etkili bir yaptırıma tabi tutulamamaktadır[1159].

Dijital çağda temel hakların korunması bakımından belirginleşen temel ikilemlerden biri, uluslararası ticaret hukukunun veri akışlarının serbestleştirilmesini teşvik ederken, insan haklarının korunmasının büyük ölçüde ulusal hukuki mekanizmalara dayanmasıdır. Yapay zekâ ve veri yönetimi alanında hukukun üstünlüğü ile inovasyon arasındaki gerilim, demokratik değerlerle ekonomik çıkarlar arasında kurulması gereken dengenin zorluğunu göstermektedir[1160]. Ekonomik faaliyetlerin çevrimiçi ortama taşınmasıyla teknoloji şirketlerinin yeni merkezi otoriteler hâline gelmesi, bu aktörlerin nasıl denetleneceği sorununu gündeme getirmekte; klasik siyaset felsefesinin "bekçileri kim denetleyecek?" sorusu dijital platform ekonomisinde yeniden ortaya çıkmaktadır[1161].

Algoritmik ayrımcılık, veri sömürüsü ve ifade özgürlüğünün keyfî sınırlandırılması gibi ihlaller artarken, bu ihlalleri dengeleyecek uluslararası iş birliği mekanizmaları aynı hız ve etkinlikte gelişmemektedir[1162]. BM İş Dünyası ve İnsan Hakları Rehber İlkeleri (Ruggie İlkeleri), şirketlerin insan haklarına saygı sorumluluğunu vurgulasa da devletlerin şirketlerden hak ihlali doğuracak taleplerde bulunması sorununa yeterli çözüm sunmamaktadır[1163]. BM'nin rehber ilkeleri ve OECD 2019 Yapay Zekâ İlkeleri'nin devletlerin koruma yükümlülüğü ile şirketlerin insan haklarına saygı sorumluluğunu ayrıştırarak çok aktörlü bir yaklaşım[1164] geliştirse de bağlayıcılık eksikliği ve uygulama güçlükleri, dijital teknolojinin yarattığı yeni ihlaller karşısında koruma

---

[1159] VPN (Virtual Private Network: Sanal Özel Ağ), internette gizli, güvenli ve özel bir bağlantı kurmayı sağlayan bir teknolojidir. Kullanıcının verilerini şifreleyerek kimliğini gizler ve cihazla sunucu arasında güvenli bir tünel oluşturarak tüm internet trafiğini korur. (Chip Online, "VPN nedir, nasıl çalışır ve nasıl kullanılır? Soru ve cevaplarla VPN," https://www.chip.com.tr/makale/vpn-nedir-nasil-calisir-ve-nasil-kullanilir-soru-ve-cevaplarla-vpn_154128.html (E.T.: 1 Şubat 2026).

[1160] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.241-242.

[1161] Lehdonvirta, s.7.

[1162] Akın Karatay, "Bilişim ve Teknoloji Şirketlerinin İnsan Hakları Sorumluluklarına İlişkin Güncel Gelişmeler", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.115.

[1163] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.10.

[1164] Organisation for Economic Co-operation and Development (OECD), **OECD AI Principles,** 2018, https://oecd.ai/en/ai-principles (E.T.: 1 Şubat 2026).

mekanizmalarının yetersizliğini görünür kılmaktadır. BM İnsan Hakları Konseyi'nin vurguladığı üzere insan hakları çevrimiçi ve çevrimdışı alanlarda eşdeğer biçimde korunmalıdır[1165]. Ancak dijital teknolojilerin aksine, insan hakları sınırları aşarak akmaz. İnsan haklarının icrası hâlen büyük ölçüde devletlerin coğrafi yetki alanları içinde örgütlenmektedir.

Avrupa Konseyi yaklaşımına göre, özel aktörlerin insan hakları ihlallerini önleyemeyen devletler bu ihlallerden sorumludur; devletler ayrıca şirketlerin uluslararası insan hakları standartlarıyla uyumsuz genel hizmet şartlarını geçersiz kılabilecek etkili hukuki mekanizmalar oluşturmakla yükümlüdür[1166]. Millî güvenlik, insan haklarına sınırsız üstünlük tanıyan bir gerekçe teşkil etmez; bu kavram ancak devletin anayasal düzenini tehdit eden durumlarda ve yargısal denetime açık biçimde meşru kabul edilebilir. Bu ilke internet ve elektronik haberleşme alanı bakımından da geçerlidir[1167]. Hukukun üstünlüğü, çevrimiçi ve çevrimdışı alanlar arasında ayrım yapılmaksızın uygulanmalı; devletler, açık rıza ya da açık, belirli ve sınırlı bir uluslararası hukuki dayanak olmaksızın sınır aşan veri akışlarına erişmemelidir. Şirketlerin yükümlülüklerini ve devletin denetim sorumluluğunu netleştiren bağlayıcı rehberlik mekanizmaları geliştirilmelidir[1168]. Bu bağlamda şirketlerin hak ihlali doğurabilecek devlet talepleri karşısındaki sorumluluklarını kapsayacak şekilde uluslararası ilkelerin güçlendirilmesi ve özel hayatın gizliliği konusundaki insan hakları düzenlemelerinin millî güvenlik ve istihbarat faaliyetleri dâhil tüm devlet eylemlerine uygulanması gerekmektedir[1169].

1982 Anayasası m. 13'e göre temel hak ve özgürlükler ancak kanunla, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uygun olarak sınırlandırılabilir. İfade, basın ve örgütlenme özgürlüklerine ilişkin anayasal hükümler ile

---

[1165] United Nations Development Programme (UNDP), İş Dünyası ve İnsan Hakları Rehber İlkeleri: Guiding Principles on Business and Human Rights (Türkçe yayın), 2023, https://www.undp.org/sites/g/files/zskgke326/files/2023-06/bhr_ungp_rehberilkelerrapor.29.05.23_web.pdf (E.T.: 1 Şubat 2026), s.3.

[1166] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.14.

[1167] Millî Güvenlik, İfade Özgürlüğü ve Bilgiye Erişim Üzerine Johannesburg İlkeleri, devletlerin insan haklarına müdahale etme sebebi olarak millî güvenliğe, ancak ülkenin terör gibi bizzat yapısını ve temel kurumlarını tehdit eden konulara ilişkin olarak başvurabileceğini açıklığa kavuşturmaktadır. Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.17.

[1168] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* m. 14, 19.

[1169] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* m. 15, 18. s.21-22.

uluslararası insan hakları sözleşmeleri (AİHS m. 10, MSHS m. 19), haklara getirilecek sınırlamaların açık, öngörülebilir ve meşru amaçlı bir yasal temele dayanmasını zorunlu kılar. Buna karşın dijital platformlar, içerik kaldırma, hesap kapatma ve algoritmik filtreleme gibi uygulamalarla bireylerin ifade ve örgütlenme özgürlüklerine fiilen müdahale etmekte; bu müdahaleler çoğu zaman açık, erişilebilir ve öngörülebilir bir kanuni temele dayanmamaktadır. Bu durum, özgürlüklerin yalnızca kanunla sınırlandırılabileceği yönündeki temel ilkeyle bağdaşmayan, özel aktörler eliyle gerçekleşen fiilî bir sınırlamalar alanı yaratmaktadır.

İnsan haklarının vatandaşlara değil herkese uygulanması ilkesi dijital alanda da geçerlidir[1170]. Ne var ki özellikle ABD merkezli şirketlerin küresel dijital ekosistemdeki belirleyici konumu, bazı güvencelerin yalnızca "ABD'deki kişiler" bakımından işletilmesi sebebiyle, dijital ortamda hukukun üstünlüğünü zayıflatabilmektedir. Uluslararası insan hakları hukuku, devletlerin sınır ötesi etkileri olan eylemlerinde dahi yükümlülüklerine uymasını gerektirir; kişisel veriler bakımından bu zorunluluk daha da belirginleşir. Buna karşın ABD gibi ülkelerce bu sınır ötesi yükümlülük anlayışını resmen reddetmesi[1171] veya dar yorumlanması dijital alanda hak korumasını yapısal olarak kırılganlaştırmaktadır.

İnternet üzerinde çelişen ulusal hukukların eşzamanlı uygulanması, ifade özgürlüğü başta olmak üzere ciddi sorunlar doğurur. Devletlerin yabancı içerikler üzerinde yargı yetkisi kullanımı, kural olarak net ve yakın bir bağlantı bulunmadıkça sınırlı kalmalıdır. Rastgele ve toptan erişim engellemeleri ise ifade özgürlüğü bakımından keyfî etkiler doğurarak demokratik toplum düzeniyle bağdaşmaz. Bu bağlamda AİHM'nin Yıldırım v. Türkiye içtihadı, belirli bir içerik hedeflenirken tüm hizmete

---

[1170] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.8.

[1171] ABD hukukunda ifade, örgütlenme ve özel hayatın korunmasına ilişkin anayasal güvenceler (Birinci ve Dördüncü Değişiklikler), ayrıca FISA ve Patriot Yasaları bağlamındaki sınırlı korumalar, esas olarak yalnızca ABD'deki kişiler için geçerlidir. Buna karşılık uluslararası insan hakları hukuku, özellikle ICCPR ve AİHS, devletlere insan haklarını yalnızca kendi vatandaşları için değil, yargı yetkilerine tabi olan herkes için güvence altına alma yükümlülüğü yükler. Bu yükümlülük, güncel içtihatlarda bölgesel değil işlevsel biçimde yorumlanmakta; devletin fiilî denetimi altında bulunan ya da eylemlerinden etkilenen herkes için, sınır ötesi faaliyetler dâhil, geçerli sayılmaktadır. Ancak ABD, uluslararası insan hakları hukukunun bu sınır ötesi uygulanabilirliğini resmî olarak reddetmekte, özellikle dijital gözetim ve istihbarat faaliyetleri bakımından bu yükümlülükleri kabul etmemektedir. Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.9.

erişimin engellenmesinin, öngörülemez ve aşırı sonuçları nedeniyle ifade özgürlüğünü ihlal edebileceğini göstermiştir[1172].

İnternet altyapısının ve küresel dijital ekosistemin büyük ölçüde özel şirketlerin kontrolünde bulunması dijital alandaki düzenleme ve denetim yetkilerinin fiilen özelleştirilmesi sonucunu doğurmakta; bu yapısal dönüşüm ise temel hak ve özgürlüklerin korunması bakımından normatif ve kurumsal bir gerilim üretmektedir. Çünkü dijital platformlar, ifade özgürlüğü başta olmak üzere temel haklara yönelik sınırlamaları, devlet organlarının tabi olduğu anayasal yargısal denetim ve uluslararası insan hakları yükümlülüklerine doğrudan ve aynı yoğunlukta tabi olmaksızın uygulayabilmekte; buna ek olarak sınır ötesi veri erişimi ve veri paylaşımı talepleri, egemenlik, ticari mahremiyet ve kişisel verilerin korunması alanlarında çok katmanlı ihlal riskleri ortaya çıkarmaktadır[1173]. Bu durum, bir yandan dijital küreselleşme çağında ulus-devletin geleneksel yetki alanının aşınması ve iç hukuk kurumlarının sınır ötesi teknolojileri düzenlemede yetersiz kalmasıyla derinleşmekte, diğer yandan özel aktörlerin anayasal sınırlar dışında genişleyen fiilî iktidarı nedeniyle temel hakların korunmasında belirgin bir boşluk yaratmaktadır[1174]. Nitekim sosyal medya platformları ve dijital hizmet sağlayıcılar, kamusal alanın kurallarını belirleme, içerik denetimi yapma ve yaptırım uygulama suretiyle yasama, yürütme ve yargı benzeri işlevler üstlenmekte; ancak bu yetkiler şeffaflık, hesap verebilirlik ve hukuki öngörülebilirlik ilkeleriyle yeterince çevrelenmemektedir[1175]. Literatürde "private ordering" olarak kavramsallaştırılan bu yapı, kamusal yetkilerin özel aktörler eliyle kullanılmasına işaret ederek demokratik meşruiyet ve hak güvenceleri bakımından ciddi bir açığa neden olmaktadır[1176]. Özellikle baskıcı veya istikrarsız devletlerle küresel şirketler arasındaki ilişkilerde ortaya çıkan yapısal ihlal düzenlerinde insan haklarının korunması çok aktörlü

[1172] AİHM, Atatürk'e saygısızlık olarak görülen bir Google sitesini engellemek için Google Sites tarafından barındırılan tüm web sitelerine Türkiye'den erişimin engellenmesinin keyfi etkiler doğurduğundan demokratik ölçütleri karşılamakta yetersiz kaldığını vurgulamıştır. AİHM, 2. Daire, 18/12/2012, Başvuru No.3111/10, Ahmet Yıldırım v. Türkiye, https://hudoc.echr.coe.int/ par.64-68.

[1173] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.13-14.

[1174] Rocco Bellanova ve Diğerleri, "Towards a critique of algorithmic violence", **International Political Sociology,** Vol.15, No.1, (2021), s.140.

[1175] Çekin, s. 589.

[1176] Çekin, s. 597, 600.

bir sorumluluk alanına dönüşmekteyse de uluslararası insan hakları hukukunun sınırlı denetim ve yaptırım kapasitesi hem devletlerin dolaylı yükümlülüklerini hem de şirketlerin doğrudan sorumluluklarını etkili biçimde tesis etmeyi güçleştirmektedir[1177]. Bu nedenle, insan haklarını sınırlayan uygulamalarda özel şirketlere fiilî düzenleyici rol yüklenmesi yerine, şirketlerin insan haklarına ilişkin yükümlülüklerini açıkça tanımlayan, devletin gözetim ve denetim sorumluluğunu kurumsallaştıran ve çevrimiçi-çevrimdışı alanlar arasında eşdeğer hak korumasını güvence altına alan bağlayıcı ve çok katmanlı normatif mekanizmaların geliştirilmesi, dijitalleşmenin hukuk devleti ve demokratik toplum düzeniyle uyumlu biçimde yapılandırılabilmesi açısından zorunlu görünmektedir[1178].

İdari otoritelerin bu alanı düzenleme çabaları ise bilgi asimetrisi ve teknolojinin hızına yetişememe sorunu nedeniyle sınırlı kalmaktadır. Düzenleyici kurumlar çoğu zaman kanun koyucunun bıraktığı boşlukları ikincil düzenlemelerle doldurmaya çalışmakta; ancak bu süreçte yetki genişlemesi, menfaat dengesinin bozulması ve parçalı bir normatif yapı oluşması riski doğmaktadır. Böylece birey hem devletin hem de özel aktörlerin kullandığı dağınık ve çok merkezli iktidar ağları karşısında korunmasız kalabilmektedir[1179].

Bu çok katmanlı kriz karşısında, geleneksel liberal anayasacılığın dijital tehditler karşısında yetersiz kaldığı giderek daha açık hâle gelmektedir. Bu yetersizlik, dijital anayasacılık olarak adlandırılan yeni bir yaklaşımın ortaya çıkmasına yol açmıştır. Dijital anayasacılık, dijital alanda ortaya çıkan yeni güç odaklarına karşı temel hak ve özgürlükleri korumayı hem devletin hem de özel aktörlerin yetkisini anayasal sınırlar içinde tutmayı amaçlayan bir anayasal çabadır; dijital bir anayasa değildir[1180]. Dijital uzayın sunduğu imkânlar kadar yarattığı tehditleri de dikkate alan bu yaklaşım, özellikle çevrimiçi platformların keyfi güç kullanımına karşı bir koruma mekanizması olmayı ve dijital toplumu modern anayasacılığın fren ve denge mekanizmalarıyla uzlaştırmayı

[1177] Altın Aslı Şimşek, "İnsan Hakları Hukuku ve İş Dünyası İlişkisi: Hukuki Yükümlü ile Kurumsal Sorumlu Arasında", **Prof. Dr. Sabih Arkan'a Armağan,** İstanbul: On İki Levha Yayıncılık, (2019) s.1191.
[1178] Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* m. 14, 19.
[1179] Çekin, s.600-601.
[1180] Kama Işık, s.75; Cemil Caca Arslan, s.262.

hedeflemektedir[1181]. Ancak kavramın sınırları, araçları ve meşruiyeti konusundaki belirsizlikler, dijital anayasacılığı hem koruyucu bir çerçeve hem de yeni bir meşrulaştırma dili üretme riski taşıyan muğlak bir alan hâline getirmektedir[1182]. Klasik anayasalar, kamu otoritelerinin gücünü sınırlayarak bireyi devlete karşı korumayı amaçlarken; veri ve bilişim teknolojilerinin gelişimiyle birlikte kamusal nitelik taşıyan yeni bir dijital kuram ortaya çıkmıştır. Bu bağlamda mesele, artık yalnızca devletin dijital alanı nasıl düzenleyeceği değil; dijital uzayın yeni aktörlerince fiilen kullanılan kamusal gücün nasıl sınırlandırılacağı sorusuna dönüşmüştür[1183].

b. Algoritmik Ayrımcılık ve Fırsat Eşitliğinin Derinleşmesi

Dijital çağın ilk dönemlerinde teknoloji, temel hak ve özgürlüklerin kullanımını genişleten nötr bir araç olarak sunulmuştur. İnternet ve dijital platformların, ifade özgürlüğünü güçlendireceği, bilgiye erişimi demokratikleştireceği ve fırsat eşitliğini artıracağı varsayılmıştır. Ancak bu beklenti, dijital teknolojilerin iktidar ilişkilerinden bağımsız gelişmediğinin anlaşılmasıyla kısa sürede geçerliliğini yitirmiştir. Dijital sistemler, kamusal alanı eşitlemek yerine, mevcut toplumsal eşitsizlikleri veri temelli karar mekanizmaları aracılığıyla yeniden üretmeye başlamıştır[1184].

Modern hukukta eşitlik, bireyler için bir hak ve yönetenler için uyulması gereken bir ilke olarak, benzer durumda olanlara makul ve somut nedenler dışında eşit muamele yapılmasını zorunlu kılar; ihlali ise ayrımcılık olarak kabul edilir[1185]. Ultra teknolojilerin yarattığı dönüşüm, özellikle eşitlik ilkesi ve fırsat eşitliği bakımından belirgin bir hak aşınmasına yol açmaktadır. Dijitalleşmeyle birlikte kamu hizmetlerinden istihdama, finansal erişimden adalet sistemine kadar birçok alanda karar alma süreçleri algoritmik sistemlere devredilmektedir. Bu sistemler çoğu zaman verimlilik, hız ve tarafsızlık gerekçeleriyle meşrulaştırılsa da dayandıkları veri setlerinin toplumsal önyargılarla

---

[1181] Kama Işık, s.87-90.
[1182] Cemil Caca Arslan, s.245-249.
[1183] Cemil Caca Arslan, s.250-251.
[1184] Çalgan, s.77.
[1185] Nihat Bulut, Eşitlik (Hukuk), TÜBİTAK Yayınları Ansiklopedisi, TÜBİTAK, 2022, Erişim: https://ansiklopedi.tubitak.gov.tr/ansiklopedi/esitlik_hukuk

şekillenmiş olması nedeniyle ayrımcı sonuçlar üretme potansiyeli taşımaktadır[1186]. Böylece eşitlik ilkesi, hukuki güvenceye dayalı bir hak olmaktan çıkarak, teknik sınıflandırmaların belirlediği kırılgan bir koşula dönüşmektedir[1187].

Algoritmik ayrımcılığın ayırt edici özelliği, doğasındaki işleyiş gereği ayrımcı etkiyi açık bir kast veya niyet olmaksızın üretmesidir. Algoritmalar, geçmiş verilerden hareketle karar üretirken, bu verilerin içerdiği tarihsel eşitsizlikleri geleceğe taşır. Kredi değerlendirmeleri, işe alım süreçleri veya risk analizleri, görünüşte tarafsız ölçütlere dayanmakla birlikte; ırk, cinsiyet, sosyoekonomik statü veya sağlık durumu gibi korunan niteliklerle dolaylı bağlantılar kurarak dezavantajlı grupları sistematik biçimde dışlayabilir[1188]. Bu durum, ayrımcılığın niyet yerine sonuçlar üzerinden değerlendirilmesini zorunlu kılar.

Dijital önyargı kavramı, bu sistemlerin veri setlerine gömülü sosyal kodları nasıl yeniden ürettiğini tanımlamak için kullanılmaktadır. Bu bağlamda algoritmalar, yalnızca geçmişi taklit etmez; geçmişin eşitsizliklerini dijital biçimde sürdürerek toplumsal adaletin görünmez düşmanına dönüşür. Bu karmaşık önyargı biçimleri özellikle arama motorları gibi günlük bilgi erişimimizi belirleyen araçlarda iç içe geçmiştir[1189]. Arama motorlarının erkek kullanıcılara daha yüksek ücretli iş ilanları göstermesi[1190] sigorta primlerinin cinsiyete bağlı farklılaşması[1191] veya posta kodu gibi dolaylı göstergeler üzerinden dezavantajlı grupların riskli sınıflara itilebilmesi, dijital ayrımcılığın rastlantısal değil, yapısal olduğunu ortaya koyar. Bu etkiler özellikle bireyin hayat şansını belirleyen işe alım[1192] kredi değerlendirme, sigorta ve ceza adaleti gibi kritik eşiklerde yoğunlaşmaktadır.

[1186] Erol, s.36.

[1187] Mürvet Ece Büyükçalık, "Algoritmalar Ayrımcılık Yasağına Riayet Eder Mi?", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (31-48), Ankara: Adalet Yayınevi, 2023, s.31-33.

[1188] Ali, Erdoğan, "We Likened Them To Ourselves: Algorithmic Discrimination And Bias", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.117.

[1189] Schneider, *China's Digital Nationalism,* s.65, 66.

[1190] Gillespie, s.190.

[1191] All Tech Is Human, s.9, 13.

[1192] Amazon'un işe alım algoritması kadın adayları sistematik olarak dışlaması buna örnektir. Geçmiş işe alım verilerindeki cinsiyetçi örüntüler, algoritmanın modellemesine yansımış; kadınlarla ilişkilendirilen kelimeler içeren özgeçmişlerin puanı düşürülmüştür. Şirket projeyi sonlandırmış olsa da bu örnek dijital araçların özel sektörde dahi

Bu noktada sorulması gereken soru şudur: Algoritmalar mı ayrımcıdır, yoksa toplumdaki önyargılar mı algoritmaları biçimlendirmektedir? Cevap iki yönlüdür. Algoritmalar kendi başlarına değer üretmez; onları besleyen veri setleri, toplumsal normlar, iktidar ilişkileri ve yerleşik eşitsizliklerle şekillenmiştir. Bu nedenle ayrımcılık, çoğu zaman sistemin niyetinden değil, sistemin dayandığı verinin ve modelin kurduğu istatistiksel düzenekten doğar[1193]. Çarpıcı olan, bu mekanizmanın ayrımcı bir kast bulunmaksızın dahi ayrımcılık üretebilmesidir: Niyet yoktur, fakat etki vardır.

Bu bağlamda klasik ayrımcılık ayrımları, dijital çağda yeni bir içerik kazanmaktadır. Doğrudan ayrımcılık[1194] algoritmik kararların açık biçimde korunan bir temele dayalı farklı muamele üretmesi hâlinde ortaya çıkarken[1195] dolaylı ayrımcılık[1196] görünüşte nötr olan teknik ölçütlerin belirli gruplar üzerinde orantısız olumsuz etki doğurmasıyla gerçekleşmektedir[1197]. Algoritmik sistemlerde bu iki ayrım çoğu zaman iç içe geçmekte; biyometrik, davranışsal veya mekânsal göstergeler aracılığıyla ayrımcı sonuçlar teknik zorunluluk görüntüsü altında meşrulaştırılabilmektedir[1198].

---

ciddi bir denetim ihtiyacına işaret etmektedir. Jeffrey Dastin, "Insight - Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters*, 11 Ekim 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (1 Şubat 2026).

[1193] UNESCO, Preliminary Study on The Ethics of Artificial Intelligence, 2019, https://unesdoc.unesco.org/ark:/48223/pf0000367823 (14 Aralık 2024) s.8.

[1194] Doğrudan ayrımcılık, TİHEK Kanunu m. 2(d)'de, bir kişinin hukuken tanınmış hak ve hürriyetlerden karşılaştırılabilir durumdakilere kıyasla eşit yararlanmasının, kanunda sayılan ayrımcılık temellerine dayanılarak engellenmesi veya zorlaştırılması şeklinde tanımlanır.

[1195] Büyük veri ve algoritmik karar verme süreçleri bireyleri; ırk, cinsiyet, inanç gibi korunan niteliklerle bağlantılı biçimde sınıflandırıp farklı muameleye tabi tuttuğunda ister kasıtlı ister kasıtsız olsun ayrımcılığı pekiştirme potansiyeline sahiptir. Örneğin bir bireyin çevrimiçi ortamda araştırdığı hastalık bilgileri veya psikolojik durumuna ilişkin dijital izleri, sağlık sigortası primini artıran bir risk faktörü olarak kullanıldığında, bu durum doğrudan ayrımcılığın çağdaş bir görünümü hâline gelebilir. Oostveen ve Irion, s.10.

[1196] Dolaylı ayrımcılık, TİHEK Kanunu m. 2(e)'de, görünüşte ayrımcı olmayan bir işlem veya uygulamanın, ayrımcılık temelleriyle bağlantılı olarak kişiyi nesnel olarak haklılaştırılamayan bir dezavantajlı konuma sokması şeklinde tanımlanır.

[1197] Algoritmalar bakımından, modelin kurulumu veya kullanımının bazı gruplar üzerinde orantısız olumsuz etki üretmesi, dolaylı ayrımcılık kapsamında değerlendirilebilir. Örneğin algoritmik işe alım süreçlerinde nötr görünen biyometrik ölçütler (boy uzunluğu, belli fiziksel yeterlilik eşikleri gibi) kadınları veya bazı etnik grupları sistematik biçimde dışlıyorsa, bu dolaylı ayrımcılığın tipik bir örneğidir. Büyükçalık, s.44.

[1198] TürkiyeHukuk.org, "Algoritmaların Adalet Sınavı," https://www.turkiyehukuk.org/algoritmalarin-adalet-sinavi/ (E.T.: 1 Şubat 2026).

Yapay zekâ ve otomatik karar sistemlerinin etik muhakemeden yoksun olması, bu süreci daha da derinleştirmektedir[1199]. Algoritmalar, bağlamı yorumlayamaz; empati, hakkaniyet veya gerekçelendirme kapasitesine sahip değildir[1200]. Bu nedenle kararlar, insan muhakemesinin sağladığı düzeltici esneklikten yoksun biçimde üretilir[1201]. Üstelik "kara kutu" olarak tanımlanan bu sistemler, hem bireylerin haklarını neden kaybettiklerini anlamalarını zorlaştırmakta hem de etkili başvuru ve itiraz yollarını fiilen işlevsiz kılmaktadır. Bu durum, hak arama özgürlüğü ve hukuki güvenlik ilkeleri açısından ciddi bir sorun alanı yaratmaktadır[1202].

Algoritmik ayrımcılığın uluslararası düzeyde en çok tartışılan örneklerinden biri, ABD'de ceza adaletinde kişilerin yeniden suç işleme riskini tahmin eden fakat ırksal önyargı iddialarıyla tartışmalı olan COMPAS algoritmasıdır. Beyaz tenlilere yüksek, siyah tenlilere düşük risk atfedilmesine rağmen sonuçların tersine gerçekleşmesi, algoritmik kararların tarafsız olmadığını ve ayrımcı sonuçlar doğurabildiğini göstermiştir[1203]. ProPublica'nın 2016 tarihli incelemesi, siyah sanıkların yüksek riskli olarak yanlış sınıflandırılma oranının beyazlara kıyasla daha yüksek olduğunu ortaya koyarak, bu sistemlerin eşitlik ve hukuki güvenlik ilkeleriyle bağdaşmadığını ortaya koymuştur[1204]. Benzer biçimde ABD'de State of Wisconsin v. Loomis (2016) kararında Wisconsin Eyaleti Yüksek Mahkemesi (Wisconsin Supreme Court), bu tür skorların tek başına belirleyici kılınmaması ve dikkatle değerlendirilmesi gerektiğine işaret ederek, algoritmik çıktının yargısal karar üzerindeki ağırlığına ilişkin ilkesel bir uyarı

[1199] Büyükçalık, s.37.

[1200] Dyson, s.312. İçinde von Neumann, 1952, Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components.

[1201] Alexander Tischbirek, "Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems", Thomas Wischmeyer ve Timo Rademacher (Ed.), **Regulating Artificial Intelligence** içinde (103-122), Springer, 2020, s.112.

[1202] Janneke Gerards, "The fundamental rights challenges of algorithms", **Netherlands Quarterly of Human Rights**, Vol.37, No.3, (2019), s.205.

[1203] Murat Balcı, "Yapay Zekâ ve Ayrımcılık: Anayasa Hukukunun Dönüşümü", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (367-390), İstanbul: Adalet, 2021, s.384-385.

[1204] Seda Yağmur Sümer, "'Compas' Örneği Çerçevesinde Yapay Zekalı Risk Değerlendirme Araçları ve Ceza Muhakemesine Hâkim Olan İlkeler", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.65.

üretmiştir[1205]. Bu örnekler, algoritmik ayrımcılığın yalnızca bireysel mağduriyet yaratmadığını; masumiyet karinesi, adil yargılanma ve eşitlik gibi anayasal ilkeleri de doğrudan zorladığını göstermektedir.

Avrupa düzleminde ayrımcılık yasağının normatif temeli, AİHS m.14 ve AB Temel Haklar Şartı m.21 gibi düzenlemelerde görünürdür. Bu çerçeve, ayrımcılığın yalnızca doğrudan değil dolaylı biçimlerine karşı da koruma sağlar. AB hukukunda algoritmaları geliştirenlerin kasıtlı davranıp davranmaması ayrımcılık yasağı açısından tali nitelik taşır[1206]. Nitekim ABAD'ın Test-Achats (C-236/09) kararında, istatistiksel temellere dayansa dahi cinsiyete bağlı prim farklılıklarının sigorta tarifelerinde belirleyici unsur olarak kullanılmasının eşitlik ilkesine aykırı bulunması, teknolojik/istatistiksel gerekçelerin ayrımcılığı meşrulaştıramayacağını göstermesi bakımından önemlidir[1207]. Günümüzde bireyler, kişisel verilerine doğrudan erişmeseler bile alışveriş tercihleri, sosyal çevreleri veya çevrimiçi davranış kalıpları üzerinden cinsiyet, etnik köken veya sosyal statüye dair çıkarımlara tabi tutulabilmekte; bu da dolaylı ayrımcılığın dijital düzeyde ne kadar sistematik ve görünmez şekilde kurumsallaşabildiğini göstermektedir[1208].

AB Yapay Zekâ Yasası'nın 5. maddesi, kabul edilemez risk taşıyan yapay zekâ uygulamalarını yasaklamaktadır[1209]. 5. maddenin 1. fıkrasının (c) bendi özellikle sosyal puanlama amacıyla bireylerin davranışları veya kişisel niteliklerine göre sınıflandırılmasının haksız muamele ve orantısız ayrımcılığa yol açarak temel hak ihlalleri doğurabileceğini kabul etmektedir.

[1205] State v. Loomis, 130 Harv. L. Rev. 1530 (2017), https://harvardlawreview.org/print/vol-130/state-v-loomis/#footnote-28 (2 Şubat 2026).

[1206] Publications Office of the European Union, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1 (1 Şubat 2026), s.67.

[1207] Association belge des Consommateurs Test-Achats and Others v. Conseil des ministres, Case C-236/09, Judgment of 1 March 2011, EU:C:2011:100, https://curia.europa.eu/juris/liste.jsf?language=en&num=C-236/09 (2 Şubat 2026).

[1208] Tischbirek, s.107, 108.

[1209] European Parliament & Council of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union L 1689, https://data.europa.eu/eli/reg/2024/1689/oj (2 Şubat 2026).

Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği'nin 2021 tarihli raporunda otomatik karar sistemlerine yönelik uyarılar gibi uluslararası girişimler; yapay zekâ ve profilleme teknolojilerinin mahremiyet, adil yargılanma hakkı ve keyfî müdahale yasağı üzerinde doğrudan hak etkileri ürettiğine işaret ederek hem devletlere hem de özel sektöre yönelen normatif basıncın arttığını göstermektedir[1210].

Türkiye bakımından ise algoritmik ayrımcılığı doğrudan ele alan kapsamlı bir normatif çerçevenin yokluğu dikkat çekmektedir. Mevcut koruma, büyük ölçüde genel eşitlik ilkesi ve kişisel verilerin korunması rejimi üzerinden dolaylı biçimde sağlanmaktadır. Ancak algoritmik karar sistemlerinin karmaşıklığı ve görünmezliği, bu korumanın çoğu zaman yetersiz kalmasına yol açmaktadır.

Algoritmik ayrımcılık tartışması, yalnızca karar sistemlerinin iç işleyişine değil, fırsat eşitliğinin maddi koşullarına da uzanır. Teknolojik yayılmanın hızı ve ölçeği seçicidir; insanlar, ülkeler ve bölgeler arasında teknolojiye erişim zaman farkları, başlı başına bir eşitsizlik kaynağı üretir[1211]. Dijital uçurum bu nedenle salt internet hızı meselesi değil; bilgiye erişim hakkının, eğitim ve istihdam fırsatlarının, siyasal katılım kapasitesinin küresel ölçekte adaletsiz dağılımı problemidir[1212]. Dijital altyapıyı, veriyi ve teknik standartları kontrol eden devletler ve şirketler, bu kontrol aracılığıyla küresel bir tahakküm kurabilirken; geri kalanlar bilgiye bağımlı, edilgen ve dışlanmış bir konumda kalabilmektedir. Bu yönüyle dijital uçurum, egemenlik hiyerarşisini yeniden üreten emirleri ABD'nin verdiği dijital sömürgecilik benzeri bir ilişkiyi besleyen yapısal bir zemine dönüşebilir[1213].

Sonuç olarak algoritmalar, dijital çağda teknik araçlar olmaktan çıkmış; doğrudan siyasal ve hukuksal sonuçlar üreten iktidar teknolojilerine dönüşmüştür[1214]. Bu durum, eşitlik ilkesinin soyut ve biçimsel yorumunun yetersiz kaldığını ve algoritmik karar sistemlerinin fiilen ayrımcılık üretip üretmediğinin denetlenmesini zorunlu

[1210] Christina Cocito ve Paul De Hert, "United Nations: AI can pose risks to human rights and privacy", **Privacy Laws & Business: International Reports,** (2021).
[1211] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi,* s.43.
[1212] Sunstein, s.21.
[1213] Aust ve Ammann, s.13.
[1214] Bellanova ve Diğerleri, s.138.

kılmaktadır. Aristoteles'in, eşit olmayan durumlara eşit muamelenin adaletsizlik doğuracağı yönündeki tespiti[1215] bağlamdan kopuk algoritmik eşitleme pratikleri karşısında güncelliğini korumaktadır. Nitekim yapay zekâ sistemleri, veri setlerinin yapısı ve karar süreçlerindeki şeffaflık eksikliği nedeniyle ayrımcılığı teknik tarafsızlık görünümü altında yeniden üretebilmekte; bu da tespit ve ispat süreçlerini zorlaştırarak bireylerin hak arama imkânlarını fiilen zayıflatmaktadır. Bu nedenle fırsat eşitliği, dijital çağda yalnızca normatif bir ilke değil, algoritmik tasarım ve uygulamaya yöneltilmiş bağlayıcı bir kamusal yükümlülük hâline gelmiştir. Ayrımcılık yasağının yapay zekâya ilişkin düzenlemelerde açık ve bağlayıcı biçimde yer alması ve kasten ayrımcı kullanımların yaptırıma bağlanması gerekmektedir[1216].

c. Gözetim Çağında Kitle İletişimi ve Gizliliğin Çözülmesi

Kitle iletişiminin gözetlenmesi başlığı altında izlenen kurgu, dijitalleşmenin temel haklar üzerindeki etkisini hakları tek tek sıralayan bir yaklaşım yerine, öznenin farklı varoluş boyutları üzerinden bütünlüklü biçimde analiz etmeyi amaçlamaktadır. Mahremiyetin çöküşü, dijital çağda gözetimin yarattığı genel çerçeveyi ortaya koyarken; kişisel verilerin korunması, bu sürecin teknikleşmiş ve kurumsallaşmış boyutunu görünür kılmaktadır. Anonimlik hakkı, öznenin kamusal alandaki ifade ve varlık kapasitesinin nasıl kırılganlaştığını gösterirken; ulaşılamama hakkı, dijitalleşmenin zaman, beden ve zihin üzerindeki tahakkümünü açığa çıkarmaktadır. Unutulma hakkı ise dijital hafızanın sürekliliği karşısında bireyin kimliğini, zamanla kurduğu ilişkiyi ve gelecek tasavvurunu koruma mücadelesini merkeze almaktadır. Bu dizilim, temel hakları soyut normlar olarak değil; mekân, veri, kimlik, beden ve hafıza gibi öznenin kurucu boyutları üzerinden ele alarak, dijital çağda özgürlüğün çok katmanlı dönüşümünü ortaya koymaktadır.

- **Gözetim Toplumunda Mahremiyetin Çöküşü:** Dijitalleşme, yalnızca iletişim biçimlerini değil, egemenlik ve denetim ilişkilerinin kurucu mantığını da dönüştürmüştür. Geleneksel olarak devletin sınır çizme ve şiddet tekeli üzerinden tanımlanan egemenlik anlayışı; dijital çağda veri akışlarını, iletişim altyapılarını ve

[1215] Uygun, s.134.
[1216] Balcı, s.387.

kamusal görünürlüğü kontrol etme kapasitesi üzerinden yeniden kurulmaktadır. İletişim ve haberleşmenin devlet tekeli olmaktan çıkarak çok aktörlü ve rekabetçi bir yapıya evrilmesi[1217] kitle iletişimini genişletirken gözetim pratiklerinin yaygınlaşmasına ve gizliliğin yapısal olarak aşınmasına zemin hazırlamıştır. Bu dönüşüm, demokratik toplumun kurucu unsurlarından biri olan mahremiyet hakkını istisnai ihlallerin konusu olmaktan çıkararak süreklileşmiş bir risk alanına dönüştürmüştür.

Mahremiyet, demokratik toplum düzeninde yalnızca bireyin özel hayatını koruyan dar bir gizlilik alanı değil; özgür yurttaşlığın, özerk kişilik gelişiminin ve siyasal katılımın ön koşulu niteliğindedir[1218]. Bireyin kendisiyle baş başa kalabildiği, düşünsel ve zamansal bir iç mekânın varlığı, eleştirel düşünme ve siyasal kanaat oluşturma süreçleri bakımından belirleyici bir işleve sahiptir. Ancak dijitalleşme ile birlikte bireylerin iletişim pratikleri, gündelik davranışları ve sosyal ilişkileri sürekli izlenebilir, kaydedilebilir ve analiz edilebilir hâle gelmiştir. Bu durum, mahremiyeti fiilen kullanılan bir özgürlük alanı olmaktan uzaklaştırarak bireyin özerkliğini zayıflatmaktadır.

Sürekli izlenebilirlik durumu, yalnızca mahremiyetin ihlaliyle sınırlı kalmamakta; bireyin düşünme, ifade etme ve siyasal katılım pratiklerini de doğrudan etkilemektedir. İzleniyor olma ihtimali, açık bir yasaklama olmaksızın oto-sansürü tetiklemekte; bireylerin eleştirel düşünme, kamusal tartışmalara katılma ve siyasal görüşlerini ifade etme alanlarını daraltmaktadır. Bu bağlamda mahremiyetin aşınması, ifade özgürlüğü ve siyasal katılım gibi hakların fiilen kullanılabilmesinin ön koşullarını zayıflatarak demokratik toplum düzenini içten içe erozyona uğratmaktadır.

[1217] Osman Açıkgöz, "Elektronik Haberleşme Sektöründe Arabağlantı Sözleşmesi", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (207-218), İstanbul: Adalet, 2021, s.208-209.

[1218] United Nations Human Rights Council, The Right to Privacy in the Digital Age, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018, https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf, par.5. Demokratik toplumun temellerinden olan bu hakkın ihlali, domino etkisiyle diğer temel hakları da tehdit eder. United Nations Human Rights Council, Right to Privacy in the Digital Age, Draft Resolution, A/HRC/48/L.9, 4 October 2021, https://documents.un.org/doc/undoc/ltd/g21/268/44/pdf/g2126844.pdf s.2; United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/48/31, 2021, https://docs.un.org/en/A/HRC/48/31 par. 7.

Mahremiyetin bu şekilde aşınması, gözetimin teknik ve kurumsal araçlarıyla daha da derinleşmektedir. Kamera sistemleri, mobil cihazlar ve dijital veri tabanları aracılığıyla bireylerin; mekânsal hareketleri, tüketim alışkanlıkları ve sosyal ilişkileri sürekli izlenebilir durumdadır. Sağlık verilerinden iletişim içeriklerine kadar uzanan geniş bir veri setinin kamu ve özel aktörlerin erişimine açık hâle gelmesi, bilgi ve iletişim teknolojilerinin sunduğu kolaylıklarla birlikte ciddi mahremiyet risklerini de beraberinde getirmektedir. Geçmişte haberleşmenin gizliliği kapsamında değerlendirilen elektronik iletişim, günümüzde teknik olarak kolaylıkla ihlal edilebilir bir nitelik kazanmış; böylece iletişimin gizliliği hakkı normatif gücünü yitirme tehlikesiyle karşı karşıya kalmıştır[1219].

Dijital gözetimin ayırt edici yönü, klasik denetim biçimlerinden farklı olarak dağınık, çok aktörlü ve büyük ölçüde görünmez bir yapı üretmesidir. Devletler ile dijital platformlar arasında kurulan işlevsel ilişkiler, iletişim altyapıları ve veri akışlarının kamusal denetimden uzaklaşmasına yol açmaktadır. Birey bu yapı içerisinde aynı anda hem kamusal hem de özel aktörlerin gözetimine maruz kalmakta; mahremiyet, ihlal edilen tekil bir hak olmaktan çıkarak kullanımı giderek daraltılan bir özgürlük alanına dönüşmektedir.

Bu süreç, dijital teknolojilerin sunduğu büyük veri ve algoritmik analiz olanaklarıyla yeni bir boyut kazanmıştır. Suç kayıtları, iletişim ve seyahat verileri ya da sosyal medya içerikleri üzerinden oluşturulan dijital profiller, geleceğe yönelik öngörüler üretmek amacıyla kullanılmaktadır. Tarafsızlık iddiasıyla çalışan bu sistemler, çoğu zaman mevcut önyargıları ve yapısal ayrımcılıkları yeniden üretmekte[1220] algoritmik öngörünün belirsiz doğasına rağmen fiilî bir makul şüphe zemini olarak cezai süreçlere dâhil edilebilmektedir. Bu durum, özel hayatın gizliliği, adil yargılanma ve keyfi müdahaleden korunma gibi temel haklar bakımından ciddi riskler doğurmaktadır[1221].

[1219] Uygun, s.607.

[1220] Berçin Kuzu, "Dijital Çağda İnsan Haklarının Gelişimi", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (143-156), Ankara: Adalet Yayınevi, 2023, s.148-149.

[1221] United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age, A/HRC/48/31,* par.24.

Nitekim AİHM içtihadı, ulusal güvenlik gerekçesiyle kurulan kitlesel gözetim sistemlerinin, yeterli hukuki güvenceler ve etkili denetim mekanizmaları bulunmadığında demokrasiyi koruyan değil, onu aşındıran araçlara dönüşebileceği uyarısında bulunmuştur[1222]. Bu risk yalnızca otoriter rejimlere özgü değildir; dijital gözetim, liberal demokrasilerde de siyasal katılımı zayıflatarak kamusal alanı daraltabilir[1223].

Dijital gözetimin yaygınlaşması ve normalleşmesi, büyük ölçüde teknolojinin hayatı kolaylaştırdığı ve mahremiyet beklentilerinin "doğal olarak değiştiği" yönündeki söylemlerle meşrulaştırılmaktadır. Mark Zuckerberg'in mahremiyetin bir sosyal norm olarak yeni bir evreye girdiği iddiası, bu dönüşümü kaçınılmaz ve bireysel tercihlerin sonucu gibi sunmaktadır[1224]. Oysa bu yaklaşım, platform bağımlılığı, bilgi asimetrisi ve manipülatif rıza tasarımları gibi yapısal koşulları görünmez kılmaktadır. Bu bağlamda rıza, bireyin insan onuruna dayalı özerk iradesini yansıtan bir hak kullanımı olmaktan çıkarak, çoğu zaman hizmetlerden dışlanmama kaygısıyla verilen biçimsel ve zorunlu bir onay prosedürüne indirgenmektedir. Dijital hizmetlere erişimin verilerin işlenmesine onay verilmesine bağlanması, bireyi kendi kişisel verileri üzerinde söz sahibi bir özne olmaktan uzaklaştırarak izlenebilir ve yönetilebilir bir nesneye dönüştürmektedir. Kullanıcıların veri paylaşımının kapsamı ve sonuçları konusunda yeterli bilgiye sahip olmadan, hizmetle ilgisi olmayan veri taleplerini kabul etmek zorunda kalması, bireyin özel alanını ciddi biçimde tehlikeye sokarken[1225] özellikle çocuklar gibi kırılgan gruplar bakımından ağır sonuçlar doğurmakta[1226] rızayı koruyucu bir hak güvencesi olmaktan çıkararak mahremiyetin sistematik çözülüşünü meşrulaştıran sembolik bir formaliteye

---

[1222] AİHM, Büyük Daire, 04/12/2015, Başvuru No.47143/06, Roman Zakharov v. Russia, par.232, https://hudoc.echr.coe.int/?i=001-159324

[1223] United Nations, Human Rights Council, The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014, https://digitallibrary.un.org/record/777869 par.2

[1224] Bobbie Johnson, "Privacy No Longer a Social Norm, Says Facebook Founder", *The Guardian* (11 Jan. 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (2 Şubat 2026)

[1225] Mustafa Yeniad, "Sosyal Ağlar ve Siber Güvenlik", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya,** içinde (18-20), Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, Vol.Ocak, Sayı.9, s.19.

[1226] 30 Temmuz 2020 tarihli 2020-939 sayılı yasanın 22. maddesi, çeşitli kısıtlamalar içeren Fransız Ceza Kanunu'nun 227-24. maddesini tamamlayarak, bir kullanıcının 18 yaşında olduğunu beyan etmesinin rıza için yeterli olmayacağını belirtmiştir.

dönüştürmektedir. Böylece mahremiyetin gerileyişi, bireysel tercihlerin sonucuymuş gibi sunulurken, yapısal bir güç ilişkisi olarak görünmez hâle gelmektedir.

Bu noktada dijital gözetimin ardındaki ekonomik ve siyasal mantık, Shoshana Zuboff'un kavramsallaştırdığı gözetim kapitalizmi çerçevesinde açıklık kazanmaktadır. Zuboff'a göre gözetim kapitalizmi, insan deneyimini sistematik biçimde izleyen, ölçen ve analiz eden; bu deneyimlerden türetilen davranışsal verileri gelecekteki davranışları öngörmek ve yönlendirmek amacıyla kullanan özgün bir iktidar biçimidir. Bu düzende bireylerin dijital izleri, pasif biçimde depolanan veriler olmaktan çıkarak ekonomik değeri olan davranışsal artı-değer kaynaklarına dönüşmektedir. Böylece veri, klasik üretim süreçlerinden bağımsız bir sermaye işlevi kazanmakta; iktidarın ağırlık merkezi, devlet merkezli egemenlikten ziyade algoritmik sistemlere ve dijital platformlara kaymaktadır.

Gözetim kapitalizmi yalnızca bir ekonomik model değil, aynı zamanda bireyi yurttaşlık, hak ve siyasal katılım temelinde tanımlayan modern çerçevenin ötesine geçen, davranış temelli yeni bir toplumsallık biçiminin kurucu mantığıdır[1227]. Endüstriyel kapitalizmin emeği ve üretimi örgütleyerek doğaya egemen olmayı hedeflemesine benzer biçimde, dijital kapitalizm de insan davranışını doğrudan birikim alanına dönüştürmektedir. Bu düzende birey, hak sahibi bir yurttaş olarak değil; izlenebilir, ölçülebilir ve öngörülebilir bir veri kaynağı olarak konumlanır.

Gözetim kapitalizminin ayırt edici yönlerinden biri, mahremiyetin yalnızca kamusal alanda değil, bireyin en özel mekânı olan evde de aşınmasıdır. Tarihsel olarak korunma ve yalıtılmışlığın simgesi olan ev[1228] akıllı cihazlar, sensörler ve dijital asistanlar aracılığıyla sürekli veri üreten bir izleme alanına dönüşmektedir. Mekânın sınırları artık dışsal müdahalelerle değil, bireyin kendi dijital pratikleri yoluyla içeriden dışarıya doğru çözülmektedir. Bu dönüşümle birlikte mahremiyet, "saklanacak şeyler" meselesi olmaktan çıkarak, düşünsel özerklik, içe dönük farkındalık ve özgür kişilik gelişimi için

[1227] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.11.
[1228] Rukiye Akkaya Kia, "Mekân: Hukuk Fakültesi Apartmanı", **Hukuk Kuramı,** Cilt.6, No.2, (Mayıs-Ağustos 2019), s.48.

zorunlu olan bağlantısız zaman ve mekânın ön koşulu olarak yeniden anlam kazanmaktadır[1229].

Bu rejimde satılan şey, kişisel verinin kendisi değil, insan davranışından türetilmiş öngörü modelleridir. Dijital platformlar kullanıcıyı müşteri olarak sunarken, gerçekte onu davranışsal tahminlerin üretildiği bir hammadde kaynağına indirger. Kullanıcı klasik anlamda müşteri ya da ürün değildir; gelecekteki davranışlara ilişkin tahminlerin üretildiği ve pazara sunulduğu süreçte araçsallaştırılmış bir özne konumundadır[1230]. Google ve Facebook gibi platformların, başlangıçta hizmet kalitesini artırma gerekçesiyle topladığı verileri zamanla hedefli reklamcılık ve davranış yönlendirme mekanizmalarına dönüştürmesi, bu iktidar tekniğinin somut örneklerini oluşturmaktadır[1231].

Zuboff bu süreci, teknolojik bir evrimden ziyade, piyasa güdümlü ve toplumsal rıza üretimine dayanan sessiz bir darbe olarak tanımlar. Akıllı cihazlar ve dijital hizmetler, birer "Truva atı" gibi işleyerek insan deneyimini fark ettirmeden ele geçirir; öğrenme, anlam kurma ve toplumsal etkileşim süreçleri giderek özel şirketlerin denetimi altına girer; böylece iktidar, açık baskı araçlarıyla değil, normalleştirme, yönlendirme ve teşhir yoluyla işler. Sonuçta mahremiyetin çözülmesi, yalnızca bireysel gizliliğin kaybı değil; irade, bilinç ve özgür kişilik gelişiminin yapısal olarak aşındırıldığı bir toplumsal duruma işaret eder[1232].

Bu noktada tehdit, teknolojinin kendisinden ziyade, teknolojiyi yönlendiren piyasa temelli tahakküm mantığıdır[1233]. Gözetim kapitalizmi, her yere yayılmış dijital aygıtlar aracılığıyla bireylerin davranışını sistematik biçimde izleyen, hesaplayan ve yönlendiren görünmez bir düzenek gibi çalışır[1234]. Bu iktidar biçimi, bireylerin dijital izlerini ekonomik bir rasyonaliteye bağlayarak her tıklamayı, etkileşimi ve çevrimiçi

---

[1229] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.586-591.
[1230] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.24, 123-127.
[1231] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.16.
[1232] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s. 586-591, 628-629.
[1233] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.28-29.
[1234] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.463-464, 543.

davranışı davranışsal artı-değer üreten bir kaynağa dönüştürür; böylece veri, pasif biçimde depolanan bir unsur olmaktan çıkıp gelecekteki davranışları öngörmek ve yönlendirmek amacıyla işlenen stratejik bir sermaye niteliği kazanır. Davranışsal artı-değerin keşfiyle, hizmet sunumu için gerekli olandan çok daha fazla veri toplanarak bireyin erişemediği algoritmik süreçlerde işlenir ve tahmin sistemlerini besler.

Duyguların ve tepkilerin pazarlanabilir verilere indirgenmesiyle şirketler kullanıcıların gelecekteki davranışlarını tahmin etmeye ve etkilemeye çalışmakta; iktidar, görünmeyen fakat son derece etkili olan algoritmik mekanizmalar aracılığıyla kurulmaktadır[1235]. Bu süreçte iktidarın ağırlık merkezi klasik anlamda devletten ziyade algoritmik sistemlere kayarken, sanayi kapitalizminin doğayı sömürerek çevresel krizler üretmesine benzer biçimde, dijital kapitalizm de insan deneyimini ve davranışlarını dönüştürerek yeni bir toplumsal kriz alanı yaratır[1236]. Dijital platformların mahrem verileri sistematik biçimde ticarileştirmesi, bireyi hak sahibi bir özne olmaktan ziyade ölçülebilir, öngörülebilir ve yönlendirilebilir bir veri kaynağına indirgerken, rıza kavramı da çoğu zaman hizmetlerden dışlanmama zorunluluğu altında verilen biçimsel bir onay mekanizmasına dönüşmektedir[1237]. Böylece mahremiyet, evrensel ve eşit bir hak olmaktan uzaklaşarak teknik bilgiye ve dijital okuryazarlığa sahip olanların görece erişebildiği ayrıcalıklı bir alana indirgenmektedir. Facebook'un Moments uygulaması bağlamında yüz verilerinin işlenmesine ilişkin davanın 650 milyon dolarlık tazminatla sonuçlanması[1238] sorunun münferit skandalları aşan yapısal niteliğini göstermektedir.

Gözetim kapitalizmi, bireyin mahremiyetini yalnızca teknik bir sorun olarak değil, benliğin, düşünsel özerkliğin ve özgür kişilik gelişiminin temeli olarak aşındırır. Birey, kendini özgür sanırken kendi gözetim zincirlerini üretir[1239] ve teşhir, norm hâline

---

[1235] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.48-50, 104-105; Hatipoğlu Aydın, s.102-103.
[1236] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.16, 630.
[1237] Küzeci, s.231.
[1238] "Facebook settles facial-recognition privacy lawsuit", *BBC News* (30 Jan. 2020), https://www.bbc.com/news/technology-51309186 (2 Şubat 2026); "Facebook privacy lawsuit over facial recognition leads to $650M settlement", *CNET* (2020) https://www.cnet.com/tech/services-and-software/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/ (2 Şubat 2026).
[1239] Han, s.1, 7-9.

gelir[1240]. Sosyal medya ve akıllı cihazlar, özgürlük ve seçenek vaatleri altında sürekli izleme ve yönlendirme ağları kurar. İktidar artık açık emirlerle değil, dürtme ve yönlendirme yoluyla işler. Platon'un mağara alegorisini andırır biçimde, bireyler hakikatin kendisiyle değil, onun dijital gölgeleriyle yetinmeye razı olur[1241].

Bu yeni tahakküm rejimi, açık zor kullanımıyla değil; gönüllü katılım, konfor ve ücretsiz hizmet söylemi üzerinden işler. Tıpkı sömürgecilik döneminde yerel halkların rıza ve aldatma yoluyla mülksüzleştirilmesi gibi, dijital çağda da kullanıcılar farkında olmadan veri teslimi yoluyla deneyimlerinin mülkiyetini kaybetmektedir. Google ve Facebook gibi büyük platformlar, hukuki boşluklardan ve politik ilişkilerden yararlanarak bireylerin yaşamlarını veri madenciliğiyle metalaştırmış; dijital teknolojilere duyulan bağımlılık ise bu yapının sorgulanmasını güçleştirmiştir. Böylece öğrenme, davranış üretme ve toplumsal anlam kurma süreçleri giderek özel şirketlerin denetimi altına girmiştir[1242].

Dijital gözetim, veri akışlarının izlenmesi ve depolanması yoluyla bir yandan bireyin mahremiyetini tehdit ederken, diğer yandan ulusal güvenlik, kamu düzeninin korunması ve suçla mücadele gibi gerekçelerle zorunlu ve meşru bir araç olarak sunulmaktadır. Bu ikili yapı, temel hak ve özgürlüklerin istisnalar üzerinden yeniden tanımlandığı esnek ve genişlemeye açık bir hak rejimini beraberinde getirmektedir[1243]. Dijital teknolojilerin sağladığı izleme, depolama ve analiz kapasitesi, devletlerin de gözetim yetkilerini tarihsel olarak eşi görülmemiş bir yoğunluk ve kapsama ulaştırmış; böylece gözetim, belirli kişi veya olaylara yönelik istisnai bir tedbir olmaktan çıkarak süreklileşmiş bir yönetim tekniğine dönüşmüştür[1244].

Avrupa İnsan Hakları Mahkemesi içtihadı, kitlesel gözetim uygulamalarının ancak açık, öngörülebilir ve sıkı hukuki güvencelere bağlı olması hâlinde demokratik toplum düzeniyle bağdaşabileceğini vurgulamaktadır. Özellikle Big Brother Watch v.

[1240] Han, s.10-13; Aydeniz, s.38.
[1241] Şenel, s.144-145.
[1242] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.242-244.
[1243] Eren, s.563.
[1244] Küzeci, s.230.

Birleşik Krallık kararında Mahkeme, ulusal güvenlik gerekçesiyle kurulan geniş ölçekli izleme sistemlerinin etkili yargısal denetimden ve yeterli hukuki sınırlardan yoksun olması durumunda, demokrasiyi koruyan değil, onu aşındıran araçlara dönüşebileceği uyarısında bulunmuştur[1245]. Bu bağlamda gözetim, yalnızca otoriter rejimlerin bir pratiği olarak değil, liberal demokrasilerde de siyasal katılımı zayıflatan ve kamusal alanı daraltan yapısal bir risk olarak değerlendirilmelidir.

Dijital çağda gözetimin niteliğini köklü biçimde değiştiren temel unsur, büyük veri analitiği ve yapay zekâ teknolojilerinin devletlerin karar alma süreçlerine dâhil edilmesidir. Gözetim artık yalnızca geçmişe dönük izleme faaliyeti olmaktan çıkmış; bireylerin davranışlarını sınıflandıran, geleceğe yönelik öngörüler üreten ve bu öngörüler üzerinden müdahalede bulunabilen bir dijital disiplin tekniğine dönüşmüştür. Bu durum, masumiyet karinesi ve keyfi müdahaleden korunma ilkeleri bakımından ciddi sorunlar doğurmakta; bireylerin fiilî davranışlarından ziyade istatistiksel olasılıklar üzerinden değerlendirildiği yeni Orwellvari bir güvenlik mantığını kurumsallaştırmaktadır.

Bazı örneklerde bu dönüşüm, açıkça otoriter bir denetim rejimine evrilmektedir. Özellikle Çin'de yüz tanıma sistemleri, kamusal alan izleme ağları ve sosyal puanlama mekanizmaları, güvenlik ve toplumsal düzen gerekçesiyle bireyin mahremiyetini bastıran ve davranışları yönlendiren bütüncül bir dijital disiplin düzeni oluşturmuştur. Ancak benzer tekniklerin farklı yoğunluk ve gerekçelerle demokratik devletlerde de kullanılması, sorunun belirli siyasal rejimlerle sınırlı olmadığını; dijital gözetimin yapısal olarak otoriterleşme potansiyeli taşıyan bir araç olduğunu göstermektedir[1246]. Hukuki çerçevelerin varlığına rağmen, verilerin kullanım zamanı, amacı ve yetkili aktörleri konusundaki belirsizlikler, ciddi hak ihlallerine zemin hazırlamaktadır.

[1245] AİHM'in Big Brother Watch/UK kararı, ulusal güvenlik ve uluslararası suçlarla mücadele kapsamında kitlesel gözetlemeye geniş takdir yetkisi tanımakla birlikte, bunun bağımsız ve etkili denetime tabi olması gerektiğini vurgulamıştır. Sosyal medya platformları bilgiye erişim ve katılım imkânları sunsa da dezenformasyon, nefret söylemi ve demokratik süreçlerin manipülasyonu gibi riskler nedeniyle dijital egemenlik mücadelesinin en yoğun yaşandığı alandır. Eren, s.564.

[1246] Kuzu, s.147.

Gözetim kapitalizmi teknolojik bir zorunluluk değil, tarihin belirli bir döneminde bilinçli biçimde inşa edilmiş bir piyasa modelidir[1247]. Bu model, kapitalizmin kâr ve büyüme hedeflerini korurken, işleyiş düzeyinde köklü bir kırılma yaratır. Üretim araçları artık fabrikalar değil; makine zekâsına dayalı davranış modifikasyon sistemleridir. Nesnelerin internetiyle birleşen bu yapı, sensörler ve bağlı cihazlardan oluşan maddi bir izleme altyapısını zorunlu kılar. Dijital evren, insan davranışlarını bilmek, tahmin etmek ve yönlendirmek üzere tasarlanmış devasa bir çıkarma makinesine dönüşür[1248]. Ford üretimi ölçeklendirmişken, Google davranışsal veri çıkarımını ölçeklendirmiştir. Bu düzende kullanıcı, hizmetin muhatabı değil; başkalarının amaçları için kazınan bir kaynak hâline gelir.

Bu yapıda bireyin deneyimi, bedelsiz bir hammadde olarak sistematik biçimde gasp edilir. Dijital platformlar, kullanıcıyı özgür bir müşteri gibi sunarken, gerçekte onu gönüllü bir veri üreticisine ve sürekli gözetim nesnesine dönüştüren teşhir mekanizmalarıdır. Şiddete dayanmayan; ikna, yönlendirme ve normalleştirme üzerinden işleyen bu araçsalcı iktidar biçimi, bireyleri özgür oldukları yanılsaması içinde yönlendirir. Kullanıcı, özne olmaktan çıkar; emeği veriye indirgenen bir dijital emekçiye dönüşür[1249]. Gözetim kapitalizmi, insan davranışını ham maddeye, insanı ise çıkar döngülerinin nesnesine indirgeyen özgün bir kapitalizm biçimi yaratır[1250]. Böylece devlet ile birey arasındaki bağ; hak ve sorumluluk dengesine dayanan siyasal bir ilişki olmaktan çıkar; veri üretimi karşılığında hizmete erişim sunan sözleşmesel bir ilişkiye indirgenir.

Sonuç olarak dijital gözetim rejimi, bireyi giderek daha öngörülebilir, ölçülebilir ve yönlendirilebilir bir varlığa indirgerken, özgürlük kavramını algoritmik sınırlar içinde yeniden tanımlamaktadır. Bu dönüşüm, yalnızca mahremiyet hakkının zayıflamasıyla sınırlı olmayıp, demokratik toplumun kurucu ilkelerine yönelen yapısal bir krizi ifade etmektedir[1251]. Mesele artık teknik veri güvenliği ya da bireysel gizlilik tercihlerinin

---

[1247] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.100, 114, 235.
[1248] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.91-92, 254-255.
[1249] Aust ve Ammann, s.171-173.
[1250] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.434, 630-631.
[1251] All Tech Is Human, s.17, 19.

ötesine geçmiş; bireyin dijital çağda özerk bir özne olarak varlığını sürdürebilme mücadelesi hâline gelmiştir.

Dijital gözetim, teknik bir yönetim aracı olmaktan çıkarak doğrudan siyasal, etik ve anayasal bir sorun alanına dönüşmektedir. Gözetim kapitalizmiyle iç içe geçen bu rejim, yalnızca bireyin dikkatini değil; iradesini, tercihlerini ve davranışlarını da öngörülebilir ve yönlendirilebilir kılmayı hedeflemektedir. Bu yeni düzende birey, hem sürekli izlenen hem de kendini gönüllü olarak ifşa etmeye teşvik edilen bir veri öznesine dönüşmekte; yurttaşlık statüsü, hak ve sorumluluk dengesine dayanan siyasal bir ilişki olmaktan uzaklaşmaktadır.

Bu bağlamda içinde bulunduğumuz dönemi bir mahremiyetsizlik çağı olarak tanımlamak mümkündür. Bu çağ, birey-devlet ilişkisindeki güç dengesini birey aleyhine çeviren, özgür yurttaşlık statüsünü sessiz ve kademeli biçimde aşındıran bir dijital egemenlik yapısının kurumsallaştığı bir toplumsal düzeni ifade etmektedir[1252]. Dolayısıyla mahremiyetin korunması, salt teknik bir güvenlik meselesi değil; demokratik denetimin, özgür kişilik gelişiminin ve siyasal katılımın sürdürülebilmesinin zorunlu bir koşuludur. Dijital çağda temel hak ve özgürlüklerin korunması, ancak gözetimin sınırlandırıldığı, şeffaflık ve hesap verebilirlik mekanizmalarının güçlendirildiği bir anayasal çerçeveyle mümkün olabilir[1253].

- **Kişisel Verilerin Korunması:** Mahremiyetin yapısal aşınması, dijital çağda en somut karşılığını kişisel verilerin korunması alanında bulmaktadır. Dijital çağda kişisel veriler, bireyin kimliği, bedeni, düşünsel yönelimi ve yaşam tarzı hakkında kapsamlı bir bilgi üretimini mümkün kılmaktadır. Bu verilerin sürekli ve sistematik biçimde toplanması ile işlenmesi, bireyin kendi yaşamı üzerindeki tasarruf alanını daraltmakta; mahremiyeti hak temelli bir koruma alanı olmaktan çıkararak yönetsel ve ekonomik pazarlıkların konusu hâline getirme riskini doğurmaktadır. Bu nedenle teknolojik gelişmelerin insan onuru bakımından yarattığı yapısal riskler karşısında ortaya

[1252] Küzeci, s.229.
[1253] Tischbirek, s.117.

çıkan dördüncü kuşak haklar arasında yer alan[1254] kişisel verilerin korunması hakkı, dijital özgürlüğün ve insan onuruna dayalı bireysel özerkliğin temel ön koşullarından biri olarak değerlendirilmektedir. Kişinin, hangi bilginin kimlerle, hangi amaçla ve ne zaman paylaşılacağı üzerinde etkili bir denetime sahip olmaması, onun özne olarak varlığını sürdürmesini güçleştirmektedir[1255].

Dijital toplumda bireyin kamusal ve sosyal ilişkilerden bütünüyle çekilmesi fiilen mümkün olmadığından, kişiliğin serbestçe gelişiminin ve insan onurunun korunması büyük ölçüde kişisel verilerin etkin biçimde korunmasına bağlıdır. Bu çerçevede kamu ve özel aktörler tarafından zorunlu olarak toplanan kişisel verilerin, yalnızca açık rıza ya da belirli, öngörülebilir ve sınırlı bir kanuni dayanak temelinde işlenmesini sağlayan hukuki güvencelere ihtiyaç vardır[1256]. Kişisel verilerin korunması, yalnızca özel hayatın gizliliğiyle sınırlı dar bir alanı değil; ifade özgürlüğü, unutulma hakkı, insan onuru ve bilgi edinme hakkı gibi birçok temel hakla kesişen geniş bir insan hakları alanını kapsar. Bu nedenle kişisel verileri yalnızca gizlilik kavramı çerçevesinde ele almak, dijital çağın gerçekliği karşısında yetersiz ve indirgemeci bir yaklaşım oluşturmaktadır[1257].

Bilişim teknolojilerinin gelişmesiyle birlikte kişisel verilerin kapsamı, çeşitliliği ve işlenme kapasitesi önemli ölçüde artmış; bu veriler yalnızca özel hayatın gizliliği çerçevesinde korunamaz hâle gelmiştir. Günümüzde bireyler, doğumdan önce başlayıp ölümden sonra da devam edebilen yoğun bir veri gözetimine maruz kalmaktadır. Fiziksel, biyolojik ve psikolojik veriler farklı tekniklerle kaydedilmekte; bireylerin davranışları, alışkanlıkları ve düşünsel eğilimleri analiz edilebilmektedir. Bu süreç kimi zaman toplumsal yarar sağlasa da özgürlük, mahremiyet ve insan onuru bakımından ciddi riskler ve etik sorunlar doğurmaktadır. Veri toplama faaliyetlerinin yalnızca devletle sınırlı kalmayıp özel aktörleri de kapsaması, bireyi çok katmanlı ve sürekli bir gözetim ilişkisi

---

[1254] Uygun, s.538.
[1255] All Tech Is Human, s.16.
[1256] Ali Tanju Sarıgül, "Kişisel Verilerin Korunmasına Yönelik Suçlarla Korunan Hukuki Değer", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (501-512), İstanbul: Adalet, 2021, s.501.
[1257] Sarıgül, s.509.

içine çekmekte; bu da kişisel verilerin insan onuruna uygun biçimde toplanması, saklanması ve kullanılmasını düzenleyen yeni ilkelere olan ihtiyacı artırmaktadır. Kişisel verilerin korunmasının özü, bireyin kendi verileri üzerinde fiilî ve etkili bir tasarruf yetkisine sahip olmasıdır[1258].

Kişisel verilerin korunması hakkı, tarihsel olarak Avrupa'da "bilgi kendiliği" kavramı ile gelişmiş ve bireyin özel hayatı üzerindeki tasarruf hakkı olarak tanımlanmıştır: bireyin kendi yaşamı ve kimliği hakkında hangi bilgilerin, kimlerle, hangi koşullarda ve ne ölçüde paylaşılacağına karar verebilmesini ifade eder[1259]. Bu hak, zaman içinde piyasa süreçlerini destekleyen tali bir araç olmaktan çıkarak, bireysel özerkliği güvence altına alan bağımsız bir temel hak niteliği kazanmıştır[1260]. Bu yönüyle kişisel verilerin korunması, yalnızca bireysel mahremiyetin değil; demokratik toplum düzeninin ve hukuk devleti ilkesinin de kurucu unsurlarından biri olarak değerlendirilmelidir. AİHM bu hakkı AİHS 8. madde kapsamında ve bireysel özerklik temelinde değerlendirirken[1261] AB Temel Haklar Şartı, 8. maddede 7. maddedeki özel hayatın gizliliği ve mahremiyetten bağımsız ve özerk bir temel hak olarak düzenleyerek, bireyin veri üzerindeki denetimini demokratik toplum düzeninin güvencelerinden biri hâline getirmektedir.

Kişisel verilerin korunması hakkı, yalnızca bireyin özel alanını değil; kamusal alanda eşit katılımı, ayrımcılıktan korunmayı ve siyasal tercihlerin manipülasyondan arındırılmasını da doğrudan etkilemektedir. Veri işleme pratikleri, bireylerin ifade özgürlüğünü, örgütlenme özgürlüğünü ve siyasal katılımını fiilen kullanabilme koşullarını belirleyen yapısal bir işleve sahiptir. Bu bağlamda veri koruma ve gizlilik hakları, diğer temel hakların kullanılmasını mümkün kılan etkinleştirici bir rol (enabling

---

[1258] Uygun, s.608-610.

[1259] Kişisel verilerin korunması, 1970'te ilk defa Almanya'nın Hassen eyaletinde düzenleme altına alınmıştır. Almanya Anayasası Mahkemesi'nin Nüfus Sayımı davası (1984) ile popülerleşen bilgi kendiliği hakkı, bireyin, kendiliği fikrine dayalı olarak, özel hayatı hakkında başkalarına ne zaman ve hangi sınırlar içinde bilgi verileceğine karar verme yetkisi olarak tanımlanmıştır. Bodó ve Diğerleri, *"Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks",* s.18.

[1260] Granger ve Irion, *"The right to protection of personal data: The new posterchild of European Union citizenship?",* s.301.

[1261] Oostveen ve Irion, s.6.

function) üstlenmektedir[1262]. Bununla birlikte ABAD; kişisel verilerin korunmasının mutlak bir hak olmayıp, demokratik toplum düzeninde diğer temel haklarla dengelenmesi gereken bir yapı arz ettiğini vurgulamıştır. Bu da hakkın, sadece bireyin çıkarını değil, demokratik hukuk devleti ilkesini de ilgilendiren bir boyuta sahip olduğunu ortaya koymaktadır[1263].

Dijitalleşmenin hızlanması, kişisel verilerin korunmasını zorlaştıran yeni uygulamaları da beraberinde getirmiştir. Otomatik karar alma sistemleri, profilleme, uzun süreli veri saklama ve güvenlik gerekçeli veri toplama pratikleri, temel hakların ikincil plana itilmesine yol açabilmektedir. Özellikle siyasi mikro-hedefleme uygulamaları, bireylerin siyasal tercihlerini yönlendirme potansiyeli taşıyarak hem mahremiyeti hem de demokratik seçim süreçlerini tehdit etmektedir. Bu nedenle çağdaş veri koruma rejimleri, şeffaflık, amaçla sınırlılık, veri minimizasyonu ve otomatik karar süreçlerine itiraz gibi mekanizmalar yoluyla bireye belirli bir özerklik alanı tanımayı amaçlamaktadır. Bu konuda temel olan şeffaflık ilkesi, veriyi işleyen aktörlerin bireylere veri türleri, işleme amaçları ve olası sonuçlar hakkında açık ve anlaşılır bilgi sunmasını gerektirir[1264].

Kişisel verilerin kullanımını kontrol etmeye yönelik araçlar, bireyin belirli veri işleme faaliyetlerine katılmamayı tercih edebilmesine imkân tanıyarak bireysel özerkliği güçlendirmektedir. Bu araçlar, hizmet sunumunun sınırlanması pahasına da olsa, hedefleme ve kişiselleştirme pratiklerini engelleyebilmekte; aynı zamanda yapay zekâ temelli karar alma mekanizmalarının meşruiyetini ve hesap verebilirliğini artırmaktadır[1265]. Bu yönüyle veri koruma düzenlemeleri, bireylerin demokratik

---

[1262] Oostveen ve Irion, s.3.

[1263] Granger ve Irion, *"The right to protection of personal data: The new posterchild of European Union citizenship?",* s.302.

[1264] GDPR'nin 22. maddesi bireylerin otomatik karar alma sistemlerinin amacı ve olası sonuçları hakkında bilgilendirilmesi; hatalı verilerin düzeltilmesini veya silinmesini talep etme ve bu tür karar süreçlerine tamamen itiraz etme haklarını tanımaktadır. Şeffaflık burada kişisel verileri işleyen kuruluşların, bireye verilerin türü, işlenme amacı gibi çeşitli bilgileri sunulmasını gerektirerek elde edilir. Oostveen ve Irion, s.12.

[1265] Sümeyra Sena Kurt, "Genel Veri Koruma Tüzüğü (GDPR) Çerçevesinde Veri Sahibinin Otomatik Karar Verme Mekanizmaları Karşısındaki Hakları", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.112.

süreçlerde manipülasyondan korunmasına ve siyasal tercihlerinin özgürce oluşmasına katkı sağlamaktadır.

Sağlık alanında dijitalleşmenin artması, hassas kişisel verilerin korunmasını daha da karmaşık hâle getirmiştir. Sağlık verileri, ruhsal durum ölçümleri ve duygusal analizler, bireyin bedensel ve psikolojik bütünlüğüyle doğrudan ilişkili olup mahremiyet bakımından yüksek riskler taşımaktadır. Mobil sağlık uygulamalarının yaygın biçimde üçüncü taraflarla veri paylaşması[1266] bireylerin rızası dışında verilerinin dolaşıma girmesi riskini artırmakta ve bireysel özerkliğe doğrudan müdahale anlamı taşımaktadır. Bu nedenle sağlık verilerinin toplanması ve işlenmesi, diğer kişisel veri türlerine kıyasla daha sıkı hukuki güvencelere tabi tutulmalıdır. Türkiye'de de e-Nabız sisteminde işlenen sağlık verileri, bireyin biyolojik ve psikolojik durumu hakkında son derece hassas bilgiler içerdiğinden, bu verilerin toplanması ve işlenmesi daha sıkı düzenlemelerle korunmalıdır. Türkiye'de Sağlık Bakanlığı tarafından yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik, ABD'deki HIPAA ve AB'deki e-Gizlilik Yönergesi, sağlık verilerinin üçüncü taraflara izinsiz aktarımını engellemeye yönelik düzenlenmiştir.

Kişisel verilerin ihlali yalnızca özel aktörlerden değil, doğrudan kamu otoritelerinden de kaynaklanabilmektedir. Özellikle iletişim ve konum verilerinin herhangi bir şüphe ya da yargı kararı olmaksızın toplanması ve saklanması, temel haklar açısından ciddi bir tehdit oluşturmaktadır. Bu tür uygulamalar, bireysel soruşturmalara özgü istisnai tedbirler olmaktan çıkarak, tüm toplumu kapsayan kitlesel gözetim mekanizmalarına dönüşmektedir[1267]. Güvenlik gerekçesiyle sınırsız veri saklama uygulamalarının, özel hayatın gizliliği ve kişisel verilerin korunması hakkına ağır müdahaleler içerdiği; bu nedenle hukuk devleti ilkeleriyle bağdaşmadığı kabul edilmektedir. Nitekim ABAD, Digital Rights Ireland kararında bu tehlikeyi açıkça ortaya koymuş; AB'nin iletişim verilerinin zorunlu olarak saklanmasını öngören düzenlemelerinin güvenlik ile temel haklar arasında gerekli dengeyi kuramadığını

[1266] 2021'de yapılan bir araştırmaya göre mobil sağlık uygulamalarının %87'si verileri üçüncü taraflarla paylaşmaktadır. All Tech is Human, s.28.
[1267] Granger ve Irion, s.837.

belirtmiş; bu sistemin özel hayatın gizliliği ile kişisel verilerin korunması hakkına ağır müdahaleler içerdiğini vurgulamıştır[1268].

Sınır ötesi veri transferleri, dijital ekonominin işleyişi açısından zorunlu olmakla birlikte, mahremiyet ve anayasal haklar bakımından önemli riskler üretmektedir. Küresel veri akışları, yalnızca teknik ve ekonomik bir mesele değil; aynı zamanda normatif ve siyasal bir güç ilişkisi alanıdır. Schrems kararları[1269] ve ABD-Çin rekabeti, veri akışının aynı zamanda bir güç ve norm çatışması[1270] olduğunu göstermektedir. Kişisel verilerin ekonomik bir değere indirgenmesi, mahremiyetin toplumsal ve anayasal niteliğini zayıflatmakta; temel hakların piyasa mantığına tâbi kılınması riskini beraberinde getirmektedir[1271]. Oysa temel haklar, ekonomik değerlerle ölçülemez ve fiyatlandırılamaz kamusal nitelikli güvencelerdir[1272].

Sonuç olarak kişisel verilerin korunması hakkı, dijital çağda birey üzerinde kurulan çok katmanlı gözetim ve yönlendirme ilişkilerine karşı hem bireysel hem de kamusal bir savunma hattı oluşturmaktadır. Bu hak, yalnızca veri güvenliğini değil; insan onurunu, bireysel özerkliği, demokratik katılımı ve toplumsal eşitliği doğrudan ilgilendiren çok boyutlu bir yapıya sahiptir. Bu nedenle kişisel verilerin korunması, yalnızca dijital özgürlüklerin değil, demokratik toplum düzeninin sürdürülebilirliğinin de vazgeçilmez bir güvencesi olarak değerlendirilmelidir.

- **Anonimlik Hakkı: Dijital Hayatta Kimliksiz Kalma Özgürlüğünün Çöküşü:** Kişisel verilerin kontrolünün zayıflaması, anonimliği dijital hayatta giderek

---

[1268] Granger ve Irion, s.835.

[1269] Barbara Li, "China's New Cross-Border Data Transfer Regulations: What You Need to Know and Do", IAPP (3 Apr. 2024), https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do (2 Şubat 2026). 2023'te ABD ile AB arasında bu kopukluğu gidermesi amacıyla oluşturulan Veri Gizliliği Çerçevesi (Data Privacy Framework) ile kurallara uyan Amerikan şirketleri AB'den gelen kişisel verileri koruma altına almış sayılmaktadır.

[1270] Ticari çıkarları öne alan görüşler, ülkeler arasındaki farklı kuralların uyum maliyetlerini artırdığını ve veri yerelleştirmenin teknolojik gelişmeleri ve dijital ticareti sınırladığını savunur. Buna karşıt görüş ise GDPR m.49'un veri aktarımını kural olarak mümkün kıldığını, dolayısıyla ticareti engellemediğini vurgular. Yakovleva ve Irion, s.202-205.

[1271] Christine Breining-Kaufmann, "The Legal Matrix of Human Rights and Trade Law: State Obligations Versus Private Rights and Obligations", Thomas Cottier, Joost Pauwelyn ve Elisabeth Burgi (Ed.) **Human Rights and International Trade** içinde (95-136), Oxford: OUP, (2005) s.103, 104.

[1272] Yakovleva ve Irion, s.208.

işlevsizleştiren bir süreci beraberinde getirmektedir. Anonimlik, dijital çağda yalnızca bireyin kimliğini gizlemesi anlamına gelmemekte; izlenme, fişlenme ya da yaptırıma maruz kalma korkusu olmaksızın düşünme, üretme, eleştirme ve muhalefet edebilme kapasitesini ifade etmektedir. Bu yönüyle anonimlik, ifade özgürlüğü, bilgiye erişim ve özel hayatın korunmasıyla iç içe geçen, demokratik toplum düzeninin işleyişi bakımından temel bir ön koşul niteliği taşır[1273]. Bireyin kimliğini açıklamadan dijital alanda var olabilmesi, özellikle baskıcı siyasal iklimlerde ya da dijital linç ve hedef göstermenin yaygın olduğu çevrimiçi ortamlarda, oto-sansürü aşan koruyucu bir işlev görmektedir. Ancak dijital ekosistemin mevcut işleyişi, anonimliği bu işlevinden sistematik biçimde uzaklaştırmaktadır.

Dijital ortamda anonimlik, bireyin kendisini tanımlamadan veya kişisel verilerini ifşa etmeden iletişim kurabilme ve kamusal tartışmalara katılabilme hakkını ifade eder. Bu hak, salt bir mahremiyet talebi değil; aynı zamanda eleştirel düşüncenin, bilgi paylaşımının ve fikir açıklamanın sürdürülebilmesi için gerekli bir özgürlük alanıdır[1274]. Ancak güncel dijital ekosistem, anonimliği fiilen daraltan yapısal bir dönüşüm içindedir. Platformlar ve hizmet sağlayıcılar, kullanıcıların her çevrimiçi hareketini kaydeden, izleyen ve profilleyen sistemler kurmakta; anonimlik çoğu zaman güvenlik tehdidi ya da sistemsel bir istisna olarak kodlanmaktadır. Hizmetlere erişimin kapsamlı veri paylaşımına bağlanması, anonimliği kullanılabilir bir hak olmaktan çıkararak ya maliyetli bir ayrıcalığa ya da dijital yurttaşlıktan dışlanma pahasına tercih edilebilen marjinal bir seçeneğe dönüştürmektedir.

Oysa anonimlik, hizmetten feragat etmeksizin kullanılabilir olmalıdır. Aksi hâlde kişiselleştirme, bireysel bir tercih olmaktan çıkmakta; hakları algoritmik profillere indirgeyen zorunlu bir yönlendirme mekanizmasına dönüşmektedir. Algoritmik sistemler, bireyi geçmiş davranış ve tercihlerine sabitleyerek onun değişme, yeniden konumlanma ve kendini dönüştürme kapasitesini sınırlandırmakta; böylece bireysel

---

[1273] ARTICLE 19, Right to Online Anonymity, s.6, https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf (2 Şubat 2026).
[1274] ARTICLE 19, s.10.

özerkliği zayıflatmaktadır. Bu bağlamda anonimlik, yalnızca gizlenme değil; bireyin kimliğini sabitlenmiş kategorilerin dışına taşıyabilme özgürlüğü olarak da değerlendirilmelidir[1275].

Dijital iletişimin yoğun biçimde izlenebilir hâle gelmesi, anonimliği giderek işlevsiz bir yanılsamaya dönüştürmektedir. Günümüzde sorun, bireyin saklayacak bir şeyinin olup olmamasından ziyade, saklamanın fiilen mümkün olup olmaması hâline gelmiştir. Wikileaks'in kurucusu Julian Assange'a göre mobil cihazlarla kurulan iletişimler askerî gizli servisler tarafından dinlendiğinden özel hayatın sınırları içerisine "askerî bir bölge" kurulmakta; bu durum dijital ortamda anonimliği büyük ölçüde çökertip illüzyona dönüşmektedir[1276]. Bu koşullar altında anonimlik, hukuki ve teknik güvencelerle desteklenmediği sürece sembolik bir özgürlük alanı olarak kalmaktadır.

Right to Online Anonymity bildirisine göre, anonimlik hakkının yalnızca normatif düzeyde tanınması yeterli değildir; bu hakkın fiilen kullanılabilmesi için şifreleme, anonim ağlar ve benzeri teknik araçların meşru ve erişilebilir olması gerekir[1277]. Dijital yurttaşlığın anlamlı biçimde var olabilmesi, bireyin devlet ya da şirket gözetiminden bağımsız olarak bilgiye ulaşabilme ve ifade üretme kapasitesine bağlıdır. Anonimliğin hizmete erişimden vazgeçilmeden kullanılamadığı bir dijital düzende, özgürlükten değil; yalnızca daha sofistike biçimde yürütülen veri madenciliğinden söz edilebilir. Kişiselleştirme adı altında sunulan her algoritmik müdahale, bireyin kendi kimliğini inşa etme özgürlüğüne yönelmiş dolaylı bir sınırlama niteliği taşımaktadır.

Anonimlik hakkı, özellikle yaptırım tehdidinin bulunduğu siyasal bağlamlarda, bireylerin düşüncelerini serbestçe ifade edebilmesi açısından hayati bir öneme sahiptir. Anonimlik, riskli ya da rahatsız edici söylemlerin artmasına yol açabilse de hangi ifadelerin sınırlandırılacağı ve denetimin hangi ölçüde uygulanacağı meselesi özünde siyasal bir tercihtir[1278]. AİHM de Delfi AS v. Estonia kararında anonimliğin internette

[1275] Irion ve Helberger, s.19.
[1276] Aust ve Ammann, s.156-159.
[1277] ARTICLE 19, s.24.
[1278] Ardıç, s.261.

düşünce ve bilgi akışını güçlendirdiğini vurgulamaktadır[1279]. Buna karşın devletlerin ve özel aktörlerin artan müdahaleleri, kişisel verilerin rıza dışı kullanımı ve anonimliği fiilen ortadan kaldıran uygulamalar dijital ifade özgürlüğü bakımından ciddi sorunlar yaratmaktadır.

Dijital ortamda anonimlik imkânı, bireylerin ve toplulukların ifade alanlarını genişletirken, fiilî muhataplık ilişkisini doğrudan bu hizmetleri sunan platform şirketlerine kaydırmaktadır[1280]. Anonimlik görünürde bireyi koruyan bir özgürlük alanı yaratırken, pratikte denetim ve kontrol yetkisini dijital alanı yöneten özel aktörlerin elinde yoğunlaştırmaktadır. Bu durum, devleti kamusal alanın asli düzenleyicisi olmaktan çıkararak aracı ve dolaylı bir konuma itmekte; klasik devlet-birey ilişkisinin doğrudanlığını zayıflatmaktadır. Böylece anonimlik hakkı, bir yandan bireysel özgürlük vaadi taşırken, diğer yandan egemenliğin platformlar lehine aşındığı ve kamusal otoritenin dolanımlı hâle geldiği yapısal bir dönüşümü görünür kılmaktadır. Bu durum, temel hakların korunmasında devletin asli muhatap olduğu yönündeki klasik kamu hukuku varsayımını işlevsizleştirmektedir.

- **Ulaşılamama Hakkı: Dinlenme Değil, Sürekli Tetikte Olmak:** Dijitalleşme, çalışma yaşamının zaman ve mekân sınırlarını görünürde esneklik adına belirsizleştirmiş; işin belirli bir yer ve saatle sınırlı olduğu klasik çerçeveyi aşındırmıştır. İnternet erişiminin olduğu her yer potansiyel işyeri, günün her saati ise olası mesai zamanı hâline gelirken[1281] bu dönüşüm çalışanlara gerçek bir özerklikten ziyade daimî ulaşılabilirlik, sürekli çevrimiçilik ve kesintisiz gözetim/denetim yüklemiştir[1282]. Özellikle uzaktan ve esnek çalışma pratiklerinin yaygınlaşmasıyla birlikte iş ve özel hayat arasındaki sınırlar

[1279] AİHM, Büyük Daire, 16/06/2015, Başvuru No:64569/09, Delfi AS v. Estonia, par. 147..
[1280] Çelik ve Aydoğan, *"Sosyal Medyada Hukuku Yerleşik Kılma Çabaları",* s.304.
[1281] Başak Ozan Özparlak, **Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme,** İstanbul: On İki Levha, 2021, s.41.
[1282] Deniz Ugan Çatalkaya, "Dijitalleşmenin Çalışma İlişkileri Üzerinde Çift Yönlü Etkisi: 'Görünürde' Özgürlükler, 'Gerçekte' Daha Sıkı Bir Bağımlılık İlişkisi Lehine Gelişmeler ve Olası Riskler", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (285-304), Ankara: Adalet Yayınevi, 2023, s.285-290.

giderek erimiş; dinlenme zamanı, fiilen her an müdahaleye açık bir tetikte olma hâline dönüşmüştür[1283].

Bu yeni çalışma rejiminde çalışan, çoğu zaman açık bir talimat olmaksızın çevrimiçi kalma zorunluluğunu içselleştirir; mesajlara ve taleplere gecikmeden yanıt verme baskısını sürekli hisseder. Böylece ulaşılamama hâli, korunması gereken bir hak olmaktan çıkarak riskli ya da sorumsuzlukla ilişkilendirilen bir davranış biçimi gibi algılanmaya başlar. Daimî çevrimiçilik, teknostres, tükenmişlik, kaygı bozuklukları ve uyku problemleri gibi çok sayıda fiziksel ve psikolojik sonuca yol açarken; algoritmik performans ölçümleri, zaman takip yazılımları ve dijital denetim araçları yönetsel gözetimi otomatikleşmiş bir disiplin mekanizmasına dönüştürmektedir. Bu bağlamda ulaşılamama hakkı, yalnızca iş disiplini veya verimlilik tartışmasının konusu değil; beden ve zihin bütünlüğünün, özel hayatın ve insan onurunun korunmasıyla doğrudan ilişkili temel bir mesele hâline gelmektedir[1284].

Ulaşılamama hakkı, çalışanın iş saatleri dışında işverenin iletişim ve erişim taleplerine kapalı olabilmesini ifade eder ve anayasal düzlemde dinlenme hakkı, özel hayatın korunması ve sağlık hakkının doğal uzantısı olarak değerlendirilmelidir. Ancak güncel çalışma kültürü, çalışanı giderek sürekli erişilebilir bir üretim unsuruna indirgemekte; özel yaşam alanına yönelik müdahaleleri olağanlaştırmaktadır. Bu durum, "İşçinin emeği bir meta değildir" ilkesine[1285] karşı, emeğin insan onurundan bağımsız bir meta gibi ele alınmasına yol açmakta; dijital çağda bu yaklaşım daha görünmez ama daha yoğun bir baskı biçimi üretmektedir. Ulaşılamama hakkının tanınması, bu nedenle yalnızca etik bir tercih değil; devletin bireyin yaşamını, sağlığını ve kişisel bütünlüğünü

[1283] Karolina Predotova ve Oscar Vargas Llave, "Workers Want to Telework but Long Working Hours, Isolation and Inadequate Equipment Must Be Tackled", **Working Conditions and Sustainable Work,** Eurofound, 6 September 2021, https://www.bollettinoadapt.it/wp-content/uploads/2021/09/Workers-want-to-telework-but-long-working-hours-isolation-and.pdf (2 Şubat 2026), s.5-7.

[1284] Ugan Çatalkaya, s.292-294.

[1285] ILO, Declaration of Philadelphia, Art. I, https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40asia/%40ro-bangkok/%40ilo-hanoi/documents/publication/wcms_818973.pdf (2 Şubat 2026).

koruma yükümlülüğünün de bir parçası olarak ele alınmalıdır[1286]. Avrupa'da bu hakkı tanımaya yönelik girişimler varken[1287] Türkiye'de ise doğrudan düzenlenmemiş olmakla birlikte işçi sağlığını koruma yükümlülükleri ve Anayasa m. 50'de düzenlenen dinlenme hakkı kapsamında tartışılabilecek bir çerçeve bulunmaktadır[1288].

Sonuç olarak ulaşılamama hakkı, yalnızca çalışanın huzur içinde dinlenebilmesini değil; zihinsel ve bedensel bütünlüğünü sürdürebilmesini mümkün kılan hayati bir güvencedir. İnsan, sürekli erişilebilir bir üretim aygıtına indirgenemez. Bu hak, aynı zamanda toplumun genel sağlık düzeyi, sosyal denge ve sürdürülebilir iş yaşamı açısından da koruyucu bir işleve sahiptir. Dijitalleşme, çalışana vaat ettiği esnekliği çoğu zaman özgürlük olarak değil, kesintisiz erişim ve denetim olarak üretmiştir. Ulaşılamama hakkı, bu yapısal baskıya karşı bireyin son savunma hattını oluşturur. Bu hak yasal güvence altına alınmadıkça, dijitalleşme bir özgürleşme süreci olmaktan ziyade, giderek derinleşen bir denetim rejimi olarak varlığını sürdürmeye devam edecektir.

- **Unutulma Hakkı: Dijital Hafızanın Tehdidiyle Yaşamak:** Özel hayata ilişkin verilerin bir bölümünü oluşturan sır; saklanmasında yarar görülen bilgilerin bireyin mahrem alanına dâhil edilerek korunmasını ifade eder[1289]. Bu tür bilgiler, kişinin kendisiyle ve çevresiyle kurduğu ilişki bakımından sınırlandırılmış bir dolaşım alanına sahiptir ve kişilik bütünlüğünün önemli bir parçasını oluşturur.

Dijital çağda bilginin üretilmesi, saklanması ve dolaşıma sokulması benzeri görülmemiş bir hız ve süreklilik kazanmıştır. Bu dönüşüm, bireyin geçmişiyle kurduğu ilişkiyi köklü biçimde değiştirmiş; unutmayı istisna, hatırlamayı ise varsayılan hâle

---

[1286] Serenay Kara, Alp Limoncuoğlu ve Zeynep Şişli, "Dijitalleşen Çalışma Hayatında İşçinin Ulaşılamama Hakkı", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde (357-368), Ankara: Adalet Yayınevi, 2023, s.360.

[1287] 2021'de Avrupa Parlamentosu, Avrupa Komisyonu'na ulaşılamama hakkına dair bir direktif hazırlaması çağrısında bulunmuş ve bir taslak metin yayımlanmıştır. 2022'de düzenlenen AB konferansında bu hakkın yasal zemine kavuşturulmasının önemi vurgulanmıştır. Kara, Limoncuoğlu ve Şişli, s.357-361.

[1288] Anayasa'nın 17., 5. ve 49. maddeleri, bireyin maddi-manevi varlığının korunması, yaşam kalitesinin yükseltilmesi ve özel hayatın geliştirilmesi yönünde devlete pozitif yükümlülükler yüklemektedir. Buna ek olarak TBK m. 417 ve 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, işverenin çalışan sağlığını koruma borcu çerçevesinde bu hakkın dolaylı olarak tanınmasını ve uygulanmasını zorunlu kılmaktadır. Kara, Limoncuoğlu ve Şişli, s.363, 365.

[1289] Rukiye Akkaya Kia, "Devlet Sırrı, Kimin Sırrı?", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.19, No.2, (2013), s.749.

getirmiştir. Dijital ortamda bir kez kayda geçen bilgi, bağlamından koparılarak sürekli yeniden dolaşıma sokulabilmekte; geçmişte yapılmış bir hata, bir paylaşım ya da bir haber, bireyin bugünkü kimliğini belirleyen kalıcı bir etikete dönüşebilmektedir. Bu koşullar altında unutulma hakkı, dijital hafızanın sınırsızlığına karşı bireyin kişilik bütünlüğünü ve yaşam anlatısını korumaya yönelik bir savunma mekanizması olarak ortaya çıkmıştır.

Unutulma hakkı, dijital ortamda bireyin geçmişine ilişkin bazı bilgilerin erişilebilirliğinin sınırlandırılmasını talep edebilmesini ifade eder[1290]. Kamusal açıdan bu hak, basit bir veri silme işleminden ibaret değildir; bireyin kendi yaşam anlatısını yeniden kurabilme, kişiliğini dönüştürebilme ve geçmişin dijital yükü altında sabitlenmeme özgürlüğüne dayanır. Dijital hafızanın mutlaklığı bireyi sürekli geçmişiyle tanımlanan bir veri nesnesine indirgerken, unutulma hakkı bireyin kendisini yeniden özne olarak konumlandırma talebini içerir[1291]. Bu yönüyle unutulma hakkı, insan onuru, kişisel verilerin korunması ve özel hayatın gizliliğiyle doğrudan bağlantılı yapısal bir haktır.

Bu hakkın tanınması, dijital geleceğin kim tarafından ve hangi ölçütlerle belirleneceğine ilişkin önemli bir kırılma noktasını da temsil eder. Arama motorları ve dijital platformlar, bilgiyi tarafsız biçimde yansıtan nötr araçlar değil; ekonomik çıkarlar doğrultusunda sıralama, görünürlük ve hafıza rejimleri kuran aktörlerdir. Dolayısıyla unutulma hakkı, yalnızca bireysel menfaatleri değil, dijital kamusal alanın nasıl şekillendirileceğini de ilgilendiren demokratik bir sorundur. Salt ekonomik fayda gerekçesi, bireyin kişilik haklarına yönelik sınırsız müdahaleleri meşrulaştıramaz; bu yaklaşım, dijital kapitalizmin tek taraflı hafıza kurma gücünü sınırlamaya yönelik daha geniş bir eğilimin parçasıdır.

Unutulma hakkı, ifade özgürlüğü ve kamunun bilgiye erişim hakkı ile gerilimli bir ilişki içerisindedir. Bu hak, geçmişte ifade edilmiş bir görüşün ya da yapılmış bir eylemin bütünüyle silinmesini değil; güncelliğini ve kamusal değerini yitirmiş bilgilerin

---

[1290] Emel Badur, "Dijital Çağda Çocuğun Unutulma Hakkı", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.299-300.

[1291] Zeynep Nur Subaşı, "İnternette Unutulma ve Silme Hakkı", Süleyman Yılmaz (Ed.), **Bilişim Hukuku Güncel Sorunlar** içinde (389-437), Ankara: Yetkin, 2020, s.393-403.

bireyin yaşamını orantısız biçimde belirlemesini engellemeyi amaçlar. Aksi hâlde birey, söylediği bir söz ya da yaptığı bir paylaşım nedeniyle bu içerikle kalıcı biçimde özdeşleştirilerek fiilen o sonuçla birlikte yaşamaya zorlanır. Bu durum, bireyin düşüncelerini açıklama cesaretini zayıflatarak ifade özgürlüğü üzerinde dolaylı bir baskı yaratır.

Unutulma hakkı, dijital ortamda bilginin kalıcı ve kolay erişilebilir hâle gelmesinin yarattığı riskler bağlamında özellikle arama motorları üzerinden somutlaşmış ve ABAD'ın 2014 yılında Google hakkında verdiği kararla hukuksal bir içerik kazanmıştır. Söz konusu karar, arama sonuçlarının kaçınılmaz ve tarafsız bir yansıma olmadığı; aksine ekonomik ve yapısal tercihlerle şekillenen bir sistem ürünü olduğu kabulüne dayanarak, arama motoru işletmecilerinin kişisel verilerin ve temel gizlilik hakkının korunmasına yönelik sorumluluğunu vurgulamıştır[1292]. Bu çerçevede salt ekonomik çıkarların, kişisel verilerin korunmasına yönelik müdahaleleri meşrulaştıramayacağı açıkça ortaya konulmuştur. Benzer şekilde California'da 2015 yılında yürürlüğe giren "Çevrimiçi Silici" yasası, reşit olmayanlara geçmişte paylaştıkları içerikleri sonradan kaldırabilme imkânı tanıyarak, bilginin sınırsız dolaşımı iddiasını sınırlamış ve dijital alanda bireyin kendi geleceği üzerinde söz sahibi olmasını güçlendiren yeni bir hukuki mücadele hattı açmıştır[1293]. Bu çerçevedeki girişimler, kişisel verilerin silinmesine ilişkin teknik düzenlemelerin ötesinde, dijital geleceğin kim tarafından belirleneceğine dair demokratik bir eşik oluşturmuştur. Bu yaklaşım, arama sonuçlarının kaçınılmaz ve tarafsız olmadığı; aksine ekonomik ve yapısal tercihlerle şekillenen bir sistem ürünü olduğu kabulüne dayanır ve platform işletmecilerinin temel hakları gözetme yükümlülüğünü vurgular.

Unutulma hakkının en kırılgan ancak en hayati kullanım alanlarından biri çocuklardır. Dijital ortamda ebeveynler veya üçüncü kişiler tarafından paylaşılan içerikler, yani "*Sharenting*" (paylaşan ebeveynlik) pratikleri, çocuğun henüz ayırt etme ve rıza gösterme kapasitesi oluşmadan kalıcı bir dijital kimlik inşa edilmesine yol

[1292] Küzeci, s.445. Kama Işık, s.75.
[1293] Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.81-83.

açmaktadır. Bu içeriklerin ilerleyen yıllarda kaldırılabilmesi, çocuğun kişilik gelişimi, özerkliği ve onurlu bir yaşam sürme hakkı bakımından özel bir önem taşır[1294]. Çocukların dijital geçmişlerinin kontrolsüz biçimde arşivlenmesi, unutulma hakkını soyut bir talepten ziyade somut bir korunma ihtiyacına dönüştürmektedir.

Uygulamada unutulma hakkı, çoğu zaman büyük dijital aktörler tarafından etkisizleştirilmekte ya da bireyler açısından erişilmesi son derece güç, bürokratik bir mücadele alanına dönüştürülmektedir. Arama motorları ve sosyal medya platformları, bireyin geçmişini silmeye değil; arşivleyerek dolaşıma sokmaya dayalı bir işleyiş mantığına sahiptir. İnsan deneyimini veri nesnesine dönüştüren dijital kapitalist yapı içerisinde unutulmak, sistem açısından bir tehdit olarak algılanmaktadır. Bu nedenle unutulma hakkı, yalnızca bireysel bir talep değil; platform merkezli hafıza rejimine karşı anayasal bir denge unsurudur[1295].

Sonuç olarak unutulma hakkı, dijital çağda bireyin veri üzerindeki tasarruf yetkisini ve kişilik gelişimini koruyan temel bir güvencedir. Orwell, bilişim teknolojisindeki gelişmelerin gelecekte devlete kişinin özel alanı üzerinde tam bir kontrol yetkisi verip bireysel özgürlüklerin yok edildiği totaliter bir egemenliği mümkün kılacağından bahsetmişti[1296]. Büyük veri çağında gözetim, bireyin yaşamı ve kimliği dijital ortama taşındıkça daha derin ve kalıcı bir nitelik kazanmış; dijital kişilik hakları kaçınılmaz hâle gelmiştir. Dijital ortamda kişisel veriler üzerinde özerklik sağlanmadıkça ne bireysel özgürlükten ne de demokratik bir toplum düzeninden söz edilebilir[1297]. Unutulma hakkı, bireyin yalnızca gözetlenen ve profillenen bir veri kaynağına indirgenmesine karşı, özgür bir özne olarak varlığını sürdürebilmesinin ön koşullarından biridir. Bu hakkın etkili biçimde korunması, yalnızca özel hayatı değil; kamusal eleştiriyi, toplumsal çoğulculuğu ve demokratik kamusal alanın sağlığını da güvence altına alır.

[1294] Badur, s.299-300.

[1295] Jürgen Kühling, "Germany: The Right to Be Forgotten", Franz Werro (Ed.), **The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia** içinde (125-140), Springer, 2020, s.127.

[1296] Uygun, s.597.

[1297] Aust ve Ammann, s.215-216.

d. Dijitalleşmenin Gölgesinde İfade Özgürlüğü: Denetim, Manipülasyon ve Hak İhlalleri

Immanuel Kant'a göre insanı doğadaki diğer varlıklardan ayıran ve saygıya layık kılan temel özellik, ahlaki seçimler yapabilme kapasitesidir. Özgür iradesi sayesinde insan, doğa yasalarının belirleyiciliğinin ötesine geçerek kendi koyduğu ahlaki yasaya göre hareket edebilir; iyiyi kötüden ayırt edip kendisi için bağlayıcı normlar belirleyebilir[1298]. Bu açıdan ifade özgürlüğü, insanın düşünen ve vicdan sahibi bir varlık olmasının doğal sonucu olarak, düşünce ve kanaatlerini açıklayabilmesini güvence altına alan temel bir haktır. Bu özgürlük, yalnız bireysel kendini gerçekleştirme bakımından değil; gerçeğin ortaya çıkarılması, eleştirel tartışmanın mümkün olması ve demokratik rejimlerin işleyebilmesi açısından da kurucu bir işleve sahiptir[1299]. AİHM'nin yerleşik içtihadında da ifade özgürlüğü, demokratik toplumun en önemli temellerinden biri ve bireyin kişiliğini geliştirmesinin vazgeçilmez şartı olarak kabul edilmektedir[1300].

Bu normatif çerçeve, ifade özgürlüğünün yalnız bireysel bir hak değil, kamusal bir işlev gördüğünü de ortaya koyar. İfade özgürlüğüne dayalı özgürlükler, siyasal katılımın düşünsel altyapısını oluşturur ve kamuoyunun oluşumunda merkezi rol oynar[1301]. Kamuoyu, siyasal karar alma süreçlerini etkileyen ve iktidarı sınırlayan temel bir güç olmakla birlikte, belirleyiciliği çoğunluk olmaktan ziyade ikna edici ve etkileyici olmasından kaynaklanır. Bu etki kapasitesi ise bireyler ve toplumsal gruplar arasında eşit dağılmaz[1302]. Çoğulcu demokrasilerde kamuoyu kuramsal olarak özgür kabul edilse de pratikte bilginin doğruluğu, dolaşım kanalları ve söylemi üreten aktörler tarafından sınırlandırılır. Bu nedenle serbest kamuoyu, ancak doğru bilginin serbestçe dolaşıma

---

[1298] Uygun, s.510.
[1299] Uygun, s.619-620.
[1300] AİHM, Büyük Daire, 27/06/2017, Başvuru No.17224/11, Medžlis Islamske Zajednice Brčko and Others v. Bosnia and Herzegovina, https://hudoc.echr.coe.int/ par.75; AİHM, 13/02/2025, Başvuru No.56310/15, P. v. Polonya, https://hudoc.echr.coe.int/ par.70; AİHM, Büyük Daire, 15/12/2025, Başvuru No.16915/21, Danileţ v. Romanya, https://hudoc.echr.coe.int/ par.142; AİHM, Büyük Daire, 23/04/2015, Başvuru No.29369/10, Morice v. Fransa, https://hudoc.echr.coe.int/ par.124; AİHM, Büyük Daire, 15/10/2015, Başvuru No.27510/08, Perinçek v. İsviçre, https://hudoc.echr.coe.int/ par.196-197.
[1301] Akad, Dinçkol ve Bulut, s.302.
[1302] Bihterin Vural Dinçkol, "Çoğulcu Demokrasilerde Siyasal Partiler ve Kanaatler", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi,** Vol.1, No.2, (2002), s.24-25.

girdiği ve ifade özgürlüğünün etkin biçimde güvence altına alındığı bir hukuk düzeninde anlam kazanır[1303]. Dijitalleşme bu tabloyu niteliksel olarak dönüştürmüştür.

• **Platform İktidarında İfade Özgürlüğü Zemininin Aşınması:** Dijitalleşme, kamuoyunun oluşumunu hızlandırmış ve görünürlüğünü artırmıştır; ancak siyasal etkileme gücünü eşitlememiştir. Ekonomik güç, eğitim düzeyi, siyasal bilinç ve dijital erişim gibi yapısal faktörler, dijital kamuoyunda da belirli aktörlerin daha baskın hâle gelmesine yol açmaktadır. İnternet ve özellikle sosyal medya, ifade özgürlüğünü erişim ve hız bakımından genişleterek bilgi üretimini ve kamusal tartışmayı güçlendirmiştir; ancak aynı ortamlar, güvence, öngörülebilirlik ve eşit kamusallık bakımından ifade özgürlüğünü kırılganlaştırmıştır. Yalan haber, nefret söylemi ve görünmez sansür pratikleri aracılığıyla ortaya çıkan bu yeni ihlal alanları, dijital çağda ifade özgürlüğünden fiilen yararlanmayı karmaşık ve eşitsiz bir sürece dönüştürmektedir[1304]. Böylece kamusal tartışma görünürde genişlerken, fiilen dar, asimetrik ve hiyerarşik bir zeminde şekillenmektedir.

Bu gerilim, kamuoyu teorisi açısından yeni değildir; ancak dijital ortamda derinleşmiştir. Bu dönüşümü teorik düzeyde açıklayan önemli çerçevelerden biri, Walter Lippmann'ın "hayalet kamu" eleştirisidir[1305]. Lippmann'a göre kamuoyu ve seçmen iradesi, demokraside varsayıldığı kadar rasyonel, bilgili ve yönlendirici değildir; bireyler karmaşık siyasal süreçleri kavrayacak zaman ve bilgiye çoğu kez sahip değildir. Kamuoyunun işlevi, karar üretmekten ziyade, yönetenler başarısız olduğunda tepki vermek ve saf tutmakla sınırlıdır[1306]. Lippmann, toplumsal eylem ve düşüncenin kolektif değil, bireysel aktörler tarafından gerçekleştirildiğini; toplumun ise bu bireyler arasındaki

---

[1303] Bihterin Dinçkol, "Yönetilenlerin 'Öz' Yönetimi-Kamuoyu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,** Cilt.5, No.10, Güz 2006/2, (2006), s.60.

[1304] Ardıç, s.251.

[1305] Lippmann'ın fikirleri dijital çağ öncesinde analog düzen için ileri sürülmüş olmakla beraber dijital çağ için de oldukça uygundur. Lippmann'a göre modern toplumlarda bilinçli, rasyonel ve bilgili bir kamu fikri bir yanılsamadır; halk karmaşık siyasal süreçleri kavrayacak ve tutarlı bir irade oluşturacak imkânlara sahip değildir. Bu nedenle halk iradesi çoğu zaman teorik bir inanç, kamu ise fiilî etkisi olmayan bir hayalettir. Lippmann, s.13.

[1306] Lippmann, s.46-47.

ilişkilerden ibaret olduğunu vurgular[1307]. Bu nedenle daha fazla görünürlük ve daha sık görüş bildirme, bireyleri bilinçli siyasal özneler hâline getirmek yerine, onları daha yönlendirilebilir ve edilgen kılabilmektedir[1308]. Günümüzde dijital platformlar görünürde katılımı artırsa da algoritmik yönlendirme ve dezenformasyon, çoğu zaman bilinçli bir kamuoyu yerine yönlendirilebilir kitleler üretmektedir. Sosyal medya tepkileri, dijital dilekçeler ve anlık anketler, gerçek siyasal katılım değil; egemenliğin meşruiyetini görünürlük üzerinden yeniden üretilmesine hizmet eden meşruiyet perdeleridir. Bu nedenle dijital teknolojiler, halk egemenliğini derinleştirmekten çok, "dijital hayalet kamu" üzerinden modern egemenliğin dijital yüzünü meşrulaştıran yeni bir yönetim tekniği yaratmıştır.

Dijital alan, yalnızca manipülasyon ve gözetim rejimleriyle özdeşleştirilemez; aynı zamanda kamusal alan oluşturma ve muhalefet aracı olma potansiyeline de sahiptir[1309]. Ancak Çin örneğinde görüldüğü üzere, bireysel ve dağınık eleştiriler belirli ölçüde tolere edilirken, kolektif eylem çağrıları sistematik biçimde bastırılmaktadır. Bu durum, internetin hem kamuoyunu izleme ve yönlendirme aracı hem de siyasal iktidar açısından sürekli denetlenmesi gereken bir risk alanı olarak kurgulandığını göstermektedir[1310]. Veri kontrolü ve teknik altyapının siyasal iktidarla bütünleşmesi hâlinde, bu direnç alanları son derece kırılganlaşmaktadır[1311].

Bu dönüşüm, dijital kamusal alanın yapısında da kendini göstermektedir. Dijital kamusal alan, kamusal denetimin dışına taşarak platform iktidarı altında yeniden kurulmaktadır. İçeriğin görünürlüğü ve dolaşımı, kamusal ölçütlerden ziyade ticari hedefler, siyasal baskılar ve risk yönetimi mantığıyla işleyen algoritmalar tarafından

---

[1307] "*Eyleyen, bireylerdir; toplum değil. Düşünen, bireylerdir; ortak akıl değil. Resim yapan, ressamlardır; çağın sanatsal ruhu değil. Savaşan ve öldürülen, askerlerdir; ulus değil. İhracat yapan, tüccarlardır; ülke değil. Bir toplumu oluşturan, bunların birbirleriyle olan ilişkileridir"*. Lippmann, s.106.

[1308] Lippmann, s.26-29.

[1309] Kezban Karagöz, "Yeni Medya Çağında Dönüşen Toplumsal Hareketler ve Dijital Aktivizm Hareketleri", **İletişim ve Diplomasi,** No.1, (2013), s.147-149). Benzer biçimde, X gibi platformlarda açılan etiketler aracılığıyla futbol kulüplerinin, belediyelerin ve çeşitli kurumların kamuoyundan gelen talepler doğrultusunda kararlar alması, dijital alanın ademi merkeziyetçi ve demokratikleştirici potansiyeline işaret eder.

[1310] Creemers, *"Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century",* s.87.

[1311] Schneider, *China's Digital Nationalism,* s.224.

belirlenmektedir. Filipinler'de Facebook-Duterte ilişkisi[1312] bağlamında ortaya çıkan sahte hesap ağları, koordineli kampanyalar ve algoritmik önceliklendirme pratikleri, eleştirel içeriğin bastırılmasının yalnızca doğrudan sansürle değil, dağıtımın siyasallaştırılması yoluyla da gerçekleşebildiğini göstermektedir[1313]. Bu durum, ifade özgürlüğünü yalnız konuşabilme değil, görünür olabilme hakkı bakımından da kırılganlaştırmaktadır.

Kamusal alan tartışmaları bu nedenle yeniden düşünülmektedir. Küresel bilgi dolaşımını hızlandıran dijital ortam, kamusal alan kuramının da dönüşmesine yol açmıştır. Jürgen Habermas'a göre özgür iletişim ve serbest bilgi akışı, iktidarın denetimini zayıflatan kamusal alanın temel koşuludur[1314]. Dijitalleşme, bu varsayımı güçlendirmiş; ancak pratikte ortaya çıkan platformlar, bu iyimser beklentiyi sınırlamıştır. Günlük dijital pratikler çoğu zaman demokratik müzakere yerine tüketime ve yüzeysel etkileşime[1315] yönelmekte; görünürde katılımcı olan yeni medya, fiilen şirket egemenliğinin belirlediği dar ve denetimli bir kamusal alan üretmektedir[1316]. Bilgi görünürde erişilebilir olsa da gündem belirleme gücü "bilgi bekçiliği" (gatekeeping) yapan platform temelli dar bir dijital ruhban sınıfı[1317] ve uzman elitinin elinde yoğunlaşmaktadır[1318].

[1312] Filipinler'de Facebook'un Duterte yönetimiyle kurduğu ilişki, bu sürecin somut bir örneğini oluşturur: Sahte hesaplar, koordineli kampanyalar ve algoritmik önceliklendirme yoluyla eleştirel içerikler bastırılmış; platform, siyasal sadakat karşılığında piyasa hâkimiyetini güçlendirmiştir. Lauren Etter, "How Duterte Turned Facebook Into a Weapon: With Help From Facebook", *Bloomberg Businessweek* (7 Dec. 2017), https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook (2 Şubat 2026).

[1313] Bu örnek, dijital teknolojilerin demokratik alanı genişletmek yerine otoriter pratiklerin uzantısına dönüşebileceğini göstermektedir. Kamusal denetimden yoksun bir dijital alan, ifade özgürlüğünü güvence altına almak yerine onu manipülasyona açık bir propaganda zeminine indirger. Lawrence Lessig, **Code: And Other Laws of Cyberspace, Version 2.0**, New York: Basic Books, 2006, s.290.

[1314] Serkan Bulut, s.63; Bkz: Jürgen Habermas, The Structural Transformation of the Public Sphere (1962).

[1315] Keza kullanıcılarının internette arkadaşları ve aileleriyle bağlantı kurmak, selfie paylaşmak, ucuz tüketim ürünleri satın almak ve ne yediklerini paylaşmakla daha sık ilgilenmektedirler. Schneider, *China's Digital Nationalism,* s.12.

[1316] Yalçın, s.106-109.

[1317] İnternet, bilgiye erişimi kitleselleştirerek matbaanın yarattığı devrimi katlayan güçlü bir demokratikleşme vaadi sunsa da arka planda bilgi tekelinin kontrolünü elinde tutan ve matbaa öncesi dönemi andıran bir bağımlılık ilişkisi sunan yeni bir dijital ruhban sınıfı ortaya çıkarmıştır. Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.239.

[1318] Judith Moeller ve Diğerleri, "Shrinking core? Exploring the differential agenda setting power of traditional and personalized news media", **Digital Policy, Regulation and Governance,** Vol.18, No.6, (2016), s.26-30.

Bu dönüşümle birlikte ifade özgürlüğü, artık yalnızca devletin doğrudan müdahalelerine değil; platform mimarisi, veri ekonomisi ve algoritmik dağıtım rejimi üzerinden işleyen özel iktidar biçimlerine de açık hâle gelmiştir. Sosyal medya platformlarının demokratik süreçleri yönlendirme kapasitesi, milli iradenin oluşumunda geleneksel siyasal partilerin önüne geçen yeni aracılar üretmiş; ifade özgürlüğü ile kişisel haklar arasında denge kuran özel düzenleyici çerçeveleri zorunlu kılmıştır[1319]. Sorun, bireylerin daha fazla konuşabilmesinden ziyade, ifadelerin hangi koşullarda özgür, çoğulcu ve hakkaniyetli biçimde dolaşıma girebildiği meselesine dönüşmüştür.

Big Tech'in içerik kaldırma, görünürlük azaltma veya algoritmik önceliklendirme yoluyla gerçekleştirdiği müdahaleler, açık yasaklar içermese dahi fiilî bir sansür etkisi yaratabilmektedir. Karar alma süreçlerinin şeffaf olmaması ve algoritmik sistemlerin "kara kutu" niteliği, bu müdahalelerin ifade özgürlüğü üzerindeki etkilerini öngörmeyi ve denetlemeyi güçleştirmektedir[1320]. Ayrıca sınır aşan ölçekte veri kontrolüne sahip bu platformlar, hukuka aykırı içeriklerin yayılımı açısından da ciddi riskler barındırmaktadır[1321]. BM İnsan Hakları Yüksek Komiserliği'nin de vurguladığı üzere dijital teknolojiler, gözetim, sansür, taciz ve algoritmik önyargı üretme kapasitesiyle temel haklar bakımından riskli bir araç seti hâline gelmiştir[1322].

Buna rağmen dijital alan bütünüyle tek yönlü bir tahakküm alanı değildir. Dijital platformlar kullanıcıları pasif izleyiciler olmaktan çıkararak içerik üreticilerine dönüştürmüş; siyasal görünürlük ve eylemlilik açısından yeni imkânlar da yaratmıştır[1323]. Çevrimiçi topluluklar ve bağımsız kullanıcılar, dijital örgütlenme yoluyla yerleşik siyasal anlatılara meydan okuyabilmekte ve kolektif eylemler geliştirebilmektedir[1324].

[1319] Eren, s.565.

[1320] All Tech Is Human, s.19; Floridi, s.370. Zararsız gibi görünen kısa videolar dahi siyasi veya toplumsal mesajlar içerebilmekte ve yapay zekâ kararları doğrudan ya da dolaylı olarak insan hakları ihlallerine zemin hazırlayabilmektedir.

[1321] Işık, s.19.

[1322] Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği Ofisi, About Digital Space and Human Rights, https://www.ohchr.org/en/topic/digital-space-and-human-rights (2 Şubat 2026).

[1323] Ethan Zuckerman, "New Media, New Civics?", **Policy and Internet,** Cilt.6, No.2, (June 2014), s. 156; Kjerstin Thorson ve Chris Wells, "Curated flows: a framework for mapping media exposure in the digital age", **Communication Theory,** Vol.26, No.3, (2015), s.313-314.

[1324] Schneider, *China's Digital Nationalism,* s.171-172.

Dijitalleşme çevrimiçi siyasal katılım bakımından dijital aktivizm gibi yeni imkânlar sunmakla birlikte, bu imkânlar demokratik meşruiyet açısından ciddi tartışmaları da beraberinde getirmektedir. Katılımın artması, tek başına demokratik bir kazanım anlamına gelmemekte; hukuken düzenlenmemiş, sorumluluğu belirsiz ve yaptırım mekanizmaları zayıf bir dijital alan, hakların genişlemesinden ziyade rastlantısallaşmasına yol açabilmektedir. Örneğin uzaktan elektronik oy kullanımı, erişimi kolaylaştırmasına rağmen kimlik doğrulama, anonimlik, mahremiyet ve denetlenebilirlik gibi temel gereklilikler nedeniyle güvenlik ve gizli oy ilkesi bakımından önemli riskler barındırmaktadır. Bu nedenle e-oy uygulamaları, modern demokrasilerde temkinle yaklaşılması gereken araçlar olarak değerlendirilmektedir[1325]. Bu ikili yapı, dijital kamusal alanın normatif değerinin teknolojiden değil; kuralların, aktörlerin, güç ilişkilerinin ve hesap verebilirlik mekanizmalarının nasıl kurulduğundan kaynaklandığını göstermektedir[1326]. Bilgi bolluğu, doğrudan daha bilgili yurttaşlar yaratmamakta; yeni siyasal imkanların ortaya çıkışı da kendiliğinden demokratik sonuçlar üretmemektedir[1327].

Başlangıçta devletin ifade özgürlüğü karşısındaki yükümlülüğü, bu hakka müdahale etmemekle sınırlı görülmüş; ancak zamanla bunun yeterli olmadığı ve ifade özgürlüğünün etkin biçimde kullanılabilmesi için devletin pozitif yükümlülükler üstlenmesi gerektiği kabul edilmiştir. Bu çerçevede devletin, yasal, kurumsal ve idari önlemler yoluyla ifade özgürlüğünü koruyacak bir ortam tesis etme sorumluluğu bulunmaktadır[1328]. Avrupa İnsan Hakları Mahkemesi de içtihadında, devletin yalnızca müdahaleden kaçınmakla yetinemeyeceğini; ifade özgürlüğünü koruyacak hukuki ve kurumsal çerçeveyi oluşturmakla da yükümlü olduğunu vurgulamaktadır[1329]. Bu yükümlülük, özellikle medya alanında tekelleşmenin çoğulculuğu tehdit ettiği

---

[1325] Bihterin Vural Dinçkol ve Alper Işık, "Katılımcı Demokrasi ve Online Karar Alma Bağlamında E-Oy ve Estonya Örneği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt.25, Sayı.2, (2019), s.721.
[1326] Yalçın, s.110-111.
[1327] Bart A. Barendregt ve Florian A. Schneider, "Digital Activism in Asia: Good, Bad, and Banal Politics Online", **Asiascape: Digital Asia,** Vol.7, No.1-2, s.5-8.
[1328] Uygun, s.622-623.
[1329] AİHM, 5/5/2011, Başvuru No. 33014/05, Editorial Board of Pravoye Delo and Shtekel v. Ukrayna, https://hudoc.echr.coe.int/ par.62-65.

durumlarda, farklı görüşlerin kamusal alanda serbestçe yer almasının güvence altına alınmasını gerektirir.

Dijitalleşme sürecinde ifade özgürlüğünü kırılganlaştıran temel unsurlardan biri, çevrimiçi izleme ve profilleme pratikleridir. İfade özgürlüğü, AİHS m.10 ve AB Temel Haklar Şartı m.11 kapsamında, yalnızca düşünce ve bilgilerin yayılmasını değil, aynı zamanda bunlara erişme ve alma hakkını da kapsar. Ancak çevrimiçi davranışların sürekli izlenmesi ve kalıcı biçimde kaydedilmesi, bireylerde izlenme bilinci yaratarak bilgi arayışını dolaylı biçimde sınırlandırmakta ve oto-sansürü teşvik etmektedir. Bu nedenle gözetim, yalnızca mahremiyetle ilgili bir sorun değil; ifade özgürlüğünün demokratik işlevini aşındıran yapısal bir müdahale niteliği taşımaktadır[1330]. Bu bağlamda dijital çağda ifade özgürlüğüne yönelik en belirgin tehditlerden biri, AİHM içtihadında "caydırıcı etki" (chilling effect) olarak adlandırılan olgudur. Caydırıcı etki, bireylerin doğrudan bir yaptırıma maruz kalmasalar dahi, gözetim, izleme veya yaptırım ihtimalinin yarattığı belirsizlik nedeniyle düşünce ve kanaatlerini açıklamaktan kaçınmalarını ifade eder[1331]. Sürekli gözetim algısı, hukuken yasaklanmamış ifadelerin dahi fiilen bastırılmasına yol açarak kamusal tartışma alanını daraltmaktadır[1332]. Dijital gözetim teknolojileri, yaygın veri toplama pratikleri ve belirsiz denetim mekanizmaları bu etkiyi derinleştirerek, bireylerin düşünce ve kanaatlerini serbestçe açıklama cesaretini zayıflatmakta ve dijital kamusal alanın ifade özgürlüğüne dayalı zeminini aşındırmaktadır.

Toplantı ve gösteri yürüyüşü özgürlüğü, ifade özgürlüğünün kolektif bir görünümü olarak bireylerin görüş ve taleplerini kamusal alana taşımasına imkân tanır[1333]. Siyasal özgürlüklerin görece gelişmiş olduğu ülkelerde dijital araçlar, hukuki güvencelerle birleştiğinde ifade özgürlüğünü ve siyasal katılımı genişletebilmektedir. Buna karşılık özgürlüklerin sınırlı ve kurumsal denetimin zayıf olduğu rejimlerde aynı dijital altyapı, gözetimi yoğunlaştıran ve oto-sansürü derinleştiren bir denetim mekânına

---

[1330] Avrupa Birliği Adalet Divanı, hükümetler veya şirketler tarafından yapılan gözetlemenin, gizlilik ve veri koruma temel haklarına ciddi bir müdahale teşkil ettiğini ve ifade özgürlüğü üzerinde potansiyel olarak soğutucu bir etkisi olduğunu kabul etmiştir. Oostveen ve Irion, s.7.

[1331] AİHM, İkinci Daire, 25/6/2013, Başvuru No. 48135/06, Youth Initiative for Human Rights v. Serbia,, https://hudoc.echr.coe.int/ par.24-26.

[1332] AİHM, İkinci Daire, 8/7/2008, Başvuru No. 33629/06, Vajnai v. Hungary, https://hudoc.echr.coe.int/ par.53-54.

[1333] Uygun, s.691.

dönüşmektedir. Siber güvenlik başlığı altında getirilen ve pratikte sansür işlevi görebilen düzenlemeler, ifade ve düşünce özgürlüğü ile çevrimiçi toplanma hakkını kırılganlaştırmakta; dijital kamusal alanın demokratik kapasitesini güvenlik gerekçesiyle daraltabilmektedir. Ülkeler arasında örülen dijital duvarlar açık interneti aşındırırken, etik dışı yapay zekâ uygulamaları otoriter yönetimlerin gözetim kapasitesini genişleten bir teknik kaldıraca dönüşebilmektedir[1334]. Bu nedenle dijitalleşmenin özgürleştirici ya da baskıcı etkisi, teknik kapasiteden ziyade bireysel iradeyi güvence altına alan siyasal ve hukuki koşullara bağlıdır.

Bireyin ifadesi, dikkat ekonomisinin girdisine indirgenmekte; anlam üretimi yerini hız, tepki ve görünürlük mantığına bırakmaktadır. Bu süreç, eleştirel kamusallığın bilişsel ve zamansal zeminini aşındırarak ifade özgürlüğünü öznel anlam kurma alanı olmaktan uzaklaştırmaktadır[1335]. Bu noktada ifade özgürlüğüne yönelik devlet müdahalesinin biçimi değişmelidir. Dijital çağda ifade özgürlüğü, artık yalnızca devletin doğrudan sansürüne karşı korunmayı değil; platform mimarisi, algoritmik dağıtım ve ekonomik iktidar tarafından dolaylı biçimde şekillendirilen ifade alanına karşı da güvenceler geliştirilmesini zorunlu kılmaktadır.

Sonuç olarak internet yalnızca bir iletişim aracı değil, hareketlerin örgütsel altyapısı hâline gelmiştir. Zapatista deneyimi ve küreselleşme karşıtı hareketlerde görüldüğü gibi, internet tabanlı ağlar farklı aktörleri eşgüdüm içinde birleştirmiş; e-posta listeleri, forumlar ve çevrimiçi tartışmalar, süreklilik taşıyan bir dijital agora oluşturmuştur[1336]. Dijital kamusal alan aynı anda hem manipülasyon hem de direniş imkânlarını barındıran tenakuz içeren bir yapı arz etmektedir[1337]. Bununla birlikte, dijital çağda ifade özgürlüğü yalnızca yasaklama tehdidiyle değil; görünmez kılma, yönlendirme ve caydırma mekanizmalarıyla kuşatılmıştır. Platform mimarisi, veri ekonomisi ve algoritmik dağıtım rejimi, ifade alanını yapısal biçimde dönüştürmektedir.

[1334] Karagöz, s.143.
[1335] Çalgan, s.8-11.
[1336] Castells, *Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü,* s.113, 201, 212-213.
[1337] Karagöz, s.142.

Bu zemin, bir sonraki aşamada ele alınacak olan algoritmik manipülasyon ve mikrohedefleme rejimlerinin üzerinde yükseldiği yapısal arka planı oluşturmaktadır.

• **Manipülasyon Rejimi: Algoritmik Yönlendirme, Dezenformasyon ve Mikrohedefleme:** Dijital çağda ifade özgürlüğüne yönelen tehdit, yalnızca doğrudan yasaklama veya sansür biçiminde ortaya çıkmamaktadır. Daha sofistike ve yapısal olan tehdit, bireyin kanaat oluşturma sürecine nüfuz eden algoritmik yönlendirme, veri temelli ikna ve davranışsal manipülasyon teknikleri üzerinden işlemektedir. Dijital kamusal alanda ifade özgürlüğü, yalnızca söylenenlerin bastırılmasıyla değil; hangi bilgilerin görünür kılındığı, hangilerinin geri plana itildiği ve bireyin hangi içeriklerle karşılaşacağının önceden belirlenmesi yoluyla aşındırılmaktadır.

21. yüzyılda dijital medya, giderek bir manipülasyon mimarisine dönüşmüştür. Başlangıçta bilgi sağlayan platformlar zamanla sosyal yapının kendisi hâline gelmiş; örneğin Google ve Facebook gibi platformlar yalnızca düşünceleri ölçen araçlar olmaktan çıkıp düşünce ve ilişkileri biçimlendiren aktörlere dönüşmüştür[1338]. Sosyal medya görünürde çoğulcu bir paylaşım alanı sunsa da algoritmalar kullanıcıları filtre balonlarına hapseder; ilgi ve dikkat metalaştırılarak ekonomik ve siyasal yönlendirme üretilir[1339]. Bu süreçte iletişim teknikleri, bireyin biyometrik ve davranışsal verileri üzerinden işleyen görünmez bir kontrol mekanizmasına dönüşür. Manipülasyon, zaaflar üzerinden ve fark edilmeden işler; anlık haz döngüleri duygusal bütünlüğü ve toplumsal sorumluluğu zayıflatır. Böylece sömürü, iş zamanının ötesine taşarak sürekli hâle gelir[1340].

Modern demokratik düzende siyasal haklar, yurttaşların yöneticileri belirleme ve kamusal kararları denetleme yetkisine dayanır; bu haklar yurttaşlığın özü olup demokrasinin vazgeçilmez koşuludur[1341]. Ancak algoritmik kişiselleştirme pratikleri, kullanıcıları geçmiş tercihleri ve etkileşimleri etrafında kuşatarak yankı odaları

[1338] Dyson, s.310.

[1339] Timothy W. Luke, "Digital Citizenship", Phillip Kalantzis-Cope ve Karim Gherab-Martín (Ed.), **Emerging Digital Spaces in Contemporary Society: Properties of Technology,** içinde (83-96) London: Palgrave & Macmillan, 2010, s.86.

[1340] Çalgan, s.54-56.

[1341] Vural Dinçkol, *"Yurttaşlık ve Seçilme Hakkı Üzerine Bir Değerlendirme",* s.101.

üretmekte; fikir çeşitliliğini zayıflatarak kamusal tartışmayı ortak bir zemin yerine parçalı ve kapalı bilgi evrenlerine bölmektedir[1342]. Böylece rasyonel ve eleştirel müzakere idealinin yerini; hız, dikkat ve duygusal tepki ekonomisinin belirlediği bir dolaşım rejimi almaktadır. Kamusal önemi haiz meseleler görünmez kılınırken, suni gündemler ve duygusal tetikleyiciler toplumsal hafızayı işgal etmekte; kamusal tartışma derinlikten yoksun ve yönlendirilebilir hâle gelmektedir.

Bu yapısal dönüşüm, dijital araçların manipülasyon ve dezenformasyon amacıyla kullanımını kolaylaştırmaktadır. Ekonomik güç, eğitim düzeyi ve dijital okuryazarlık gibi faktörler dijital kamuoyunda da belirleyici olmakta; böylece dijitalleşme eşitsizlikleri ortadan kaldırmak yerine çoğu zaman yeniden üretmektedir. Kodu yazanların ve platformu yönetenlerin, siyasal tartışmayı dolaylı biçimde belirlediği asimetrik bir güç ilişkisi ortaya çıkmaktadır[1343].

Dijital ortamda manipülasyon artık münferit yanlış bilgi üretimi değil; bot ağları, sahte hesaplar, mikrohedefleme ve algoritmik yönlendirme yoluyla yürütülen organize bilgi operasyonlarıdır. Bu yapı, kamusal hakikat zeminini sistematik biçimde aşındıran bir dezenformasyon rejimi yaratmakta ve hukuki müdahale mekanizmalarını işlevsizleştirecek hızda çalışmaktadır[1344]. Yalan haber (fake news) bilgi ekosistemi; kasıtlı zarar üretmeye yönelik dezenformasyon (dis-information), niyetsizce yayılan yanlış-bilgi (mis-information) ve doğru içeriğin zarar amacıyla kullanıldığı kötü-bilgi (mal-information) biçimlerinde kurumsallaşmıştır[1345]. Bu ortamda ideolojik topluluklar ve siyasi aktörler, propaganda ve dijital kampanyalar yoluyla kolektif eylemi yeniden biçimlendirmekte; devletler dahi influencerlar ve veri odaklı iletişim stratejileriyle hakikat rekabetine katılmaktadır[1346]. Özellikle deepfake[1347] ve sentetik medya

---

[1342] Oostveen ve Irion, s.11.

[1343] Küzeci, s.124-125.

[1344] Kuzu, s.152-153.

[1345] Claire Wardle ve Hossein Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making". **Council of Europe Report,** 2017, s.20.

[1346] Schneider, *"Reality Decoupling: Rumours, Disinformation, and Studying the Politics of Truth in Digital Asia",* s.183-184.

[1347] Sentetik içerikler, yapay zekâ ve diğer dijital teknolojilerle, özellikle yanıltma amacıyla dijital içeriklerin değiştirilerek yeniden üretilmesiyle ortaya çıkan ürünlerdir. Bunlardan biri olan deepfake, bir kişinin yüzünü veya sesini başka bir kişininkiyle değiştirerek gerçekmiş gibi gösteren video ya da ses kayıtlarıdır. Gerçekte yapılmamış bir

teknolojileri, gerçek ile kurgu arasındaki sınırı bulanıklaştırarak; kişilik haklarını, mahremiyeti, fikri mülkiyeti, seçim güvenliğini ve demokratik meşruiyeti tehdit eden çok katmanlı bir manipülasyon aracı hâline gelmiştir[1348]. Deepfake ile bireylerin ya da tanınmış kişilerin yüzleri ve sesleri eğlence, dolandırıcılık[1349], ticari[1350], müstehcen[1351] ve benzeri amaçlarla amaçlı kullanılabilir; tehdit, şantaj, cinsel sömürü gibi suçlara zemin hazırlayabilir [1352]. Bu içerikler, bireylerin yüz ve seslerinin rızasız kullanımı üzerinden hem kişisel verilerin korunması[1353] hem telif hukuku bakımından ihlaller doğurmakta; aynı zamanda gerçeğin doğrulanabilirliğini aşındırarak kamusal güveni zedelemektedir[1354]. Bu teknoloji, sadece kişisel mahremiyeti ve hakları değil; aynı zamanda kamu düzeni, seçim güvenliği ve ifade özgürlüğü gibi anayasal değerleri de tehdit eder. Bu nedenle, deepfake kapsamında ifade özgürlüğü ve sanat üretme hakkı gibi temel hakların sınırları sorgulanmalıdır[1355]. Viral dolaşımın hızı, doğruluk denetimini etkisizleştirirken, dijital arşivin kalıcılığı geçmiş içeriklerin sürekli yeniden dolaşıma

---

şeyi yapılmış gibi göstermek amacıyla manipüle edilen içeriklerdir. **Cambridge Dictionary,** "Deepfake", https://dictionary.cambridge.org/dictionary/english/deepfake; **Merriam-Webster Dictionary,** "Deepfake", https://www.merriam-webster.com/dictionary/deepfake (2 Şubat 2026). İngilizcedeki 'derin öğrenme' (deep learning) ve 'sahte' (fake) kelimelerinden türetilmiştir. Türkçede derin kurgu ya da derin sahte gibi karşılıkları önerilmiş olsa da yaygın bir çevirisi yoktur. Kişisel Verileri Koruma Kurumu, Deepfake Bilgi Notu, 2024, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/015794c4-061b-4560-a0b2-e372ee536642.pdf (2 Şubat 2026), s.1.

[1348] Ecem Kirkit, "Deepfake Teknolojisi Karşısında Kişinin Kişilik Hakkının ve Kişisel Verilerinin Korunması", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.296; Mustafa Evren Berk, "Dijital Çağın Yeni Teknolojisi 'Deepfake'", **OPUS Uluslararası Toplum Araştırmaları Dergisi,** Cilt.11, Sayı.18, (2020), s.1508-1511; European Parliamentary Research Service, *Tackling deepfakes in European policy*, s. 1.

[1349] ABD'de telefonda duyduğu sesin oğlunun sesiyle tamamen aynı olduğunu iddia eden yaşlı bir adam, yapay zekâ ile oğlunun sesinin telefonda taklit edilmesi sonucu oğlunun hapisten kefaletle çıkmak için gerekli olduğu söylenen 25.000 doları panikle dolandırıcılara kaptırdı. "Oğlunun sesini taklit eden yapay zeka ile 25 bin dolar dolandırdılar", *Milliyet,* https://www.milliyet.com.tr/dunya/oglunun-sesini-taklit-eden-yapay-zeka-ile-25-bin-dolar-dolandirdilar-7213403 (2 Şubat 2026).

[1350] "Scarlett Johansson, sesini kullanan yapay zeka şirketine yasal işlem başlattı", *indyturk.com,* https://www.indyturk.com/node/671376/yaşam/scarlett-johansson-sesini-kullanan-yapay-zeka-şirketine-yasal-işlem-başlattı (2 Şubat 2026).

[1351] "Ünlü ekran yüzünü deepfake ile porno filminde oynattılar", *Sözcü,* https://www.sozcu.com.tr/unlu-ekran-yuzunu-deepfake-ile-porno-filminde-oynattilar-p42725 (2 Şubat 2026).

[1352] Kişisel Verileri Koruma Kurumu, s.2; All Tech Is Human, s.21 vd.

[1353] Bir yüz tanıma teknolojisi olan deepfake'in üretimi için geniş kapsamlı kişisel verilere ihtiyaç olduğundan, deepfake ürünlerinde kişilik hakları ve kişisel veriler tehdit altındadır. Yüz ve ses hem kişilik hakkı hem de biyometrik veri olarak hukuken koruma altındadır. Kişinin rızası olmaksızın bu değerlerin kullanılması, kişilik haklarına ve kişisel verilere yönelik bir saldırıdır. Kirkit, s.296.

[1354] Özyiğit ve Baydan, s.568-574.

[1355] Pınar Bacaksız, "Deepfake (Yapay Video Montaj) Teknolojisinin Ortaya Çıkardığı Ceza Hukuku Sorunları", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.60;

sokulması yoluyla demokratik tartışmayı bastıran bir cezalandırma mekanizmasına dönüşmektedir[1356].

Manipülasyon rejiminin demokratik etkileri, bilgi edinme özgürlüğü bağlamında daha da görünür hâle gelmektedir. Bilgi edinme özgürlüğü, düşünce ve ifade özgürlüğünün ön koşulu olup bireyin kamusal meseleler hakkında kanaat oluşturabilmesinin temel dayanağını oluşturur[1357]. Başta Birleşmiş Milletler Genel Kurulu'nun 1946 yılındaki Bildirisi[1358] olmak üzere uluslararası insan hakları belgelerinde ve anayasalarda güvence altına alınan bu özgürlük, yalnızca bilginin varlığına değil; doğru, çoğulcu ve erişilebilir olmasına bağlıdır[1359]. Ancak algoritmik filtreleme ve kişiselleştirilmiş içerik akışları, bireyin maruz kaldığı bilgi evrenini daraltarak düşüncenin oluştuğu ham maddeyi manipüle etmekte; böylece ifade özgürlüğünün maddi zeminini zayıflatmaktadır. Bu noktada devletin yükümlülüğü, yalnızca bilgiye erişimi ihlâl etmemekle sınırlı olmayıp, dijital platformlar kaynaklı yapısal kısıtlamalara karşı koruyucu önlemler almayı da kapsamaktadır[1360].

Bu bağlamda dijital çağın en tartışmalı uygulamalarından biri siyasal mikrohedeflemedir. Mikrohedefleme, bireylerin çevrimiçi davranışları ve psikolojik profilleri üzerinden özelleştirilmiş siyasal mesajlar üretilmesine dayanmakta[1361] seçmenlerin yalnızca bilgilendirilmesini değil, duygularının ve eğilimlerinin bilinçdışı düzeyde yönlendirilmesini hedeflemektedir[1362]. Bu yöntem, yurttaşı kamusal tartışmanın öznesi olmaktan çıkararak ikna edilmiş bir manipülasyon nesnesine dönüştürmekte[1363]

[1356] Han, s.28.

[1357] Ayhan Döner, "Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi,** Cilt.26, Sayı.1, (Haziran 2022), s.55.

[1358] BM, Resolution 59(I), 14 December 1946, https://digitallibrary.un.org/record/209774?v=pdf#files (2 Şubat 2026).

[1359] Döner, s.31-33; Sabahattin Nal, "Karşılaştırmalı Hukukta Enformasyon Hakkı", **Prof. Dr. Necip Kocayusufpaşaoğlu İçin Armağan,** Ankara: Seçkin Yayınları, (2004), s.709-710.

[1360] Nal, s.721-722.

[1361] All Tech Is Human, s.17.

[1362] Tarleton Gillespie, "The Relevance of Algorithms", Tarleton Gillespie, Pablo J. Boczkowski ve Kirsten A. Foot (Ed.) **Media Technologies: Essays on Communication, Materiality, and Society** içinde (167-193), Massachusetts: The MIT Press, 2014, s. 188-191; Andı, s.2.

[1363] Frederik J. Zuiderveen Borgesius ve Diğerleri, "Online Political Microtargeting: Promises and Threats for Democracy". **Utrecht Law Review,** Cilt.14, No1., (2018), s.82.

bireysel özerkliği, ifade özgürlüğünü ve düşünce oluşturma süreçlerini zayıflatmakta[1364] demokratik tartışmanın eşitlik ve şeffaflık ilkelerini zedelemektedir. Farklı seçmen gruplarına birbirinden kopuk ve çelişkili siyasal vaatlerin sunulabilmesi; ortak kamusal aklı parçalamakta[1365] ve siyasal rekabeti görünmez biçimde bozabilmektedir.

Mikrohedeflemenin en çarpıcı örneklerinden biri, Cambridge Analytica skandalında[1366] görüldüğü üzere, seçmenlerin daha karar verme aşamasına gelmeden hedeflenmesi ve siyasal tercihlerin veri temelli operasyonlarla şekillendirilmesidir[1367]. Sürekli içerik bombardımanının ve duygusal tetiklemenin; rasyonel düşünmeyi aşındırarak bireyleri hızlı tepki veren, edilgen ve yönlendirilebilir kitlelere dönüştürdüğü bu enfokrasi düzeninde bağlamından koparılmış bir tweet veya sahte bir haber, gerçeklerden daha etkilidir. Bu koşullarda demokrasi, kamusal müzakere ve özerk karar alma kapasitesini yitirerek biçimsel bir oy verme pratiğine indirgenme riskiyle karşı karşıya kalmaktadır[1368].

Bu noktada çevrimiçi siyasal mikro hedeflemenin ifade özgürlüğü kapsamında korunup korunamayacağı sorusu önem kazanmaktadır. AİHM; reklamlar, seçim broşürleri ve politik afişler gibi klasik siyasal iletişim araçlarındaki siyasal ifadelerin ilke olarak AİHS m. 10 kapsamında yüksek düzeyde koruma gördüğünü kabul etmekle birlikte demokratik toplumda eşit siyasal rekabetin ve seçmen iradesinin serbest

---

[1364] Oostveen ve Irion, s.10-11.

[1365] Zuiderveen Borgesius ve Diğerleri, s.86-87.

[1366] Facebook-Cambridge Analytica skandalı, 2018'de yaklaşık 90 milyon kullanıcının verisinin izinsiz kullanılmasıyla ortaya çıkmış; şirket bu verileri psikolojik ve siyasi profiller çıkararak seçim kampanyalarını etkilemek için kullanmıştır. 2016 ABD seçimleri, Brexit ve 2015 Birleşik Krallık seçimleri gibi süreçlerde veri analizine dayalı hedefli reklamlarla seçmen davranışının manipüle edildiği iddia edilmiştir. Zuiderveen Borgesius ve Diğerleri, s.84; "Cambridge Analytica nedir? Cambridge Analytica skandalı nasıl oldu?", *Sözcü*, https://www.sozcu.com.tr/cambridge-analytica-nedir-cambridge-analytica-skandali-nasil-oldu-wp7671806 (2 Şubat 2026); "Were There Any Links Between Cambridge Analytica, Russia and Brexit?", *The Spectator,* https://www.spectator.co.uk/article/were-there-any-links-between-cambridge-analytica-russia-and-brexit/ (2 Şubat 2026). "Cambridge Analytica, Leave.EU, UKIP, Brexit and Facebook", *Politico Europe,* https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/ (2 Şubat 2026); "Cambridge Analytica: UK watchdog fines Facebook £500,000", *BBC News*, https://www.bbc.com/news/uk-politics-54457407 (2 Şubat 2026).

[1367] 2008 ve 2012 Obama kampanyalarında, seçmenlerin davranışsal verileri analiz edilerek her birey için "ikna skoru" hesaplanmış; oy tercihi henüz oluşmadan tahmin edilip mesajlar kişiselleştirilmiştir. Google'ın öngörü modelleriyle güçlenen bu veri temelli strateji, kamuoyundan gizli yürütülen ve seçmen davranışını önceden öngören bir seçim mühendisliği pratiğine dönüşmüştür. Zuboff, *Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş,* s.157-158.

[1368] Han, s.18-24.

oluşumunun da korunması gerektiğini vurgulamaktadır[1369]. Bu nedenle mesele, mikro hedeflemenin bütünüyle yasaklanmasından ziyade; şeffaflık, denetlenebilirlik ve veri koruma ilkeleriyle sınırlandırılmasıdır. AİHS Ek 1 No'lu Protokol'ün 3. maddesinde güvence altına alınan serbest seçim ilkesi, seçmenlerin manipülasyondan arındırılmış bir bilgi ortamında siyasal kanaat oluşturabilmesini zorunlu kılmaktadır. Siyasal aktörlerin çevrimiçi reklam harcamalarının şeffaflaştırılması ve bu harcamaların erişilebilir bir veri tabanında kayıt altına alınması, demokratik dengeyi korumaya yönelik meşru araçlar olarak değerlendirilebilir. Bu kapsamda dijital reklam harcamalarının kamuoyuna açıklanması ve veri koruma otoritelerinin siyasi partilerin kişisel veri işleme faaliyetlerini etkin biçimde denetlemesi, demokratik meşruiyetin güçlendirilmesi açısından kritik önemdedir[1370].

Güncel sorun, yalnızca gözetimin yarattığı soğutucu etki değil, kişisel verilere dayalı ikna ve yönlendirme teknikleridir. Bireyler, özel aktörler ve siyasal organizasyonlar tarafından, satın alma davranışından oy tercihine kadar çeşitli eylemleri etkilemek üzere tasarlanan özelleştirilmiş mesajlarla çevrelenmektedir. Bu müdahale, görünüşte iletişim formunda olsa da belirli bir eşiği aştığında artık kanaat özgürlüğünün serbest oluşumunu değil, kanaatin üretimini hedefleyen bir manipülasyon tekniğine dönüşür. Bu noktada, düşünce-vicdan özgürlüğü (AİHS m. 9; AB Temel Haklar Şartı m. 10) dijital çağda yeniden merkezîleşen bir hak kategorisi hâline gelir: Kişisel verilerin hacmi arttıkça, bu verilerden kişinin inançlarına, eğilimlerine ve zayıflıklarına dair yeni anlamlar türetmek kolaylaşmakta; böylece düşünceye nüfuz ve düşünceyi etkileme kapasitesi büyümektedir. Bu gelişme, gizlilik ve veri korumanın etkinleştirici işlevini ifade özgürlüğünün ötesine taşıyarak, düşünce özgürlüğü bakımından da yeni bir sınır alanı açmaktadır. Veri temelli yönlendirme pratikleri, ayrıca ayrımcılık riskini artırır. Irk, din, etnik köken, cinsiyet gibi temellerle ayrımcılık AİHS m.14 ve AB Temel Haklar Şartı m. 21 ile yasaklanmıştır; ancak veri işleme pratikleri, kasıtlı olsun olmasın, belirli grupları

[1369] TV Vest v. Norveç kararında, siyasal reklam yasaklarının seçimlerde eşit bir oyun alanı sağlama amacını kabul etmekle birlikte, ifade özgürlüğüne yapılan müdahalelerin orantılı olması gerektiğini vurgulamıştır. AİHM, 11/12/2008, Başvuru No.21132/05, TV Vest AS & Rogaland Pensjonistparti/Norveç, [Turkish Translation] legal summary by the COE Human Rights Trust Fund, https://hudoc.echr.coe.int/

[1370] Zuiderveen Borgesius ve Diğerleri, s.94-95.

dışlayan veya dezavantajlılaştıran sonuçlar üretebilir. Bu nedenle veri koruma hukuku, yalnızca gizlilik değil, aynı zamanda ayrımcılığın azaltılması bakımından da kurumsal bir fren işlevi görür. GDPR 9. Maddesinde özel nitelikli kişisel verilere daha yüksek koruma tanınması (ırksal/etnik köken, siyasi görüş, dini/felsefi inanç, sendika üyeliği, sağlık ve cinsel yaşama ilişkin veriler) bu normatif mantığın ürünüdür[1371].

Sonuç olarak dijital kamusal alanda manipülasyon rejimi, ifade özgürlüğünü yalnızca içerik düzeyinde değil; kanaatin oluştuğu bilişsel, duygusal ve enformasyonel altyapı düzeyinde aşındırmaktadır. Algoritmik yönlendirme, dezenformasyon ve mikro hedefleme pratikleri; demokratik eşitliği ve kamusal aklı sistematik biçimde zayıflatmakta; yurttaşı özgürce düşünen bir özne olmaktan uzaklaştırmaktadır[1372]. Bu yapısal sorun, bir sonraki aşamada ele alınacak olan hukuki çerçeve ve demokratik denge arayışının neden zorunlu hâle geldiğini açık biçimde ortaya koymaktadır.

- **Hukuki Çerçeve ve Demokratik Denge:** Dijital çağda ifade özgürlüğünün korunması, artık yalnızca açık sansür ve doğrudan yasaklamalara karşı savunma geliştirilmesi anlamına gelmemektedir. Algoritmik yönlendirme, görünürlük kontrolü, veri temelli ikna ve platform mimarisi üzerinden işleyen dolaylı müdahaleler, ifade özgürlüğünü kanaatin özgürce oluştuğu yapısal zeminde aşındırmaktadır. Bu nedenle mesele, bireylerin ne söyleyebildiğinden ziyade, hangi koşullarda özgür, çoğulcu ve manipülasyondan arındırılmış bir kamusal tartışma içinde kanaat oluşturabildiği sorusuna dönüşmüştür. Dijital alanda ifade özgürlüğünün korunması, düzenleme boşluğunun özel iktidar alanları yaratmasını önlemek ile belirsiz ve aşırı güvenlikçi müdahalelerin caydırıcı etki üretmesini engellemek arasında hassas bir anayasal denge kurulmasını zorunlu kılmaktadır.

Bu denge arayışı, klasik siyasal düşüncede de güçlü biçimde temellendirilmiştir. Baruch Spinoza'ya göre, salt güvenliği sağlamaya indirgenen bir iktidar anlayışı meşru değildir; hakka uygun devlet, bireyin düşünme ve ifade etme özgürlüğünü güvence altına alan devlettir. Vicdan ve düşünce özgürlüğü devredilemez niteliktedir ve siyasal iktidarın

[1371] Oostveen ve Irion, s.7.
[1372] Karagöz, s.132-134.

tasarruf alanı dışında kalır[1373]. Benzer biçimde John Locke'un toplum sözleşmesi kuramında bireyler, doğal haklarından vazgeçmek için değil, bu hakları daha güçlü biçimde korumak amacıyla siyasal topluma katılırlar[1374]. Bu kuramsal çerçeve, dijital çağda ifade özgürlüğüne yönelik müdahalelerin de istisnai, öngörülebilir ve sıkı ölçütlere bağlı olması gerektiğini ortaya koymaktadır.

Bu noktada ceza hukuku araçlarının dijital ifade alanına müdahalede kullanımı özel bir sorun alanı oluşturmaktadır. Siber güvenlik veya kamu düzeni gerekçesiyle getirilen belirsiz ve geniş kapsamlı ceza normları, ifade ve düşünce özgürlüğü üzerinde ağır bir caydırıcı etki yaratabilmektedir[1375]. Örneğin Türkiye'de 2022 yılında yürürlüğe giren "halkı yanıltıcı bilgiyi alenen yayma" düzenlemesi örneğinde görüldüğü üzere, belirsiz kavramlara dayanan ceza normları; kanunilik ve öngörülebilirlik ilkeleriyle bağdaşmamaktadır. Ceza hukukunun ultima ratio niteliği göz ardı edildiğinde, ifade özgürlüğü bir güvence alanı olmaktan çıkarak oto-sansürü derinleştiren bir disiplin mekanizmasına dönüşmektedir[1376].

İfade özgürlüğü ile kamu düzeni arasındaki gerilim, yalnızca siyasal söylem alanında değil, gündelik bilgi akışını düzenleyen dijital hizmetlerde de somutlaşmaktadır. Navigasyon uygulamalarında trafik denetim noktalarının paylaşımı örneğinde olduğu gibi, kullanıcı deneyimini geliştiren anlık bilgi akışı, kamu güvenliği bakımından yeni riskler doğurabilmektedir. Fransa'da belirli denetim türlerine ilişkin konum bilgilerinin sınırlı biçimde yasaklanması ve bu düzenlemenin Conseil d'État tarafından AB hukuku bakımından ABAD'a taşınması, dijital alandaki sınırlamaların genel ve toptan yasaklar yerine hedefli, ölçülü ve denetlenebilir müdahalelerle kurulması gerektiğini

---

[1373] Kriegel, s.84-85; Uygun, s.225.
[1374] Akad, Dinçkol ve Bulut, s.134.
[1375] Örneğin, Vietnam'ın 2019'da çıkardığı siber güvenlik yasası, internet şirketlerinin devlete karşı çıkan içeriği kaldırmasını ve kullanıcıların hükümet karşıtı bilgileri çevrimiçi olarak yaymasını yasaklamaktadır. Viet Tan Alert, Hanoi's Cybersecurity Law: Implications for Human Rights and Civil Society, 2018, https://www.viettan.org/en/wp-content/uploads/sites/2/2018/12/Viet-Tan-Alert-Hanois-Cybersecurity-Law.pdf (2 Şubat 2026).
[1376] Tülay Kitapçıoğlu Yüksel, "Halkı Yanıltıcı Bilgiyi Alenen Yayma Suçu Hakkında Değerlendirme", **Uluslararası Dijital Çağda Hukuk Sempozyumu,** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022, s.74-75.

göstermektedir. Bu yaklaşım, ifade özgürlüğü ile kamu güvenliği arasında kategorik değil, bağlamsal bir denge kurulmasının anayasal önemini ortaya koyar[1377].

Dijital alanın bütünüyle düzenleme dışı bırakılması da özgürlük üretmemektedir. Dezenformasyon, algoritmik manipülasyon ve veri temelli yönlendirme pratikleri, devletin pozitif yükümlülüklerini genişletmiştir. Dijital kamusal alanda ifade özgürlüğünün korunması, artık yalnızca müdahaleden kaçınmayı değil; şeffaflık, hesap verebilirlik ve etkili başvuru yollarını güvence altına alan düzenleyici çerçevelerin oluşturulmasını gerektirmektedir[1378]. Devletin rolü, platform mimarilerini denetlemekten kaçınmak değil; bu alanlarda temel hakları koruyacak asgari normları tesis etmektir[1379].

Özellikle gözetim ve veri işleme faaliyetleri, ifade özgürlüğü bakımından yapısal bir caydırıcı etki üretmektedir. Sürekli izleme, kapsamlı profilleme ve belirsiz denetim mekanizmaları, bireylerde izlenme bilinci yaratarak hukuken yasaklanmamış ifadelerin dahi fiilen bastırılmasına yol açmaktadır. Açık sansürden ziyade öz-sansür üreten daha sofistike bir baskı biçimi ortaya çıkmakta; bu durum, kamusal tartışmanın canlılığını, çoğulculuğunu ve doğruyu söyleme cesaretini (*parrhesia)* zayıflatmaktadır. Bu nedenle dijital kamusal alanın demokratik potansiyeli; gözetimin açık yasal dayanaklara bağlanmasına, veri minimizasyonu ilkesinin uygulanmasına ve etkili yargısal denetim mekanizmalarının işletilmesine bağlıdır.

[1377] Fransa Danıştay'ının verdiği bir kararda bu konu tartışılmıştır. Dava konusunu ilgilendiren Fransa'da Karayolu Trafik Kanunu'nun L.130-11. maddesi uyarınca, alkol ve uyuşturucu denetimleri ile bazı adli polis operasyonlarının konumlarının dijital platformlarda paylaşılması, belirli süre ve mesafe için yasaklanmıştır. Bu hüküm, sürücülerin denetimlerden kaçınmasını engelleyerek trafik güvenliğini korumayı amaçlayan geçici ve hedefe yönelik bir tedbirdir. Söz konusu düzenleme genel bilgi dolaşımını değil, denetimlerin etkisizleşmesine yol açabilecek spesifik paylaşımları hedef almaktadır. Fransa, kanunun geçici ve bölgesel sınırlama içerdiğini belirterek kamu düzeninin korunması istisnasına dayanmıştır. Dava, trafik denetim bilgilerine ilişkin dijital paylaşımların yasaklanması, bilgi akışının serbestliği ile kamu düzeninin korunması arasında kırılgan bir dengeyi yansıtmaktadır. Bkz: Conseil d'État, Décision n° 453763, 6 mars 2024, ECLI: FR:CECHR:2024:453763, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-03-06/453763 (2 Şubat 2026).

[1378] İnternette bomba yapımı gibi şiddet üretme kapasitesi taşıyan bilgiler kamu güvenliği açısından tehdit oluştururken telif hakkı ihlalleri yaratıcı emeğin sürdürülebilirliğini zayıflatır. Bu tablo, online ifade özgürlüğünün mutlak olmadığını; zarar ilkesi, orantılılık ve kamu yararı çerçevesinde sınırlanabileceğini daha görünür kılar. Sunstein, s.142; Avrupa Konseyi, *İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü,* s.5.

[1379] Ardıç, s.253.

Sonuç olarak dijital çağda ifade özgürlüğü, ne sahipsiz bırakılabilecek bir serbestlik alanı ne de güvenlik gerekçesiyle sınırsız biçimde daraltılabilecek bir hak alanıdır. Kanunilik, meşru amaç, gereklilik ve orantılılık ilkeleri temelinde kurulacak şeffaf ve hesap verebilir bir hukuki çerçeve, dijital egemenlik ile özgürlük arasında anayasal denge tesis edilmesinin ön koşuludur. Aksi hâlde dijital kamusal alan, ifade özgürlüğünün güçlendiği değil; manipülasyonun olağanlaştığı bir zemine dönüşecektir.

e. Dijital Mekânda Kişilik Haklarının Kırılganlaşması

Dijital çağda internet; bireyin yaşam tarzını, toplumsal ilişkilerini ve kamusal görünürlüğünü belirleyen asli bir altyapıya dönüşmüştür. Bu dönüşüm, yalnızca bireysel pratikleri değil, devletlerin egemenlik ve hak koruma kapasitesini de doğrudan etkilemektedir. Nitekim Estonya'nın 2000 yılında internet erişimini temel bir insan hakkı olarak tanıması, dijital alanın artık ikincil bir iletişim mecrası değil, hakların kullanımı bakımından kurucu bir zemin hâline geldiğini göstermektedir. Ancak bu normatif tanımaya rağmen, internetin özellikle sosyal medya platformları aracılığıyla hızlandırıcı, çoğaltıcı ve kalıcı bir etkiyle işlemesi, kişilik haklarını dijital çağın en kırılgan hak kategorilerinden biri hâline getirmiştir[1380].

Kişilik hakları; bireyin maddi ve manevi varlığını, onurunu, saygınlığını, özel hayatını ve kimliğini koruyan temel bir hak bütününü ifade eder. Anayasal düzlemde kişiliğe bağlı hakların dokunulmaz, devredilmez ve vazgeçilmez olduğu kabul edilmektedir. Dijital ortamda bu haklara yönelik ihlaller, yalnızca daha sık görülmekle kalmamakta; aynı zamanda daha hızlı yayılmakta, daha uzun süre etkisini sürdürmekte ve çok daha geniş bir etki alanı yaratmaktadır. İnternet ve sosyal medya, kişilik hakkına yönelik saldırıların etkisini katlayan bir çarpan işlevi görmektedir. Yazılı, görsel veya işitsel içerikler aracılığıyla bireyin itibarı zedelenebilmekte; özel hayatına ilişkin bilgiler rızası dışında dolaşıma sokulabilmekte; kişinin görüntüsü, sesi veya kişisel verileri izinsiz biçimde paylaşılabilmektedir[1381]. Dijital ortamda yayımlanan bir içerik, zamansal ve

[1380] Muhammed Sabır Fırat, "Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu", Hacettepe **Hukuk Fakültesi Dergisi,** Cilt.5, No.2, (2015), s.101.
[1381] Fırat, 109, 110.

mekânsal sınırları aşarak kalıcı bir iz bırakmakta; bu durum ihlali tekil bir olay olmaktan çıkarıp süreklilik arz eden bir hak zedelenmesine dönüştürmektedir.

Bu bağlamda siber zorbalık, dijital mekânda kişilik haklarını en ağır biçimde tehdit eden ihlal türlerinden biri olarak öne çıkmaktadır. Kasıtlı ve tekrarlanan saldırılar, içeriklerin kalıcılığı ve hızla çoğalabilmesi nedeniyle etkisini katlanarak artırmaktadır. Dijital iletişim araçlarının gündelik hayatın merkezine yerleşmesi, özellikle çocuklar ve gençler bakımından özel hayatın gizliliği, şeref ve haysiyet üzerinde ciddi riskler doğurmaktadır. Bu nedenle dijital mekânda kişilik haklarının korunması, ihlallerin gecikmeksizin durdurulmasını ve platformların pasif aracılar olmaktan çıkarak etkin sorumluluk üstlenmesini zorunlu kılmaktadır[1382].

Dijital yayıncılığın yapısal özellikleri, bu kırılganlığı daha da derinleştirmektedir. İnternet yayınları, geleneksel basılı medyadan farklı olarak düşük maliyetli, anlık ve sürekli erişilebilir niteliktedir. Bu durum ifade ve iletişim özgürlüğünü genişletirken, kişilik haklarının korunmasına ilişkin hukuki mekanizmaların hız ve etki bakımından yetersiz kalması riskini artırmaktadır. Kişilik hakkına yönelik saldırıların kaynağı çoğu zaman anonimdir; saldırıyı gerçekleştiren kişiler, platform mimarisi sayesinde kimliklerini gizleyebilmektedir. Bu nedenle dijital ortamda kişilik haklarının korunması, yalnızca maddi hukuk normlarına değil; aynı zamanda hızlı, etkili ve erişilebilir usul güvencelerine de bağlı hâle gelmiştir[1383].

Ulusal hukuk düzenleri bu sorun karşısında çeşitli koruma araçları geliştirmiştir. Örneğin TMK m. 24 kapsamında kişilik hakkına hukuka aykırı saldırı hâlinde kişinin yargısal koruma talep edilebilmektedir[1384]. İhlalin etkili biçimde sona erdirilmesi adına

---

[1382] Çakır, s.241.

[1383] Kemal Gözler, "Kişilik Haklarını İhlal Eden İnternet Yayınlarının Kaldırılması Usulü ve İfade Hürriyeti-5651 Sayılı Kanunun 9'uncu Maddesinin İfade Hürriyeti Açısından Değerlendirilmesi", **Rona Aybay'a Armağan,** İstanbul: Legal, c.I, (2014), s.1060.

[1384] Kişilik haklarına yönelik her türlü saldırı, mağdurun rızası, daha üstün bir özel veya kamusal yarar veya kanunun verdiği yetkinin kullanılması gibi haklı kılınmadıkça hukuka aykırıdır. TMK 25. madde kişilik haklarının korunması amacıyla açılabilecek davaları düzenlemektedir. Davacı, hâkimden saldırı tehlikesinin önlenmesini, devam eden saldırının sona erdirilmesini veya sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini talep edebilir. Ayrıca davacı, düzeltmenin veya kararın üçüncü kişilere bildirilmesi veya yayımlanması talebinde de bulunabilir.

içerik sağlayıcısına, yer sağlayıcıya veya doğrudan sulh ceza hâkimliğine başvuru yoluyla erişimin engellenmesi gibi hızlı müdahale araçlarını içeren düzenlemelerin ihdası oldukça önemlidir. Bununla birlikte dijital içeriğin sınır aşan dolaşımı ve platformların küresel yapısı, bu araçların çoğu zaman parçalı, geçici ve reaktif kalmasına yol açmaktadır. Müdahaleler ihlali durdurmakta yetersiz kalabildiği gibi, ihlalin etkisini tümüyle ortadan kaldırmakta da güçlük yaşamaktadır.

Öğretide, kişilik haklarının korunmasında sosyal ağ hizmet sağlayıcılarının daha etkin bir rol üstlenmesi gerektiği yönünde güçlü bir eğilim bulunmaktadır. Zorbalık ve hak ihlali içeren içeriklerin hızla kaldırılması, ihlalde bulunan kullanıcıların engellenmesi ve adli makamlarla etkin iş birliği mekanizmalarının kurulması bu çerçevede önem taşımaktadır. Anonimliğin kötüye kullanımını önlemeye yönelik kimlik doğrulama ve kayıt yükümlülükleri tartışılırken; çocuklar bakımından cezalandırıcı yaklaşımlar yerine dijital farkındalık ve medya okuryazarlığının geliştirilmesi daha uygun bir koruma yöntemi olarak öne çıkmaktadır[1385].

Dijital mekânda ebeveynlerin çocuklarına ilişkin sosyal medya paylaşımları da kişilik hakları bakımından ayrı bir sorun alanı oluşturmaktadır. Çocuğun üstün yararını korumakla yükümlü olan velinin, çocuğun rızası bulunmaksızın yaptığı paylaşımlar, çocuğun özel hayatı ve kişilik hakları üzerinde kalıcı etkiler yaratabilmektedir. Çocuğun üstün menfaatini korumakla yükümlü olan velinin bu ihlali, veli açısından TMK m. 23 vd. uyarınca sorumluluk doğurabileceği gibi, TMK m. 346 vd. çerçevesinde çocuğun korunmasına yönelik tedbirlerin alınmasını da gerektirebilir. Her ne kadar ebeveyn paylaşımlarının tamamı KVKK kapsamında veri işleme olarak nitelendirilemese de çocuk adına dijital kimlik oluşturulması ve bu kapsamda paylaşılan verilerin platformlarca depolanması hâlinde KVKK hükümleri devreye girecektir[1386].

Kişilik haklarının dijital ortamda korunması, ulusal düzenlemelerle sınırlı kalamayacak ölçüde uluslararası bir boyut kazanmıştır. Birleşmiş Milletler, Avrupa

---

[1385] Çakır, s.247.

[1386] Fatma Zeynep Altıner Yolcu, "Çocuğun Sosyal Medyada Ebeveynleri Tarafından Gerçekleştirilen Kişilik Hakkı İhlallerine Karşı Korunması", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde (269-302), İstanbul: Adalet, 2021, s.298.

Birliği, OECD ve benzeri uluslararası kuruluşlar, bilişim suçları ve kişilik haklarına yönelik ihlallerle mücadele amacıyla çeşitli normatif çerçeveler geliştirmiştir[1387]. Özellikle BM İnternet Yönetimi Forumu'nun insan hakları odaklı internet anlayışı, dijital alanın yalnızca teknik değil, aynı zamanda normatif bir kamusal alan olarak ele alınması gerektiğini vurgular. İnternetin evrenselliği, eşit erişim, ifade özgürlüğü, özel hayatın gizliliği, kişisel verilerin korunması, şeffaflık, aktif katılım ve hesap verebilirlik ilkeleri; dijital mimarinin insan haklarıyla uyumlu biçimde tasarlanması gerektiğini ortaya koymaktadır[1388]. Bu çerçevede hem kamu otoritelerinin hem de özel sektör aktörlerinin, dijital ortamda insan haklarına saygı gösterme yükümlülüğü bulunduğu kabul edilmektedir[1389].

Bununla birlikte dijital çağın temel açmazı burada belirginleşmektedir. İnsan hakları evrensel nitelik taşımasına rağmen, uygulanmaları hâlen büyük ölçüde devlet merkezli ve coğrafi olarak parçalıdır. Oysa dijital platformlar, ulusal sınırları aşan ve klasik yargı yetkilerini zorlayan bir etki üretmektedir. Bu durum, kişilik haklarının korunmasında yapısal bir boşluk yaratmaktadır. İnternetin erken dönemlerinde hâkim olan özgürlükçü beklentiler, çevrimiçi alanın hukuki ve kurumsal düzenlemelerinin ihmal edilmesine yol açmış; bugün karşılaşılan yaygın ve sistematik kişilik hakkı ihlalleri bu ihmalin sonucu olarak ortaya çıkmıştır[1390].

f. Veri Temelli Davranışsal Müdahaleler Karşısında Kişinin Maddi ve Manevi Varlığını Geliştirme Hakkının Aşınması

Dijital çağda kişinin maddi ve manevi varlığını geliştirme hakkı, yalnızca bedensel bütünlüğün korunmasını değil; zihinsel kapasitenin, özgür iradenin, eleştirel düşünme yetisinin ve entelektüel derinliğin sürdürülebilir biçimde geliştirilmesini de kapsayan bütüncül bir anayasal değer olarak karşımıza çıkmaktadır. Bu hak, bireyin kendi

---

[1387] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku,** İstanbul: Seçkin Yayınları, 2014, s.185.
[1388] Birleşmiş Milletler Internet Governance Forum, The Charter of Human Rights and Principles for the Internet, 2014, http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet_Turkish_final.pdf (2 Şubat 2026).
[1389] Fırat, 106.
[1390] Irion, *"Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows",* s.235.

yaşamını anlamlandırabilmesi, yönlendirebilmesi ve özgürce inşa edebilmesi için zorunlu olan bilişsel ve iradi koşulları güvence altına alır. Ne var ki dijitalleşmenin hâkim biçimi, bu hakkı destekleyen bir araç olmaktan ziyade, onu yapısal olarak aşındıran bir etki üretmektedir. Özellikle veri temelli kişiselleştirme, profilleme ve algoritmik filtreleme pratikleri, bireyin düşünsel ufkunu daraltarak maddi ve manevi gelişimin ön koşulu olan çoğul karşılaşmaları sistematik biçimde sınırlandırmaktadır.

Dijital ortamda çerezler, arama geçmişleri ve kullanıcı davranışları üzerinden oluşturulan ayrıntılı profiller, bireye tercih özgürlüğü görüntüsü altında esasen yalnızca mevcut ilgi alanları, tüketim alışkanlıkları ve siyasal eğilimleriyle uyumlu içeriklerin sunulmasına yol açmaktadır. İlk bakışta zaman kazandıran ve kullanım konforu sağlayan bu yapı, uzun vadede bireyin farklı düşüncelerle temasını, rastlantısal öğrenme imkânlarını ve eleştirel muhakeme kapasitesini ortadan kaldırmaktadır. Böylece dijital ortam, bireyin dünyayı keşfettiği bir kamusal alan olmaktan çıkarak, kendi kanaatlerinin sürekli yeniden üretildiği kapalı bir yankı mekânına dönüşmektedir. Bu kapalı yapı, ortak tartışma zeminini zayıflatmakta; toplumsal ve siyasal kutuplaşmayı derinleştirerek demokratik kamusallığın maddi koşullarını aşındırmaktadır[1391].

Bu durum, dijital kamusal alanda yankı odaları ve dijital kabileleşme olarak adlandırılan daha geniş bir yapısal soruna işaret etmektedir. Sosyal platformlarda benzer düşünenlerin bir araya gelmesi, ötekinin varlığını ve ihtiyaçlarını dikkate alan siyasal aklı zayıflatmakta; hoşgörü, empati ve müzakere kapasitesini aşındırmaktadır. Dijital enformasyon rejiminin demokrasi açısından taşıdığı temel risk, yalnızca bireylerin profillenmesi değil; kamusal aklın parçalanması ve siyasal tartışmanın içerikten yoksun, anlık tepkilere dayalı bir etkileşim düzeyine indirgenmesidir[1392]. Bu yapı, bireyin manevi gelişimi için zorunlu olan karşıt görüşlerle yüzleşme, düşünsel gerilim yaşama ve kanaatini sorgulama deneyimini ortadan kaldırmaktadır.

Bilgi dolaşımının ekonomik ve siyasal çıkarlar tarafından yönlendirilmesi, doğru ve eşit bilgiye erişimi zedelemektedir. Oysa özgür kamuoyu, dürüst bilginin serbestçe

[1391] Küzeci, s.117.
[1392] Aydeniz, s.39.

dolaşıma girdiği ve yönetime ilişkin verilerin aleniyet ilkesi çerçevesinde herkesçe erişilebilir olduğu bir ortamda oluşur[1393]. Dijitalleşme bu ideali bir yandan genişletmiş; bilgiye erişimi hızlandırmış ve yaygınlaştırmıştır. Öte yandan algoritmik sıralama, görünürlük kontrolü ve ticari öncelikler, bilginin kamusal değerine değil, etkileşim potansiyeline göre öne çıkarılmasına yol açmıştır. Bu durum, özgür kamuoyu için yeni imkânlar yaratırken, aynı anda manipülasyon ve dezenformasyon riskini de derinleştirmiştir.

Dijital teknolojilerin bilişsel etkileri, kişinin maddi ve manevi varlığını geliştirme hakkı üzerindeki aşınmayı daha da belirgin hâle getirmektedir. Arama motorları ve yapay zekâ temelli sistemlerin bilgiye erişimi yoğun biçimde kişiselleştirmesi, nesnel ve ortak bir bilgi zeminine ulaşmayı güçleştirmektedir. Aynı arama sorgusunun farklı bireyler için farklı sonuçlar üretmesi, bilginin doğrulanabilir ortak bir referans olmaktan çıkmasına yol açmaktadır[1394]. Bu durumda bilgi, kamusal ve paylaşılabilir bir gerçeklik olmaktan ziyade, bireysel önyargılarla uyumlu kişisel bir gerçekliğe dönüşmektedir. Böyle bir enformasyon ortamı, bilimsel düşünmenin, eleştirel aklın ve kamusal tartışmanın epistemik temellerini zayıflatmaktadır.

Gelişen teknoloji ve kullanışlı teknolojik araçların sağladıkları rahatlık nedeniyle insanların bilgiye erişimi her geçen gün artmakla birlikte insanları daha bilge ya da akıllı hale getirmeyip öyle görünmelerine yol açmaktadır. Google kurucu liderlerinden Sergey Brin, "*Beyinlerinizin üçte ikisinin Google'dan oluşmasını istiyoruz*" demiştir[1395]. Bu bilişsel dönüşüm, bireyin zihinsel özerkliği bakımından da ciddi sonuçlar doğurur. Teknoloji, başlangıçta bilgiye erişimi kolaylaştıran bir araç olarak sunulsa da pratikte düşünme, hatırlama ve anlamlandırma faaliyetlerini makineler lehine ikame etmektedir. Soruların giderek daha fazla algoritmalar tarafından yanıtlanması, bireyin zihinsel emek kapasitesini köreltmekte; hafıza, dikkat ve yaratıcılık gibi temel bilişsel yetiler zayıflamaktadır. Böylece teknoloji, özgürleşmenin değil, zihinsel bağımlılığın

[1393] Bihterin Dinçkol, *"Yönetilenlerin 'Öz' Yönetimi-Kamuoyu",* s.61.
[1394] Florian A. Schneider, "Searching for 'Digital Asia' in its Networks: Where the Spatial Turn Meets the Digital Turn", **Asiascape: Digital Asia,** Vol.2, No.1-2, (2015), s.63-64.
[1395] "Google Search Event Live 2010", *Business Insider,* 2010, https://www.businessinsider.com/google-search-event-live-2010-9?r=US&IR=T (2 Şubat 2026).

altyapısını üretmektedir[1396]. Bu durum, bireyin kendi düşünsel üretimiyle anlam kurma kapasitesini aşındırarak manevi varlığın gelişimini doğrudan engeller.

Güncel bilişsel ve psikolojik araştırmalar, yoğun dijital tüketimin dikkat süresini kısalttığını, derin odaklanma ve uzun süreli düşünme becerilerini zayıflattığını ortaya koymaktadır. Sürekli bildirimler, hızlı içerik akışı ve parçalı dikkat rejimi, bireyin zihinsel bütünlüğünü bozmakta; kronik zihinsel yorgunluk, odaklanma güçlüğü ve karar verme sorunları üretmektedir. Bu tablo, yalnızca bireysel bir sağlık meselesi değil; kişinin kendi yaşamını anlamlı biçimde yönlendirme ve geliştirme kapasitesine yönelik yapısal bir müdahale niteliği taşımaktadır[1397].

Teknolojinin bireye zaman kazandırma vaadi, pratikte çoğu zaman tersine dönmekte; dijital araçlar bireyin zamanını ve dikkatini sistematik biçimde tüketmektedir. Bağımlılık üretmeye elverişli biçimde tasarlanan dijital mimariler, bireyin iradi gelişimini desteklemek yerine edilgen tüketimi teşvik etmektedir. İnsan biyolojisinin bu denli hızlı ve yoğun bir dijital uyarana uyum sağlamakta zorlanması, bireyin kendi doğasıyla çatışmasına; yalnızlık, huzursuzluk ve anlam kaybı duygularının derinleşmesine yol açmaktadır. Bu durum, manevi varlığın gelişimi bakımından ciddi bir risk alanı oluşturmaktadır. Kişinin maddi varlığını geliştirme boyutu da bu süreçten bağımsız değildir. Sürekli çevrimiçi olma hâli, uyku düzeninden sinir sistemi işleyişine kadar biyolojik sınırları zorlamakta özellikle gelişim çağındaki bireyler bakımından bilişsel ve nörolojik riskler doğurmaktadır[1398].

Kontrolsüz dijitalleşme, bireyi özgür ve düşünen bir özne olmaktan çıkararak algoritmalar tarafından yönlendirilen bir nesneye dönüştürme potansiyeli taşımaktadır.

[1396] Yogesh Malik, "Will Google Ever Become the Third Half of Our Brain?", *Medium*, 2018 https://medium.com/quotes-and-thoughts/will-google-ever-become-the-third-half-of-our-brain-bd3d36cfba97 (2 Şubat 2026).

[1397] Dijital Dünya Beyni Nasıl Etkiliyor?, 6 dak, YouTube: HaberTürk TV, 2025, https://www.youtube.com/watch?v=fflMkGJl5mY.

[1398] Teknoloji'nin İnsanlığa Kaybettirdikleri... | Sinan Canan ile Açık Beyin, 6 dak, YouTube: Prof. Dr. Sinan Canan ile Açık Beyin, 2024, https://www.youtube.com/watch?v=kCkgHw95vy8&t=3s.

Bu durum, kişinin kendi varlığını özgürce, sağlıklı ve anlamlı biçimde geliştirme imkânını daraltan çağdaş bir müdahale biçimi olarak değerlendirilmelidir.

Sonuç olarak veri temelli, piyasa merkezli ve denetimsiz dijitalleşme, bireyin maddi ve manevi varlığını geliştirme hakkının özüne yönelen yapısal bir tehdit oluşturmaktadır. Bu hak, dijital çağda yalnızca bireysel bilinç ve özdenetimle korunabilecek bir alan değildir. Algoritmik şeffaflık, çoğul karşılaşmaları teşvik eden düzenleyici çerçeveler ve insan onurunu merkeze alan anayasal bir dijital yaklaşımın inşası zorunludur. Aksi hâlde dijitalleşme, özgürleşme vaadi altında, bireyin düşünsel özerkliğini, manevi derinliğini ve özne olma kapasitesini sessizce aşındıran kalıcı bir erozyon sürecine dönüşecektir.

SONUÇ

Bu çalışma, dijitalleşmenin modern devlet egemenliği üzerindeki etkisini, teknolojik determinizme, salt araçsalcı iyimserliğe ya da devletin kaçınılmaz çözülüşü anlatısına teslim olmadan; tarihsel, hukuki, siyasal, iktisadi ve normatif boyutları birlikte dikkate alan bütüncül bir çerçevede incelemiştir. Tezin genel sonucu, dijitalleşmenin devlet egemenliğini ortadan kaldırmadığı; ancak onun klasik varsayımlarını, işleyiş mantığını ve meşruiyet zeminini eşzamanlı olarak aşındırdığı, bu aşınmanın da egemenliği giderek daha kırılgan, parçalı ve istikrarsız bir kurumsal yapıya dönüştürdüğüdür. Bu bağlamda dijitalleşme, egemenliğin sonu değildir; ancak denetimsiz bırakıldığında hem devlet hem de yurttaş açısından ciddi tehlikeler barındıran tarihsel bir metamorfozdur. Bununla birlikte yaşanan dönüşüm tek boyutlu değildir. Dijitalleşme bir yandan devletin geleneksel egemenlik kapasitesini aşındırmakta, diğer yandan devlete yeni gözetim, denetim ve müdahale araçları sunarak egemenliği belirli yönlerden pekiştirmektedir. Dolayısıyla dijital çağın temel meselesi, egemenliğin sona erip ermediği değil; hangi araçlarla, hangi aktörlerle rekabet içinde, hangi sınırlar içinde ve kimin yararına yeniden kurulduğudur.

Tez boyunca yapılan kavramsal inceleme, dijitalleşmenin salt teknik bir ilerleme ya da nötr bir modernleşme evresi olarak ele alınamayacağını göstermiştir. Dijital, algoritma, veri, yapay zekâ, platform, siber alan, bulut bilişim, blok zincir ve dijital altyapı gibi kavramlar, artık teknik olmanın yanında doğrudan siyasal ve hukuki sonuçlar üreten kurucu kategoriler hâline gelmiştir. Bu tespit, tezin ilk ve temel bulgusudur. Dijitalleşme; bilginin üretim, dolaşım ve denetim biçimlerini dönüştürürken, egemenliğin klasik olarak yasama, yürütme, zor kullanma, vergilendirme, para politikası, güvenlik ve kamusal düzen sağlama gibi görünümlerini de doğrudan etkilemektedir. İnternetin dağıtık mimarisi ile algoritmik karar sistemlerinin merkezileştirici etkisi arasındaki yapısal gerilim, dijital çağın temel iktidar paradoksunu oluşturmakta; bu paradoks, kamusal gücün görünmez biçimlerde yoğunlaşmasına ve demokratik denetimden kaçmasına elverişli bir zemin yaratmaktadır. Bu süreçte egemenlik, yalnızca hukuken tanımlanan bir yetki alanı olmaktan çıkıp veri, kod, ağ mimarisi ve altyapı kontrolü üzerinden de yeniden

şekillenen çok katmanlı bir iktidar biçimine dönüşmekte; bu da devletin klasik denetim araçlarını giderek etkisizleştirmektedir.

Bu çerçevede tezde ulaşılan ikinci önemli sonuç, dijital egemenlik kavramının ancak kamu hukuku ekseni korunarak anlamlı biçimde kullanılabileceğidir. Egemenliğin öznesi bakımından belirleyici olan unsur; salt fiilî güç, teknik kapasite veya altyapı hâkimiyeti değildir; norm koyma yetkisinin meşruiyetle birleşmesidir. Bu sebeple dijital egemenliği doğrudan şirketlere, platformlara ya da yalnızca teknik sistemlere atfeden yaklaşımlar, kavramı hukuki içeriğinden soyutlayarak onu çıplak güç ilişkilerine indirgemektedir. Tez, bu tür indirgemelerin analitik bakımdan cazip görünse de kamu hukuku bakımından sorunlu olduğunu göstermiştir. Çünkü şirketlerin fiilî kudreti ne kadar büyük olursa olsun, bu güç kendi başına siyasal meşruiyet üretmemektedir. Buna karşılık şirketlerin fiilî etkisi, devletin egemenlik kullanımını sınırlandırmakta, paylaşmakta veya dolaylı biçimde yeniden biçimlendirmektedir. Buradan çıkan sonuç şudur: Egemenlik devlete ait olmaya devam etmektedir; ancak egemenliğin kullanım sahası artık devlet dışı aktörlerle yoğun gerilim içinde şekillenmektedir.

Üretim süreçleri ile siyasal iktidarın birlikte dönüşümünü inceleyen bölümler, dijital kapitalizmin modern egemenlik krizini derinleştiren tarihsel bir iktidar rejimi yarattığını ortaya koymuştur. Platform kapitalizmi, gözetim kapitalizmi ve tekno-feodalizm tartışmaları, dijitalleşmenin ekonomik bir yapılanma olmasının ötesinde siyasal iktidarın maddi dayanaklarını da dönüştürdüğünü göstermiştir. Nitekim Shoshana Zuboff, dijital ekonominin temel dinamiğini gözetim kapitalizmi olarak tanımlamakta ve bu sistemde birey davranışlarının sürekli veri üretimine dönüştürülerek tahmin edilebilir ve yönlendirilebilir ekonomik kaynaklara çevrildiğini ileri sürmektedir. Bu modelde kullanıcı deneyimleri, platform şirketleri tarafından davranışsal artığa/veri fazlasına dönüştürülmekte ve bu veriler üzerinden davranışsal öngörü piyasaları kurulmaktadır. Benzer biçimde Yanis Varoufakis, dijital çağda büyük platformların klasik piyasa rekabetinin ötesine geçen yeni bir teknofeodal düzen yarattığını ileri sürmekte; bu düzende platform sahiplerinin bulut lordları (cloud lords) olarak adlandırdığı yeni bir egemen sınıf oluşturduğunu savunmaktadır. Bu yapıda kullanıcılar ve içerik üreticileri; verileri ve etkileşimleri üzerinden değer üreten ancak platform altyapıları üzerinde

mülkiyet hakkı bulunmayan, adeta dijital serfliğe benzer bir konuma sürüklenen yeni bir bağımlı emek kategorisi hâline gelmektedir. Böylece üretim ilişkileri teknolojik formun yanı sıra sınıfsal bakımdan da yeniden örgütlenmekte; platform altyapılarını kontrol eden dar bir küresel elit ile veri/dikkat üreten geniş kullanıcı kitleleri arasında yeni bir hiyerarşik yapı ortaya çıkmaktadır.

Sermayenin, verinin ve altyapıların belirli küresel merkezlerde yoğunlaşması, devletlerin ekonomik egemenliğini aşındırmakta; klasik vergilendirme, rekabet düzenleme, piyasa denetimi ve emek ilişkilerini yönetme kapasitesini zorlamaktadır. Bu süreçte değişen husus, üretim araçlarının niteliği kadar, üretimin denetim mantığıdır. Sanayi kapitalizminde üretim daha görünür mekânsal yapılara ve fiziksel mülkiyet biçimlerine dayanırken, dijital kapitalizmde değer üretimi görünmez veri akışları, ağ etkileri, kullanıcı etkileşimi ve davranışsal öngörü mekanizmaları üzerinden gerçekleşmektedir. Değişmeyen husus ise iktidarın maddi bir zemine dayanma zorunluluğudur. Yani üretim biçimleri değişse de iktidarın ekonomik temelden bütünüyle bağımsızlaştığı söylenemez. Aksine değişim, ekonomik temelin maddi görünümünü dönüştürmüş; fakat iktidarın maddi dayanak ihtiyacını ortadan kaldırmamıştır. Bunun nedeni, her egemenlik biçiminin sonunda kaynak, altyapı, emek, bilgi ve organizasyon gücü üzerinde belirli bir hâkimiyet gerektirmesidir.

Veri odaklı dijital teknolojilere ilişkin inceleme, egemenlikteki dönüşümün yalnızca yasa ve zor kullanma araçları üzerinden değil, öngörü, sınıflandırma, profilleme, yönlendirme ve normalleştirme teknikleri üzerinden de gerçekleştiğini göstermiştir. Büyük veri analitiği, yapay zekâ destekli karar sistemleri, kişiselleştirme ve hedefleme pratikleri; devletin ve platformların birey üzerinde yeni tip bir davranışsal müdahale alanı kurmasına imkân tanımaktadır. Bu bakımdan değişen şey, iktidarın görünümüdür. Klasik egemenlik çoğu zaman buyuran, yasaklayan ve cezalandıran açık bir siyasal kudret olarak görünürken; dijital çağın iktidarı çoğu zaman öneren, sıralayan, filtreleyen, erişimi biçimlendiren ve seçenekleri önceden yapılandıran dolaylı mekanizmalar üzerinden işlemektedir. Buna karşılık değişmeyen şey; iktidarın yön verici ve biçimlendirici niteliğidir. Yani egemenliğin normatif çekirdeğinde yer alan davranışları düzenleme işlevi devam etmektedir; yalnızca bunun araçları daha dağınık, görünmez ve teknikleşmiş

hâle gelmektedir. Bu araçların değişmesinin nedeni; dijital teknolojilerin davranışsal veri üretimini ve öngörü kapasitesini olağanüstü artırmış olmasıdır; buna karşılık iktidarın insan davranışını düzenleme yönündeki tarihsel eğiliminin değişmemesinin nedeni, siyasal düzenin her dönemde belirli bir öngörülebilirlik ve itaat biçimi aramasıdır.

Tezin önemli tespitlerinden biri, dijital alanın çok aktörlü yapısının egemenliği ne tamamen devletsizleştirdiği ne de bütünüyle eski biçimiyle devlette bıraktığıdır. Devletler, büyük teknoloji şirketleri, düzenleyici teknik kuruluşlar, kullanıcılar, sivil toplum örgütleri ve zaman zaman ademimerkeziyetçi dijital ağlar arasında şekillenen bu alan, egemenliğin fiilî kullanımını parçalamakta; bu parçalanma hukuki sorumluluğun dağılması ve meşruiyetin bulanıklaşması sonucunu doğurmaktadır. Özellikle devlet-platform ilişkisi bu bakımdan belirleyici bir düğüm noktasıdır. Devlet ile platform arasındaki ilişki saf bir karşıtlık ilişkisi değildir; rekabet, bağımlılık, iş birliği ve karşılıklı araçsallaştırma unsurlarını aynı anda içeren hibrit bir ilişkidir. Devlet; platformların veri birikimi, iletişim altyapısı, yapay zekâ kapasitesi ve toplumsal etki gücüne ihtiyaç duymakta; platformlar ise devletin hukuki korumasına, pazar erişimine, kamu ihalelerine, ulusal güvenlik çerçevelerine ve düzenleyici tercihlerine bağımlı kalmaktadır. Bu nedenle aralarındaki ilişki ne yalnızca egemenliğin platformlara kaptırılması ne de devletin platformları mutlak biçimde tahakküm altına alması şeklinde okunabilir. Daha doğru ifade etmek gerekirse, devlet-platform ilişkisi dijital çağda egemenliğin fiilen müzakere edildiği, çatıştığı ve yeniden dağıtıldığı merkezi sahadır.

Bu ilişkinin sonucu olarak tezde ulaşılan bulgulardan biri, platformların fiilî norm koyucu hâle geldiğidir. İçerik moderasyonu, hesap kapatma, görünürlük sıralaması, tavsiye sistemleri, reklam hedefleme ve uygulama ekosistemleri üzerindeki kontroller yoluyla platformlar, kamusal iletişim alanında hangi sözün ne kadar dolaşacağına, hangi içeriğin öne çıkacağına ve hangi davranışların ödüllendirilip bastırılacağına etkide bulunmaktadır. Bu durum, klasik medya çalışmalarında tanımlanan kapı bekçiliği (gatekeeping) işlevinin dijital ortamda içerik akışının büyük ölçüde algoritmik sıralama sistemleri ve platform politikalarınca belirlendiği algoritmik kapı bekçiliği biçimine evrildiğini göstermektedir. Böylece kamusal iletişim alanına giriş ve görünürlük eşikleri, şeffaflığı sınırlı teknik ve kurumsal karar mekanizmaları tarafından belirlenmektedir. Bu

yapı, literatürde özel normatif düzen (private ordering) olarak adlandırılan ve kamusal davranış kurallarının devlet dışı aktörler tarafından fiilen belirlenmesi anlamına gelen yeni bir normatif düzen üretmektedir. Bu durum, devletin hukuk üretme ve düzenleme tekeline doğrudan rakip bir normatif alan üretmektedir. Fakat burada da değişmeyen bir husus vardır: nihai meşruiyet beklentisi hâlâ kamusaldır. Kullanıcılar, platformların kararlarını bile çoğu zaman adalet, şeffaflık, itiraz hakkı ve hesap verebilirlik gibi kamusal-hukuki ölçütlerle değerlendirmektedir. Yani değişen şey norm koyucunun biçimi ve aracı; değişmeyen şey ise normların meşruiyet talebine tabi olmasıdır. Platformlar bu meşruiyeti tam anlamıyla üretemedikleri için devletle aralarındaki gerilim yapısal olarak sürmektedir. Dolayısıyla dijital platformların ürettiği bu özel normatif düzen, egemenliğin tamamen ortadan kalktığını değil; fakat norm koyma ve kamusal iletişim alanını düzenleme kapasitesinin devlet ile platformlar arasında parçalanarak egemenliğin klasik bütünlüğünü aşındırdığını göstermektedir.

Tezin ikinci ana ekseninde modern devletin kurucu unsurları bakımından dijitalleşmenin yarattığı aşınma derinleştirilmiştir. İnsan unsurunun dönüşümü, egemenlik krizinin yalnızca kurumsal değil, aynı zamanda antropolojik bir kriz olduğunu göstermiştir. Yurttaşın verileşmesi yani siyasal özne olmaktan çıkıp veri izlerine indirgenebilir, analiz edilebilir ve yönlendirilebilir bir profile dönüşmesi, egemenliğin toplumsal meşruiyet temelini içten içe çözmektedir. Andrew Shapiro'nun "kontrol devrimi" kavramsallaştırmasının işaret ettiği üzere, dijital ağlar bireye artan tercih ve hareket özgürlüğü sunduğu izlenimini yaratırken, aynı anda daha yoğun izleme ve yönlendirme mekanizmalarını da devreye sokmaktadır. Böylece dijital çağda özgürlük, çoğu zaman özerkliğin genişlemesinden çok, kontrolün görünmezleşmesiyle üretilen bir yanılsamaya dönüşmektedir.

Burada değişen husus, yurttaşlık deneyiminin niteliğidir. Modern siyasal düzende yurttaş, hak sahibi, rıza gösteren, temsil edilen ve kamusal akla katılan bir özne olarak düşünülürken; dijital çağda giderek daha fazla ölçülebilir, segmentlere ayrılabilir ve davranışsal tahmin nesnesi olarak kavranmaktadır. Buna rağmen değişmeyen husus, egemenliğin meşruiyet için hâlâ insan unsuruna ihtiyaç duymasıdır. Devletler ve platformlar ne kadar veri-temelli yönetim teknikleri kullanırlarsa kullansınlar,

nihayetinde yönettikleri şey insan topluluğudur ve insan onurunu tümüyle dışlayan bir düzenin istikrarlı meşruiyet üretmesi mümkün değildir. Bu nedenle değişmeyen unsur, insanın hukuki ve ahlaki merkeziliğidir; değişen unsur ise insanın iktidar yapıları içinde kavranma ve işlenme biçimidir. Bu değişimin nedeni, veri ekonomisinin insanı öncelikle öngörülebilir davranış kalıplarının kaynağı olarak işlemesidir; değişmeyenin nedeni ise insan haklarının ve onurun modern hukuk düzeninin vazgeçilmez normatif zemini olmaya devam etmesidir.

Ülke unsuruna ilişkin inceleme de benzer bir ikili sonuç vermiş; ülke unsurunun dönüşümü egemenliğin mekânsal temelinin çözülüşünü görünür kılmıştır. Dijitalleşme ülkeyi ve sınırı ortadan kaldırmamaktadır; fakat onların işlevini dönüştürmektedir. Sınırlar artık yalnızca fiziki coğrafya üzerinden değil, veri akışları, platform erişimleri, dijital altyapı bağımlılıkları, siber güvenlik duvarları ve hukuki yetki çatışmaları üzerinden de kurulmaktadır. Bu nedenle değişen şey, ülkeselliğin görünümüdür. Klasik sınır anlayışı, fiziksel denetim ve mekânsal süreklilik üzerinden işlerken; dijital çağın sınırları çoğu zaman akışları yöneten, erişimi kısıtlayan, veriyi yerelleştiren ve ağları filtreleyen hibrit yapılara dönüşmektedir. Buna karşılık değişmeyen şey, egemenliğin yine belirli bir mekânsal ve kurumsal dayanak arayışıdır. Devletler hâlâ belirli bir ülke, hukuk düzeni ve yetki alanı üzerinden hareket etmektedir. Bunun değişmemesinin nedeni, siyasal otoritenin soyut ağlar içinde tamamen çözülmesinin henüz ne meşruiyet ne de kurumsal süreklilik üretebilmesidir. Değişimin nedeni ise dijital ağların ve küresel veri dolaşımının ülkesel hakimiyetin eski araçlarıyla tam olarak yönetilememesidir. Bu durum, devletin güvenlik ve denetim reflekslerini sertleştirirken; yurttaş açısından hukuki belirliliğin zayıflamasına ve hak koruma mekanizmalarının parçalanmasına yol açmaktadır. Egemenliğin mekânsal belirsizliği, sorumluluğun da belirsizleştiği bir yönetim pratiğini beraberinde getirmektedir.

Tezin en kritik bulgularından biri, dijitalleşmenin egemenliğin meşruiyet, iktidar ve koruma fonksiyonlarını eşzamanlı olarak zayıflatmasıdır. Dijital platformların fiilî norm koyucu hâline gelmesi, devletin yasa-uygulama-yaptırım bütünlüğünü aşındırırken; siber tehditler, veri ihlalleri ve algoritmik manipülasyonlar karşısında yurttaşın

korunmasızlığını artırmaktadır. Böylece egemenlik, hukuki olarak devlette kalmasına rağmen fiilî olarak parçalanmış ve denetlenmesi güç bir iktidar alanına dönüşmektedir.

Bu çerçevede bir diğer önemli bulgu, dijitalleşmenin egemenliğin koruma fonksiyonunu paradoksal biçimde hem güçlendirmesi hem zayıflatmasıdır. Devletler dijital araçlar sayesinde suç analizi, sınır güvenliği, istihbarat, siber savunma, kamu hizmeti sunumu ve kriz yönetimi bakımından yeni kapasitelere sahip olmaktadır. Bu yönüyle dijitalleşme egemenliği pekiştirmektedir. Ancak aynı anda siber saldırılar, hibrit savaş yöntemleri, veri ihlalleri, dezenformasyon, platform manipülasyonu ve sınır aşan dijital suçlar karşısında devletin koruyucu niteliği yeni açıklıklar vermektedir. Bu nedenle tehditlerin biçimi ve koruma araçlarının niteliği değişirken, devletin koruma yükümlülüğü değişmemektedir. Çünkü modern egemenliğin normatif meşruiyeti, önemli ölçüde yurttaşı koruma vaadi üzerine kuruludur. Bu vaat çözüldüğünde egemenliğin meşruiyet zemini de çöker. Dolayısıyla koruma fonksiyonunun değişmemesinin nedeni, onun egemenliğin özüne içkin olmasıdır; değişen koruma araçlarının nedeni ise tehditlerin artık fiziksel değil, ağsal, verisel ve algoritmik formlar kazanmış olmasıdır.

Temel hak ve özgürlükler bakımından yapılan analiz, dijitalleşmenin demokratik toplum düzenini çoğu kez açık baskıdan ziyade sessiz, dağınık ve yapısal mekanizmalar aracılığıyla aşındırdığını ortaya koymuştur. Gözetim, kişiselleştirme, algoritmik sıralama, içerik filtreleme, davranışsal müdahale ve profilleme teknikleri; ifade özgürlüğü, özel hayatın gizliliği, eşitlik, kişilik hakları ve kişinin maddi ve manevi varlığını geliştirme hakkı üzerinde kalıcı tahribatlar doğurmaktadır. Nitekim Cass R. Sunstein, dijital iletişim ortamlarında ortaya çıkan siber yayılma dalgaları (cybercascades) kuramı çerçevesinde filtre balonları ve yankı odaları olgularının bireylerin çoğunlukla benzer görüşlerle karşılaşmasına yol açtığını, bunun da kamusal tartışma alanını daraltarak bilgi dolaşımı üzerinde yapısal bir erozyon yarattığını göstermiştir. Mikro hedefleme teknikleri ise siyasal iletişimi kamusal tartışma alanından çıkararak birey düzeyinde kapalı ve görünmez ikna süreçlerine dönüştürmekte, farklı seçmen gruplarının birbirinden tamamen yalıtılmış mesajlara maruz kalmasına yol açarak demokratik karar süreçlerinin dayandığı ortak bilgi zemininin parçalanmasını hızlandırmaktadır. Bu bağlamda Byung-Chul Han'ın enfokrasi (infocracy) kavramsallaştırması, dijital çağda iktidarın zor

kullanımıyla değil, bilgi akışının yönlendirilmesi ve veri temelli iletişim ortamlarının manipülasyonu yoluyla işlediğini ortaya koymaktadır. Han'a göre bilgi fazlalığı ve sürekli veri akışı, kamusal aklı güçlendirmek yerine dikkat ekonomisi ve yönlendirilmiş enformasyon ortamı yaratarak demokratik irade oluşumunu zayıflatmaktadır.

Burada değişen husus, hak ihlalinin tarzıdır. Klasik hak ihlalleri daha doğrudan, tanımlanabilir ve faili belirli nitelikteyken; dijital çağda hak ihlalleri çoğu zaman çok aktörlü, dağınık, otomatikleşmiş ve sorumluluğu bulanıklaştırılmış mekanizmalar içinde ortaya çıkmaktadır. Buna karşılık değişmeyen husus, temel hakların egemenliğin normatif sınırı olma işlevidir. Bunun değişmemesinin nedeni, anayasal devlet fikrinin egemenliği sınırsız kudret olarak değil, hukukla bağlı kamusal yetki olarak kurgulamasıdır. Dijital çağda da bu sınır ihtiyacı devam etmektedir; hatta daha da keskinleşmektedir. Çünkü iktidar görünmezleştikçe hukuki sınırlama ihtiyacı artmaktadır.

Tez boyunca ulaşılan bir başka sonuç da şudur: kavramlar değişmekte, fakat bazı kuramsal çekirdekler direnmektedir. Egemenlik, yurttaşlık, ülke, kamu gücü, özgürlük, güvenlik ve meşruiyet gibi kavramların içerikleri dijital çağda genişlemekte, parçalanmakta veya yeni katmanlar kazanmaktadır. Örneğin egemenlik artık yalnızca hukuki üstünlük değil; veri ve altyapı üzerinde düzenleme kapasitesiyle de birlikte düşünülmektedir. Yurttaşlık artık siyasi katılımın yanında dijital kimlik, veri öznesi olma ve çevrimiçi görünürlük meselelerini de içermektedir. Ülke artık fiziksel toprağın yanında dijital altyapılar ve veri akışlarıyla ilişkili bir yetki alanıdır. Buna rağmen değişmeyen kuramsal çekirdekler vardır: siyasal otoritenin meşruiyet ihtiyacı, kamusal gücün hukukla sınırlandırılması gereği ve insan onurunun normatif üstünlüğü bunların başında gelmektedir. Bunların değişmemesinin nedeni, modern kamu hukukunun kurucu ilkeleri olmaları ve dijital dönüşümün bu ilkeleri işlevsiz kılmak yerine daha da vazgeçilmez hale getirmesidir. Değişen kavramların nedeni ise toplumsal ve teknolojik altyapının dönüşmesi; değişmeyen çekirdeklerin nedeni ise siyasal birlik ve hak rejiminin bunlar olmaksızın sürdürülememesidir.

Karşılaştırmalı olarak bakıldığında, ABD, Çin ve AB örnekleri de bu sonucu doğrulamaktadır. Modeller değişmekte fakat devletlerin dijital alan üzerindeki hakimiyet

kurma arzusu değişmemektedir. ABD daha piyasa merkezli ve şirketlerle iç içe geçmiş bir dijital egemenlik pratiği geliştirirken, Çin devlet merkezli ve güvenlik odaklı bir dijital yönetim modeli izlemekte, AB ise hak ve değer temelli bir düzenleyici model geliştirmeye çalışmaktadır. Değişen husus; yöntem, yoğunluk ve meşrulaştırma söylemidir. Değişmeyen husus ise devletlerin dijital alanı başıboş bırakmama eğilimidir. Bunun nedeni açıktır: Veri, iletişim, kritik altyapı ve platform hakimiyeti artık ekonomik olduğu kadar jeopolitik ve egemenlik meselesine dönüşmüştür. Dolayısıyla devletler arasında model farkı olsa da dijital alanın stratejik önemi konusunda ortaklaşma bulunmaktadır.

Bu çalışma ayrıca göstermiştir ki dijital aktörler arasındaki ilişkiler gelecekte daha da yoğunlaşacak, özellikle devlet-platform ilişkisi daha çatışmalı fakat daha karşılıklı bağımlı bir hâl alacaktır. Platformlar kamusal iletişim, ticaret, veri işleme ve yapay zekâ altyapıları üzerinde daha fazla etkili oldukça, devletler bunları ya daha yoğun regüle etmeye ya da daha doğrudan kendi stratejik araçlarına eklemlemeye çalışacaktır. Buna paralel olarak platformlar da salt özel şirket olarak kalmayıp fiilen yarı kamusal fonksiyonlar üstlenen, hatta kimi zaman devlet benzeri hizmetler sunan yapılara dönüşebilecektir. Ancak bu dönüşüm, onların meşruiyet sorununu çözmeyecektir. Tersine, hesap verebilirlik, şeffaflık ve hukuki sorumluluk meseleleri daha da derinleşecektir. Bu nedenle geleceğe dönük en güçlü öngörü, devlet ile platform arasında bir saf ayrışmadan ziyade artan düzenleme, seçici iş birliği, stratejik rekabet ve egemenlik alanının sürekli yeniden pazarlığı biçimindeki hibrit ilişkinin yoğunlaşacağı yönündedir.

Geleceğe dönük bir diğer öngörü, egemenliğin klasik fiziksel araçlardan çok veri, standart, altyapı, yapay zekâ kapasitesi ve yarı iletken-ekosistem gibi stratejik teknoloji alanları üzerinden tartışılacağıdır. Önümüzdeki dönemde dijital egemenlik, yalnızca veri yerelleştirmesi veya platform regülasyonu başlıklarıyla sınırlı kalmayacak; yapay zekâ modellerinin eğitimi, hesaplama gücü, bulut altyapısının jeopolitiği, kuantum güvenliği, dijital para sistemleri ve ulusal kritik veri alanlarının korunması gibi başlıklarla daha da genişleyecektir. Bu gelişmeler, devletleri bir yandan daha müdahaleci olmaya itecektir. Fakat aynı zamanda, müdahalenin sınırları ve hukuki ölçülülüğü de daha fazla tartışılacaktır. Çünkü dijital egemenlik iddiası arttıkça dijital otoriterlik riski de

büyüyecektir. Dolayısıyla geleceğin temel çatışması, dijital alanın düzenlenip düzenlenmeyeceğinden ziyade nasıl düzenleneceği; kamusal koruma ile özgürlük, güvenlik ile mahremiyet, egemenlik ile insan hakları arasında dengenin nasıl kurulacağı olacaktır.

Bu tezden çıkan nihai sonuç, dijitalleşmenin devlet egemenliğini ortadan kaldırmadığı; fakat onu klasik biçimiyle sürdürülemez hâle getirdiğidir. Egemenlik artık ne yalnızca toprak üzerinde mutlak komuta ne de sınır tanımaz ağ özgürlüğü olarak anlaşılabilir. Ortaya çıkan yapı, hukuki egemenlik ile fiilî dijital iktidar arasındaki gerilimin derinleştiği, çok aktörlü, hibrit, parçalı ve yapısal olarak istikrarsız bir egemenlik rejimidir. Bu rejimde devletin tamamen geri çekilmesi de sınırsız dijital güvenlik mantığıyla her şeyi kontrol altına alma iddiası da çözüm üretmemektedir. Çünkü ilk durumda kamusal meşruiyet ve koruma kapasitesi boşalmakta; ikinci durumda ise insan hakları ve demokratik toplum düzeni ağır bir baskı altına girmektedir.

Bu nedenle dijital çağda savunulması gereken şey, nostaljik anlamda klasik egemenlik değildir. Savunulması gereken, insan onurunu, demokratik meşruiyeti, hukuki belirliliği ve kamusal yararı koruyabilecek biçimde yeniden düşünülmüş bir egemenlik anlayışıdır. Böyle bir anlayış, devletin dijital alan üzerindeki düzenleme ve koruma kapasitesini kabul etmeli; ancak bu kapasiteyi hukukla, temel haklarla, şeffaflıkla ve hesap verebilirlikle sıkı biçimde bağlamalıdır. Aynı zamanda platformların fiilî kamusal gücünü görünür kılarak onları da sorumluluk rejimine tabi tutmalıdır. Bu tez, tam da bu nedenle, dijitalleşmenin egemenlik üzerindeki etkilerini yalnızca bir kriz anlatısı olarak değil, yeni bir kamusal-hukuki inşa zorunluluğu olarak okumaktadır.

Son tahlilde egemenliğin geleceği, teknik kapasite yarışının kim tarafından kazanılacağından daha çok, dijital iktidarın hukukla, demokrasiyle ve insanla yeniden bağ kurup kuramayacağına bağlıdır. Devlet dijital çağda hâlâ vazgeçilmezdir; fakat artık eski anlamıyla düşünülemez. Platformlar vazgeçilmez altyapı aktörlerine dönüşmüştür; fakat meşru egemenin yerini alamazlar. İnsan hâlâ hukukun ve siyasetin merkezidir; fakat veri nesnesine indirgenme riski hiç olmadığı kadar artmıştır. Sınırlar hâlâ vardır; fakat artık yalnızca coğrafyada değil, ağlarda ve veri akışlarında da çizilmektedir. İşte bu nedenle dijital çağın egemenlik sorunu, aslında devletin, platformların ve yurttaşın hangi yeni

hukuki-siyasal düzende birlikte var olacağı sorunudur. Tezin vardığı sonuç, bu soruya verilecek cevabın ne tam bir devlet gerilemesi ne de sınırsız dijital tahakküm olabileceğidir; cevap, ancak insan hakları merkezli, demokratik meşruiyete dayalı ve dijital iktidarı çok katmanlı biçimde sınırlandıran yeni bir kamu hukuku ufkunda bulunabilir.

KAYNAKÇA

I. Kitaplar ve Makaleler

Açıkgöz, Osman. "Elektronik Haberleşme Sektöründe Arabağlantı Sözleşmesi". Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.). **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.207-218.

Ağaoğulları, Mehmet Ali ve Levent Köker, **İmparatorluktan Tanrı Devletine**. 9. Baskı, Ankara: İmge Kitabevi, 2020.

Ağaoğulları, Mehmet Ali ve Levent Köker. **Kral-Devlet ya da Ölümlü Tanrı**. 5. Baskı, Ankara: İmge Kitabevi, 2018.

Ağaoğulları, Mehmet Ali, Filiz Zabcı ve Reyda Ergün. **Kral-Devletten Ulus-Devlete**. 3. Baskı, Ankara: İmge Kitabevi, 2017.

Ağaoğulları, Mehmet Ali. **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler.** 8. Baskı. İstanbul: İletişim, 2019.

Akad, Mehmet, Bihterin Dinçkol ve Nihat Bulut. **Genel Kamu Hukuku**. Gözden Geçirilmiş 16. Basım. İstanbul: Der Yayınları, 2020.

Akad, Mehmet, Nihat Bulut, Yusuf Şevki Hakyemez, Cevat Okutan. **Küreselleşme ve Türkiye (Türkiye'de Devletin Gelişimi)**. ed. Cevat Okutan. Ankara: Seçkin Yayıncılık, 2007.

Akal, Cemal Bali. "Devlet, Yasa, Hakimiyet", **Cumhuriyetin 75. Yılı Armağanı.** İstanbul: İstanbul Üniversitesi Yayınevi, 1999.

Akal, Cemal Bali. **Modern Düşüncenin Doğuşu: İspanyol Altın Çağı.** 7. Baskı, Ankara: Dost Kitabevi Yayınları, 2013.

Akçaal, Mehmet. “Profilleme Kavramının Kişilik Hakkı ve Kişisel Verilerin Korunması Bağlamında Değerlendirilmesi”, Şerafettin Ekici ve Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.487-500,

Akdenizli, Banu. “İnternet, Egemenlik ve Devlet: İnternet’in Ulusal ve Uluslararası Yönetime Etkileri Üzerine Bir Değerlendirme”, **Global Media Journal**. Cilt.Bahar, Sayı.2, 2011.

Akın, İlhan ve Mehmet Akad, “Cumhuriyetin Ellinci Yılında Temel Hak ve Özgürlükler”. **İstanbul Üniversitesi Hukuk Fakültesinin 50. Yıl Armağanı: Cumhuriyet Döneminde Hukuk** içinde. İstanbul: İstanbul Üniversitesi Yayınları, Yayın No: 1888, 1973.

Akın, İlhan. **Devlet Doktrinleri**. 3. Tıpkı Basım, İstanbul: Beta, 2016.

Akın, İlhan. **Kamu Hukuku**. İstanbul: Beta, 1993.

Akkanat Öztürk, Elif Beyza. “Rekabet Hukuku ve Veri Minimizasyonu: Sömürücü ‘Veri’ Uygulamaları”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Akkaya Kia, Rukiye. “‘Dikizleme’ Kültü ve ‘Unutuş’ Üzerine”, **Hukuk Kuramı**, Cilt. 7, No.1-2, Ocak-Ağustos 2020.

Akkaya Kia, Rukiye. “1876 Kanun-i Esasi’nin 18. Maddesi Üzerine”. **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.XV, Sayı.3-4, 2011.

Akkaya Kia, Rukiye. “Darülfünun’dan 1933 Üniversite Reformuna; Hukuk-i Siyasiye-i Osmaniye Derslerinden, Hukuk-i Âmme Derslerine Dönüşüm ve Genel Kamu Hukuku Dersinin Geçmişine Dair Notlar II”. **Journal of Istanbul University Law Faculty**. Cilt.70, No.1, 2012.

Akkaya Kia, Rukiye. “Devlet Sırrı, Kimin Sırrı?”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.19, No.2, 2013.

Akkaya Kia, Rukiye. “Doktor Lütfi Hakkında Zeyl ve ‘Fikr-i Islahât’ Eseri”, **Marmara Üniversitesi Hukuk Araştırmaları Dergisi**. Cilt.24, Sayı.2, Aralık 2018.

Akkaya Kia, Rukiye. “Hukukun Kadına Bakışı: Ergen ve Eşit Olamama Hali”. **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**. C.XIII, Sayı.1-2, 2009.

Akkaya Kia, Rukiye. “Mekân: Hukuk Fakültesi Apartmanı”. **Hukuk Kuramı**. Cilt.6, No.2, Mayıs-Ağustos 2019.

Akkaya Kia, Rukiye. “Post Modern Zamanlarda Machiavelli Okumak,” **Doç. Dr. Melike Batur Yamanerin Anısına Armağan** içinde. İstanbul: Galatasaray Üniversitesi Hukuk Fakültesi, 2014, ss.121-127.

Akkaya Kia, Rukiye. “Ulusal Ekonomi ve Girişimcilik Üzerine 1329 (1913) Tarihli ve Yazarı Belli Olmayan Bir Risale”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.24, No.2, Aralık 2018.

Akkaya Kia, Rukiye. “Uygarlık, Modernite ve Medeniyet Sözcüklerinin Hukuka Bakan Yüzü”. **Journal of Istanbul University Law Faculty**. Cilt.64, Sayı.2, 2011.

Akkaya Kia, Rukiye. **Moderniteden Postmoderniteye Egemenlik ve Hukuk**. İstanbul: Beta, 2006.

Akkaya Kia, Rukiye. **Bir Ders Konusu Olarak “Devlet” Ya Da Genel Kamu Hukuku Dersinin Kökenleri.** Genişletilmiş ve Gözden Geçirilmiş 2. Basım. İstanbul: Beta, 2016.

Akkaya, Rukiye. “Çözülen Sosyal Devlet ve Küreselleşme Olgusu”, **Prof. Dr. Necip Kocayusufpaşaoğlu için Armağan**, Ankara: Seçkin Yayınları, 2004.

Akkaya, Rukiye. “Devleti Öğretme Biçimi Olarak Siyaset Bilimi ve Fransa’daki Kökleri”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.26, Sayı.1, Haziran 2020, ss. 1-12.

Akkaya, Rukiye. “J. J. Rousseau’nun ‘Sosyal Sözleşme’ Eserinin Osmanlı Türkçesine İlk Tercümeleri II”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.26, Sayı.2, Aralık 2020.

Akkaya, Rukiye. “J.B. Bossuet: ‘Devlet Sizsiniz Majesteleri’!”. **GSÜHFD**. Cilt.2025, Sayı.2, 2025.

Akkaya, Rukiye. “Kamu Hukuku Eğitiminin Fransa’da Tarihsel Kökleri ve Kamu Hukuku Okulları Üzerine Notlar”. **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.VII, Sayı.3-4, 2003.

Akkaya, Rukiye. **Küreselleşme Olgusu Karşısında Ulus Sorunu**. İstanbul: Legal Yayıncılık, 2004.

Akkuş, Berkant, “Yapay Zekâ Tarafından İşlenilen Savaş Suçlarında Yazılımcının Sorumluluğu”, Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde. Ankara: Adalet, 2023, ss.623-648.

Aksoy, Suat. “Değişen Teknolojiler ve Endüstri 4.0: Endüstri 4.0’ı Anlamaya Dair Bir Giriş”, **SAV Katkı.** Cilt.Nisan, Sayı.4, 2017.

Altıner Yolcu, Fatma Zeynep. “Çocuğun Sosyal Medyada Ebeveynleri Tarafından Gerçekleştirilen Kişilik Hakkı İhlallerine Karşı Korunması”. Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.269-302.

Anayurt, Ömer. **Anayasa Hukuku Genel Kısım**. 5. Baskı, Ankara: Seçkin, 2022.

Anderson, Benedict. **Hayali Cemaatler: Milliyetçiliğin Kökenleri ve Yayılması**. İskender Savaşır (çev.), İstanbul: Metis Yayınları, 1995.

Andı, Simge. “Sahte Haberler ve Sosyal Medya: Yanlış Bilgi Yayılımında Algoritmaların Rolü”, **Algoritmaların Gölgesinde Toplum ve İletişim** içinde. Oğuz Kuş(drl.) Ankara: Alternatif Bilişim Derneği, 2021.

Andrews, Lori. **I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy**. New York: Free Press, 2012.

Antalya, Osman Gökhan. "Eşya Olarak Dijital Veriler: Dijital Eşya". **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.29, Sayı.2, (Aralık 2023), ss.1208-1222.

Ardıç, Zeynep. "Sosyal Medyaya İnsan Hakları Perspektifinden Bakış: İfade Özgürlüğünün Sınırlandırılması", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.251-268.

Ariel Aaronson, Susan ve Patrick Leblond, "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO". **Journal of International Economic Law**. Vol.21, No.2, June 2018. 247.

Arner, Douglas W., Jànos Barberis ve Ross P. Buckley. "FinTech, RegTech, and the Reconceptualization of Financial Regulation". **Northwestern Journal of International Law & Business**. Vol.37, No.3, 2017.

Arsène, Séverine. "Global Internet Governance in Chinese Academic Literature", **China Perspectives.** Vol.2, 2017.

Arslan, Cemil Caca. "Politik Hukukbilim Çerçevesinde Dijital Anayasacılık". **Muhafazakar Düşünce Dergisi**. Cilt.20, Sayı.67, 2024.

Artun, Emine Sevcan. "İnternet Ortamında Reklam Verenlerin Vergi Kesintisi Yapma Yükümlülükleri", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss. 513-530.

Artun, Emine Sevcan. "Kripto Madenciliği Sonucunda Ortaya Çıkan Enerji Tüketiminin Azaltılmasına Yönelik Mali Düzenleme Önerileri". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Aşkın, Uğur. “Bilişim Sistemleri Aracılığıyla İşlenen Kripto Para Dolandırıcılığı”, **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Atakan, Arda. “Putlaştırılmış Bir Kavram: Milli İrade”, **Marmara Üniversitesi Hukuk Fakültesi Mehmet AKAD’a Armağan** içinde. İstanbul: Der Yayınları, 2012, ss.143-276.

Atindande, M’Bawine. “Digital Communication in Africa at Crossroads: From Physical Exploitation in the Past to Virtual Dominance Now”, Kehbuma Langmia ve Agnes Lucy Lando (Ed.), **Digital Communications at Crossroads in Africa: A Decolonial Approach** içinde. Palgrave Pivot Cham, 2020, ss.41-70.

Aust Stefan ve Ammann Thomas. **Dijital Diktatörlük**. Erdinç Yücel ve Hasan Yılmaz (Çev.). Ankara: Hece Yayınları, 2018.

Aydeniz, Abdulsemet. “Enfokrasi: Dijitalleşme ve Demokrasinin Krizi”. **Medya Okuryazarlığı Araştırmaları Dergisi**. Cilt.2, Sayı.1, 2023.

Aydın, İlknur. “Suç Tahmini”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Aydınlı, İbrahim. “Yönetici Özeti”, İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya**. içinde. Vol.Ocak, Sayı.9, Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, ss.3-4.

Aytekin, Alper, Fatma Sönmez Çakır, Yakup Bahadır Yücel ve İlknur Kulaözü. “Algoritmaların Hayatımızdaki Yeri ve Önemi”. **Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi**. Sayı.5, No.7, 2018, ss.151-162.

Bacaksız, Pınar. “Deepfake (Yapay Video Montaj) Teknolojisinin Ortaya Çıkardığı Ceza Hukuku Sorunları”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Badur, Emel. “Dijital Çağda Çocuğun Unutulma Hakkı”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Balcı, Murat. “Yapay Zekâ ve Ayrımcılık: Anayasa Hukukunun Dönüşümü”, Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.). **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.367-390.

Balkır, Zehra Gönül. “Adalet Estetiği”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral’a Armağan**. Cilt.LXXII, Sayı.1, 2014.

Barendregt, Bart A., ve Florian A. Schneider, “Digital Activism in Asia: Good, Bad, and Banal Politics Online”. **Asiascape: Digital Asia**. Vol.7, No.1-2, 2020, ss.5-19.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace”. **Duke Law & Technology Review**. Vol.18, No.1, 2019.

Baron, David P. “Integrated Strategy: Market and Nonmarket Components”. **California Management Review**, Vol.37, No.2, 1995.

Başgil, Ali Fuad. “Devlet Nedir?: Realist Bir Tarif Denemesi”. **İstanbul Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.12, Sayı.4, 2011, ss.981-990.

Başgil, Ali Fuad. “Devletin Ülke Unsuru”. **İstanbul Hukuk Mecmuası**. Cilt.3, Sayı.4, 1947.

Batu, Mikail. “Sosyal Medya ve Dijital Toplumun Güvenliğine Yönelik Bir Tartışma”, İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya.** Cilt.Ocak, Sayı.9, 2021, ss.5-9.

Bellanova, Rocco, Kristina Irion, Katja Lindskov Jacobsen, Francesco Ragazzi, Rune Saugmann ve Lucy Suchman. “Toward a Critique of Algorithmic Violence”. **International Political Sociology**. Vol.15, No.1, 2021, ss.121-150.

Benabdallah, Lina. **Shaping the Future of Power: Knowledge Production and Network-Building in China-Africa Relations**. Ann Arbor: University of Michigan Press. 2020.

Berk, Mustafa Evren. "Dijital Çağın Yeni Teknolojisi 'Deepfake'". **OPUS Uluslararası Toplum Araştırmaları Dergisi**. Cilt.11, Sayı.18, 2020.

Biegel, Stuart. **Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace**. London: MIT Press, 2001.

Bingöl Schrijer, Bilge. "Vatandaşlık Hakkının Kapsamı ve Egemenlik İlişkisi Üzerine Bir Değerlendirme". **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi.** Cilt.XXII, Sayı.1, 2018.

Bodó, Balázs, Kristina Irion, Heleen Janssen ve Alexandra Giannopoulou. "Personal data Ordering in Context: the Interaction of Meso-Level Data Governance Regimes with Macro Frameworks", **Internet Policy Review**. Vol.10, No.3, 2021.

Bodó, Balázs, Natali Helberger, Kristina Irion, Frederik Zuiderveen Borgesius, Judith Moller, Bob van de Velde, Nadine Bol, Bram van Es ve Claes de Vreeseve. "Tackling the Algorithmic Control Crisis: the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents", **Yale Journal Of Law And Technology**. Vol.19, No.1, 2017.

Bratton, Benjamin H. **The Stack: On Software and Sovereignty**. Massachusetts: The MIT Press Direct, 2016.

Breining-Kaufmann, Christine. "The Legal Matrix of Human Rights and Trade Law: State Obligations Versus Private Rights and Obligations". Thomas Cottier, Joost Pauwelyn ve Elisabeth Burgi (Ed.). **Human Rights and International Trade** içinde. Oxford: OUP, (2005), ss.95-136.

Broeders, Dennis, Liisi Adamson ve Rogier Creemers. "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace", **The Hague Program For Cyber Norms Policy Brief**. Vol. November, 2019.

Bulut, Nihat. "Ölümüne Rekabetten Barış İçinde Yarışa: Hobbes'un Eşitlik Anlayışı", Prof. Dr. Abuzer Kendigelen (ed.). **Prof. Dr. Ömer Teoman'a 55. Yaş Günü Armağanı** içinde. İstanbul: Beta Yayınevi, 2002, ss.1377-1397.

Bulut, Nihat. "Sahte Bir Karşıtlığın Çözümü: Hukuk Devletinde Özgürlük Güvenlik İlişkisi". **Marmara Üniversitesi Hukuk Fakültesi Mehmet AKAD'a Armağan** içinde. İstanbul: Der Yayınları, 2012, ss.297-318.

Büyükçalık, Mürvet Ece. "Algoritmalar Ayrımcılık Yasağına Riayet Eder Mi?", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.). **Dijital Çağda Hukuk** içinde. Ankara: Adalet Yayınevi, 2023, ss.31-48.

Castells, Manuel. **Enformasyon Çağı: Ekonomi, Toplum ve Kültür Birinci Cilt: Ağ Toplumunun Yükselişi.** Ebru Kılıç (çev.). İstanbul: Bilgi Üniversitesi Yayınları, 2008.

Castells, Manuel. **Enformasyon Çağı: Ekonomi, Toplum ve Kültür İkinci Cilt Kimliğin Gücü**. Ebru Kılıç (çev.). İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2008.

Castells, Manuel. **Enformasyon Çağı: Ekonomi, Toplum ve Kültür Üçüncü Cilt Binyılın Sonu**. Ebru Kılıç (çev.), İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2008.

Chander, Anupam, Margot E. Kaminski ve William McGeveran, "Catalyzing Privacy Law", **Minnesota Law Review**. No.105, 2011.

Chander, Anupam. "How Law Made Silicon Valley", **Emory Law Journal**. Vol.63, No.3, 2014.

Cheney-Lippold, John. "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control: Soft Biopolitics and the Modulation of Control". **Theory, Culture & Society**. Vol.28, No.6, 2011.

Chorzempa, Martin. “Fintech in China: Trading off Growth and Risk, Innovation, and Control”, Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers., 2023, ss.83-100.

Christakis, Theodore. “‘European Digital Sovereignty’: Successfully Navigating Between the ‘Brussels Effect’ and Europe’s Quest for Strategic Autonomy”. SSRN, 2020, https://ssrn.com/abstract=3748098 (14 Aralık 2025).

Chrobak, Lennart. “Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law”, Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?** içinde. Springer Nature, 2018, ss.253-272.

Coche Eugenie ve Ans Kolk. “When digitalization meets regulation across borders: An explainer with actionable insights”. **AIB Insights**, Vol.24, No.3, 2024.

Cocito, Christina ve Paul De Hert, “United Nations: AI can pose risks to human rights and privacy”. **Privacy Laws & Business: International Reports**. 2021.

Coroado, Susana. “Leviathan vs Goliath or States vs Big Tech and What the Digital Services Act Can Do About It”. **Forum Transregionale Studien**. 2023.

Couture, Stephane ve Sophie Toupin, “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?”, **New Media & Society**. Vol.21, No.10, 2019.

Creemers, J.E.H. Rogier, “China’s Conception of Cyber Sovereignty: Rhetoric and Realization”, Dennis Broeders ve Bibi van den Berg (Ed.). **Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics** içinde. Lanham: Rowman & Littlefield, 2020, ss.107-142.

Creemers, Rogier J.E.H. “China’s Approach to Cyber Sovereignty”, **Konrad Adenauer Stiftung**, 2020,

https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty (11 Ocak 2026).

Creemers, Rogier J.E.H. "China's emerging data protection framework", **Journal of Cybersecurity.** Vol.8, No.1, 2022.

Creemers, Rogier J.E.H. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century", **Journal of Contemporary China**. Vol.26, No.103, 2017.

Creemers, Rogier J.E.H. "Disrupting the Chinese State: New Actors and New Factors", **Asiascape: Digital Asia**, Vol.5, No.3, 2018.

Creemers, Rogier J.E.H. "The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies", Nicholas Wright (Ed.), **Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives** içinde. Alabama: Air University Press, 2018, ss.129-135.

Creemers, Rogier J.E.H. "Uneven coverage and blank spaces: bringing the state back in", **Asiascape: Digital Asia**. Leiden, Vol.10, No.1-2, 2023.

Creemers, Rogier J.E.H. **The Ideology Behind China's AI Strategy**. London: Nesta, 2020.

Creemers, Rogier. "Cybersecurity Law and Regulation in China: Securing the Smart State". **China Law and Society Review**. Vol.6, 2023.

Creemers, Rogier. "The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy". **Journal of Contemporary China**. Vol.33, No.146, 2024.

Creemers, Rogier. "The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Age", Jacques deLisle, Avery Goldstein ve

Guobin Yang (ed.), **The Internet, Social Media, and a Changing China** içinde. Philadelphia: University of Pennsylvania Press, 2016, ss.86-105.

Culpepper, Pepper D. ve Kathleen Thelen. "Are We All Amazon Primed? Consumers and the Politics of Platform Power", **Comparative Political Studies**. Vol.53, No.2, 2020.

Çakır, Kerim. "Sosyal Ağlarda Siber Zorbalık ve Ceza Hukuku", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.). **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.235-250.

Çalgan, Kemal. **Kapitalizmin Egemenlik Yapısı ve Dijital Tahakküm**. Ankara: Klaros Yayınları, 2023.

Çekin, Mesut Serdar. "Dijital Çağda Anayasa Yargısı: Özel Hukuk Perspektifinden Bir. İnceleme". **Anayasa Yargısı**. Cilt.42, Sayı.1, 2025.

Çelik Muharrem ve Muhammed Beheşti Aydoğan. "Sosyal Medyada Hukuku Yerleşik Kılma Çabaları", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.). **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.303-323.

Çevik, Nevzat. "'Panta Rei - Her Şey Akar' Mı?". **Son Nokta Dergisi**. Sayı.30, 2007.

Danowski, Mei. "Becoming a Cyber Superpower: China Builds Offensive Capability with Military, Government, and Private Sector Forces", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.). **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers. 2023, ss.171-196.

Deleuze, Gilles. "Postscript on the Societies of Control." **October**, Vol.59, 1992, ss. 3-7.

Demir, İbrahim ve Fatih Cemil Özbuğday, "Siber Güvenlik Bağlamında Sosyal Medya Platformları Ekonomisi ve Endüstriyel Organizasyonu", İbrahim Demir (Ed.),

Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya içinde, Vol.Ocak, Sayı.9, Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, 2021, ss.10-17.

Demir, Remzi. "Konut ve Çatılı İşyeri Kira Sözleşmelerinde, Akıllı Sözleşme Sisteminin Uygulanabilirliği". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Demircioğlu, Murat. "Günümüz Endüstriyel İlişkilerinde Çokuluslu Şirketlerin Etkileri", **Prof. Dr. Kenan Tunçomağ'a Armağan**, İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Eğitim, Öğretim ve Yardımlaşma Vakfı Yayını, Yayın No: 4, 1997, ss. 101-115.

Dikmengil, Nil. "Siber-Ulus: Dijital Egemenlik Alanı ve Barbados'un Metaverse Elçiliği", Aslı Şen Taşbaşı, Bahadır Er, Erol Ülker ve Özlem Kayhan Pusane (ed.), **Dünyada Birey, Toplum, Siyaset Kongresi Bildiri Kitabı** içinde. İstanbul: Işık Üniversitesi Yayınları, 2022, ss.170-182.

Dinçkol, Bihterin. "Atina Demokrasisinden Roma Cumhuriyetine – 'Demos'tan 'Populus Romanus'a", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.23, Sayı.3, 2017.

Dinçkol, Bihterin. "Yönetilenlerin 'Öz' Yönetimi-Kamuoyu". **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**. Cilt.5, No.10, Güz 2006/2, 2006.

Dirlik, Arif. **Küresel Modernite: Küresel Kapitalizm Çağında Modernite**. Ahmet Fethi Yıldırım (çev.), İstanbul: Akademim Yayınları, 2024.

Dirlik, Arif. **Küreselleşmenin Sonu Mu?** İsmail Kovacı ve Veysel Batmaz (çev.), İstanbul: Ayrıntı Yayınları, 2012.

Dirlik, Arif. **Postkolonyal Aura: Küresel Kapitalizm Çağında Üçüncü Dünya Eleştirisi.** Galip Doğduaslan (çev.). İstanbul: Boğaziçi Üniversitesi Yayınevi, 2010.

Doehring, Karl. **Genel Devlet Kuramı (Genel Kamu Hukuku).** Ahmet Mumcu (çev.). İstanbul: İnkılap Kitabevi, 2019.

Dorwart, Hunter. "China and Global Data Transfers Implications for Future Rulemaking", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers., 2023, ss.123-152.

Döner, Ayhan. "Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler". **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.26, Sayı.1, (Haziran 2022).

Dönmez, Hakan. "Şirketin Doğasına İlişkin Teorilere Göre DOA'ların (Merkezsiz Özerk Kuruluş) Konumu". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Dönmezer, Sulhi. "Devletin Ülkesi ve Millî ile Bütünlüğü ve Bölünmezliği İlkesi". **İstanbul Üniversitesi Hukuk Fakültesinin 50. Yıl Armağanı: Cumhuriyet Döneminde Hukuk** içinde. İstanbul: İstanbul Üniversitesi Yayınları, Yayın No: 1888, 1973.

Drexl, Josef. "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", Alberto Di Franceschi ve Reiner Schulze (Ed.), **Digital Revolution - New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies** içinde. H. Beck; Nomos, 2019, ss.19-41.

Drucker, Peter F. **Kapitalist Ötesi Toplum.** Belkıs Çorakçı (çev.), İstanbul: İnkılap Yayınları, 1994.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**. İstanbul: Seçkin Yayınları, 2014.

Dülger, Muzaffer. "Homo Commoditus: 'Sahip Olmak, Genetik Metalar ve Fikri Mülkiyet'", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan**, Cilt.LXXII, Sayı.1, 2014.

Dyson, George. **Turing's Cathedral: The Origins of the Digital Universe**. New York: Pantheon, 2013.

Ecemiş Yılmaz, Hatice Kübra. "Siber Uzay, Siber Güvenlik, Dijital Egemenlik Kavramlarının Uluslararası Hukuk Bağlamında Değerlendirilmesi", İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya**, Cilt.Ocak, Sayı.9, 2021, ss.21-26.

Eger, John M. "Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?". **Law and Policy in International Business**. Vol.10, No.4, 1978.

Ekman, Alice. "China's Blockchain and Cryptocurrency Ambitions: The First-Mover Advantage", **European Union Institute for Security Studies**, 13 Temmuz 2021, https://www.iss.europa.eu/content/chinas-blockchain-and-cryptocurrency-ambitions#_introduction/ (1 Şubat 2026)

Emir, Nergiz. "Siber Operasyonlar ve Özen Yükümlülüğünün İhlalinden Devletin Sorumluluğu", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.61-74.

Erdoğan, Ali. "We Likened Them To Ourselves: Algorithmic Discrimination And Bias". **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Erdoğdu, Semih. "Yapay Zekâ Rekabeti Bağlamında Çin'in Ontolojik Güvenlik Algısı", **Uluslararası Hukuk ve Sosyal Bilim Araştırmaları Dergisi**, Cilt.3, Sayı.2, 2021.

Eren, Abdurrahman. “Dijital Egemenlik Kavramı ve Anayasa Mahkemesinin Dijital Egemenliğe Yaklaşımı”. **Anayasa Yargısı**. Cilt.42, Sayı.1, 2025, ss.557-582.

Ergin, Ergül. **Siber Güvenlik Hukuku Temel Mevzuatı**, Ankara: Adalet Yayınları, 2025.

Ergin, Ergül. **Yapay Zekâ ve Hukuk**. Ankara: Adalet Yayınevi, 2025.

Erol, Ömer Faruk. **Algoritmik Regülasyon: Yapay Zekâ ve İdarenin Regülasyon Faaliyeti**. İstanbul: On İki Levha Yayıncılık, 2023.

Erözden, Ozan. **Ulus-Devlet**. 3. Basım, İstanbul: On İki Levha Yayıncılık, 2013.

Erturan, Ela. “Veri Sorumlusunun Siber Tehditleri ve İnternet Dolandırıcılığını Önlemek Amacıyla ‘Başkalarının’ Kişisel Verilerini İşlemesinin ‘Meşru Menfaat’ Kapsamında Değerlendirilmesi Meselesi”. **Prof. Dr. Sabih Arkan’a Armağan.** İstanbul: On İki Levha Yayıncılık, 2019.

Eugène, Enriquez. **Sürüden Devlete**. Nilgün Tutal Cheviron (çev.). İstanbul: Ayrıntı Yayınları, 2019.

Evren, Mehmet. “Jean Jacques Rousseau’da Bilim ve Sanatın Yeri”. **Tabula Rasa Felsefe & Teoloji Dergisi**. No.35, 2020.

Fabiano, Nicola. “Digital Sovereignty Between Accountability and the Value of Personal Data”. **Advances in Science, Technology and Engineering Systems Journal**. Vol.5, No.3, 2020.

Ferdinand, Peter. “The Internet, Democracy And Democratization”. **Democratization**. Vol.7, No.1, 2000.

Fırat, Muhammed Sabır. “Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu”. **Hacettepe Hukuk Fakültesi Dergisi**. Cilt.5, No.2, 2015.

Floridi, Luciano. “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU”. **Philosophy & Technology**. Vol.33, No.3, 2020.

Fuchs, Christian. “Baidu, Weibo and Renren: the global political economy of social media in China”. **Asian Journal of Communication**. Vol.26, No.1, 2015.

Gábriš, Tomáš ve Ondrej Hamuľák. “Pandemics in Cyberspace: Empire in Search of a Sovereign?”, **Baltic Journal of Law & Politics**. Vol.14, No.1, 2021.

Ganascia, Jean-Gabriel, Eric Germain ve Claude Kirchner, “Sovereignty in the Digital Age: Keeping Control Over Our Choices and Values”, CERNA, 2018, https://www.allistene.fr/files/2019/05/55817_Sovereignty_CERNA_2018.pdf (11 Ocak 2026).

Geçer, Ahmet Emrah. “Kripto Varlıkların Vergilendirilmesi Üzerine Düşünceler”, Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.553-572.

Gerards, Janneke. “The fundamental rights challenges of algorithms”. **Netherlands Quarterly of Human Rights**. Vol.37, No.3, 2019.

Giddens, Antony. **Ulus Devlet ve Şiddet**. Cumhur Atay (çev.), İstanbul: Kalkedon Yayınları, 2008.

Gillespie, Tarleton. “The Relevance of Algorithms”. Tarleton Gillespie, Pablo J. Boczkowski ve Kirsten A. Foot (Ed.). **Media Technologies: Essays on Communication, Materiality, and Society** içinde. Massachusetts: The MIT Press, 2014, ss.167-193.

Gillespie, Tarleton. **Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media**. Connecticut: Yale University Press, 2018.

Goodwin, Tom. **Digital Darwinism: Surviving the new age of business disruption**. 2nd edition, London: Kogan Page Inspire, 2022.

Gourley, Stephen K. "Cyber Sovereignty", Panayotis A. Yannakogeorgos ve Adam B. Lowther (Ed.). **Conflict and Cooperation in Cyberspace: The Challenge to National Security** içinde. Florida: Taylor & Francis, 2014, ss.277-290.

Göze, Ayferi. **Siyasal Düşünceler ve Yönetimler**. Tıpkı 18. Bası, İstanbul: Beta, 2020.

Gözler, Kemal. "Kişilik Haklarını İhlal Eden İnternet Yayınlarının Kaldırılması Usulü ve İfade Hürriyeti: 5651 Sayılı Kanun'un 9'uncu Maddesinin İfade Hürriyeti Açısından Değerlendirilmesi". **Rona Aybay'a Armağan** içinde. İstanbul: Legal, c.I, 2014.

Granger, Marie-Pierre ve Kristina Irion. "The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection", **European Law Review**. Vol.39, No.6, 2014.

Granger, Marie-Pierre ve Kristina Irion. "The right to protection of personal data: The new posterchild of European Union citizenship?", Sybe de Vries, Henri de Waele ve Marie Pierre Granger (Ed.). **Civil Rights and EU Citizenship: Challenges at the Crossroads of the European, National and Private Spheres** içinde. Cheltenham: Edward Elgar Publishing. 2018, ss.279-302.

Griffiths, James. **The Great Firewall of China: How to Build and Control an Alternative Version of the Internet**. London: Zed Books. 2019.

Gritsenko, Daria ve Matthew Wood. "Algorithmic governance: A modes of governance approach". **Regulation & Governance**. Vol.16, 2022.

Güney, Necmeddin ve Ömer Faruk Tekdoğan. "Merkez Bankası Dijital Paralarının (Mbdp) İslam Hukuku Açısından Değerlendirilmesi". **Uluslararası Dijital Çağda Hukuk Sempozyumu**, İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Gürbüz, Ahmet. "Günümüz Batılı Politik Yaklaşımların Kökeni Olarak İngiliz Yararcılığı/Utilitarianism". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan**. Cilt.LXXII, Sayı.1, 2014.

Habermas, Jürgen. **Kamusal Alanın Yapısal Dönüşümü**. İstanbul: İletişim, 2003.

Hadi, Muhammad Jawad. "Digital Battlegrounds: Data Sovereignty and Regulatory Challenges in Armed Conflicts", SSRN, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4608863 (14 Aralık 2025).

Han, Byung-Chul. **Enfokrasi: Dijitalleşme ve Demokrasinin Krizi**. Mustafa Özdemir (çev.). İstanbul: Ketebe, 2022.

Harari, Yuval Noah. **Homo Deus: Yarının Kısa bir Tarihi.** Poyzan Nur Taneli (çev.), İstanbul: Kolektif Kitap, 2016.

Hardt, Michael ve Antonio Negri. **Çokluk: İmparatorluk Çağında Savaş ve Demokrasi,** Barış Yıldırım (çev.), İstanbul: Ayrıntı Yayınları, 2004.

Hardt, Michael ve Antonio Negri. **İmparatorluk**. Abdullah Yılmaz (çev.), İstanbul: Ayrıntı Yayınları, 2003.

Haskel, Jonathan ve Stian Westlake. **Capitalism Without Capital: The Rise of the Intangible Economy**. Princeton: Princeton University Press, 2017.

Hatipoğlu Aydın, Duygu. **Siber Alan ve Hukuk**. İstanbul: On İki Levha Yayıncılık, 2022.

Herzog, Don. **RIP Sovereignty**. New Haven: Yale University Press, 2020.

Hillman, Amy J. ve Michael. A. Hitt, "Corporate Political Strategy Formulation: A Model of Approach, Participation, and Strategy Decisions". **Academy of Management Review**, Vol.24, No.4, 1999.

Hobsbawm, Eric. **1780'den Günümüze Milletler ve Milliyetçilik: "Program, Mit, Gerçeklik".** Osman Akınhay (çev.), İstanbul: Ayrıntı Yayınları, 2010.

Hummel, Patrik, Matthias Braun, Max Tretter ve Peter Dabrock. "Data sovereignty: A review", **Big Data & Society**. Vol.8, No.1, 2021.

Irion, Kristina ve Natalie Helberger. "Smart TV and the online media sector: User privacy in view of changing market realities", **Telecommunications Policy**. Vol.41, No.3, 2017.

Irion, Kristina, Mira Burri, Ans Kolk ve Stefania Milan. "Governing 'European values' inside data flows: Interdisciplinary perspectives". **Internet Policy Review**. Vol.10, No.3, 2023.

Irion, Kristina. "A special regard: The Court of Justice and the fundamental rights to privacy and data protection" U. Faber ve Diğerleri (Ed.), **Gesellschaftliche Bewegungen-Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte** içinde. Nomos, 2016, ss.873-890.

Irion, Kristina. "Government Cloud Computing and National Data Sovereignty". **Policy and Internet**. Vol.4, No.3-4, 2012.

Irion, Kristina. "Panta rhei: A European Perspective on Ensuring a High Level of Protection of Digital Human Rights in a World in Which Everything Flows", Mira Burri (Ed.). **Big Data and Global Trade Law** içinde. Cambridge: Cambridge University Press, 2021, ss.231-242.

Irion, Kristina. "Separated Together: The International Telecommunications Union and Civil Society". **International Journal of Communications Law and Policy**. Vol.13, 2009.

Irion, Kristina. "Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms The (Legal) Relationship Between Individuals And Their Personal Records". **International Journal of Law and Information Technology**. Vol.23, No.4, 2015, ss.348-371.

Işık, Alper. **İnternet Aktörleri ve Egemenliğin Değişen Boyutları**. Güncellenmiş 2. Baskı, İstanbul: On İki Levha Yayıncılık, 2025.

Işıktaç, Yasemin. "İrade Özgürlüğüne Giriş Açısından 'Ben İnşâsı'". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan**. Cilt.LXXII, Sayı.1, 2014.

Ivic, Sanja ve David Ramiro Troitiño. "Digital Sovereignty and Identity in the European Union: A Challenge for Building Europe", **European Studies: the Review of European law, Economics and Politics,** Vol.9, No.2, 2022.

İçel, Kayıhan. "Cumhuriyetimizin 75. Yılında Türk Ceza Hukuku ve Globalleşme", **Cumhuriyetin 75. Yılı Armağanı** içinde. İstanbul: İstanbul Üniversitesi Yayınevi, 1999.

Janssen, Heleen, Jennifer Cobbe, Chris Norval ve Jatinder Singh, "Decentralized data processing: personal data stores and the GDPR". **International Data Privacy Law**. Vol.10, No.4. 2020, ss. 356-384.

Kabadayı, Talip. "Felsefenin Işığında '(Haklı) Savaş' Üzerine Kısa Bir Deneme". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan**, Cilt.LXXII Sayı.1, 2014.

Kama Işık, Sezen. "Klasik Anayasacılıktan Dijital Anayasacılığa: Anayasa Hukukunun Dönüşümü", Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.75-96.

Kapani, Münci. **Politika Bilimine Giriş.** 59. Baskı, Ankara: Serbest Akademi, 2020.

Kaplanhan, Fatih. "Dijitalleşme, Vergi ve Egemenlik Sorunu". **Bilişim Teknolojileri ve İletişim: Birey ve Toplum Güvenliği**, 2020.

Kaplanhan, Fatih. "Türkiye'de Sosyal Medyanın Vergilendiril(eme)mesi ve Çözüm Önerileri: Google, Facebook, Twitter Örneği". **Turkish Journal of Police Studies/Polis Bilimleri Dergisi**. Vol.18, Sayı.3, 2016.

Kara, Serenay, Alp Limoncuooğlu ve Zeynep Şişli. "Dijitalleşen Çalışma Hayatında İşçinin Ulaşılamama Hakkı". Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.). **Dijital Çağda Hukuk** içinde. Ankara: Adalet Yayınevi, 2023, ss.357-368.

Karagöz, Kezban. "Yeni Medya Çağında Dönüşen Toplumsal Hareketler ve Dijital Aktivizm Hareketleri". **İletişim ve Diplomasi**. No.1, 2013.

Karakoç, Elif. "Algoritmalardaki Cinsiyet Yanlılığına Queer Teori Perspektifinden Bakmak", **Algoritmaların Gölgesinde Toplum ve İletişim**, Oğuz Kuş (drl.), Ankara: Alternatif Bilişim Derneği, 2021.

Karataş, Hacer Gizem. "Mossad'ın Çağrı Cihazı Operasyonunun Silahlı Çatışma Hukukunun Temel İlkeleri Bakımından Değerlendirilmesi". **GSÜHFD**. Cilt.2025, No.2, 2025.

Karatay, Akın. "Bilişim ve Teknoloji Şirketlerinin İnsan Hakları Sorumluluklarına İlişkin Güncel Gelişmeler". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Karaturp, Aydıner ve Nüket Evrim "Nitelikli Fikri Tapu (NFT) ve Telif Hakkı", **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Karl Marx ve Friedrich Engels. **Komünist Parti Manifestosu.** Eriş Yayınları, https://www.antikapitalist.net/kutuphane/acik-kitaplik/marxengels/manifesto.pdf (23.01.2026).

Karmutoğlu, Başak. "Telif Hakkında Orijinallik Ölçütü ve Bunun Yapay Zekâ Tarafından Meydana Getirilen Eserler Açısından Değerlendirilmesi". **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.2025, Sayı.2, 2025.

Kaya, İpek. "Enfokrasi: Dijitalleşme ve Demokrasi Krizi". **Kocaeli Üniversitesi İletişim Fakültesi Araştırma Dergisi**. Cilt.23, Sayı.66, 2024.

Kelsen, Hans. **Saf Hukuk Kuramı: Hukuk Kuramının Sorunlarına Giriş**. Ertuğrul Uzun (çev.), İstanbul: Nora Kitap, 2020,

Ketizmen, Muammer. **Türk Ceza Hukukunda Bilişim Suçları**. İstanbul: Adalet, 2008.

Kılıç, Muharrem. "Bilgi-İktidar İlişkisi Bağlamında Yasa Düşüncesi: İktidarın Yasa(l)laşması". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan**. Cilt.LXXII, Sayı.1, 2014.

Kırca, Ali Coşkun. "Devlet ve Üniversite (Bir Reform Taslağının Anahatları)", **İnan Kıraç'a Armağan**. İstanbul: Galatasaray Üniversitesi Yayınları, Yayın No: 1, 1994.

Kıvılcım, Fulya. "From 1980 on, the Impact of the Globalization on Democracy and Nation State Concept: Turkey Evaluation", **Journal of Social and Administrative Sciences**. Vol.4, No.2, Haziran 2016.

Kia, Rukiye Akkaya. "'Körleşme' Üzerine (2)". **Hukuk Kuramı**. Cilt.5, Sayı.3, (Eylül-Aralık 2018).

Kirkit, Ecem. "Deepfake Teknolojisi Karşısında Kişinin Kişilik Hakkının ve Kişisel Verilerinin Korunması". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Kitapçıoğlu Yüksel, Tülay. "Halkı Yanıltıcı Bilgiyi Alenen Yayma Suçu Hakkında Değerlendirme". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Kleinwacher, Wolfgang. "Beyond ICANN Vs ITU? How WSIS tries to enter the new territory of Internet governance". **The International Journal for Communication Studies**. Vol.66, No.3-4, 2004.

Kontoğlu Taştan, Sena. "Dijital Hizmetler Yasası'nda (DSA) Dezenformasyonla Mücadeleye Yönelik Davranış Kuralları." **Bilişim Hukuku Dergisi**. Cilt.7, Sayı.2, 2025.

Kosinski, Michal, David Stillwell ve Thore Graepel, “Private traits and attributes are predictable from digital records of human behavior”, **Proceedings of the National Academy of Sciences of the United States of America**, Vol.110, No.15, 2013.

Kriegel, Blandine. **Klasik Siyasi Felsefe Metinleri**. Zühre İlkgelen (çev.). İstanbul: İletişim Yayınları, 2010.

Kshetri, Nir. "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution". **Telecommunications Policy**, Vol.37, No.4, 2013.

Kurt, Sümeyra Sena. “Genel Veri Koruma Tüzüğü (GDPR) Çerçevesinde Veri Sahibinin Otomatik Karar Verme Mekanizmaları Karşısındaki Hakları”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Kuş, Oğuz. “Algoritmaları Dehümanizasyon Kavramı Çerçevesinde Tartışmak”, Oğuz Kuş(drl.), **Algoritmaların Gölgesinde Toplum ve İletişim** içinde. Ankara: Alternatif Bilişim Derneği, 2021.

Kuzu, Berçin. “Dijital Çağda İnsan Haklarının Gelişimi”. Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.). **Dijital Çağda Hukuk** içinde. Ankara: Adalet Yayınevi, 2023, ss.143-156

Kühling, Jürgen. “Germany: The Right to Be Forgotten”. Franz Werro (Ed.), **The Right To Be Forgotten: A Comparative Study of the Emergent Right’s Evolution and Application in Europe, the Americas, and Asia** içinde. Springer, 2020, ss.125-140.

Küzeci, Elif. **Sayısal Fil**. 1. Baskı, İstanbul: İnkılap Kitapevi, 2021.

Lefebvre, Henry. “The Production of Space”. Jen Jack Gieseking ve Diğerleri (ed.). **The people, place, and space reader** içinde, New York and London: Routledge, 2014, ss.289-293.

Lehdonvirta, Vili. **Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control**. London: The MIT Press, 2022.

Leiser, Mark ve Andrew Murray. "The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies", Roger Brownsword, Eloise Scotford ve Karen Yeung (Ed.) **The Oxford Handbook of Law, Regulation and Technology** içinde. Oxford: Oxford Academic, 2017. ss.1-35.

Lessig, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

Liaropoulos, Andrew. "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics". **Journal of Information Warfare**, Vol.15, No..4, 2016.

Linklater, Andrew. **Critical Theory and World Politics**. London: Routledge, 2007.

Lippmann, Walter. **Hayalet Kamu**. Cem Evrim Aslan (çev.), İstanbul: Kabalcı Yayınevi, 2024.

Locke, John. **Yönetim Üzerine İki İnceleme.** Ömer Saruhanlıoğlu (çev.). İstanbul: Litera Yayıncılık, 2020.

Locke, John. **Yönetim Üzerine İkinci İnceleme: Sivil Yönetimin Gerçek Kökeni Boyutu ve Amacı Üzerine Bir Deneme**. Fahri Bakırcı (çev.), Ankara: Ebabil Yayınları.

Luke, Timothy W. "Digital Citizenship", Phillip Kalantzis-Cope ve Karim Gherab-Martín (Ed.), **Emerging Digital Spaces in Contemporary Society: Properties of Technology**, içinde. London: Palgrave & Macmillan, 2010, ss.83-96.

Lupton, Deborah. **Digital Sociology**. New York: Routledge, 2015.

Mayer-Schönberger, Victor ve David Lazer, "From Electronic Government to Information Government" Victor Mayer-Schönberger ve David Lazer (ed.),

Governance and Information Technology içinde. Cambridge, MA: MIT Press, 2007, ss.1-14.

Metin, Sevtap. "Oyun Teorileri Işığında Thomas Hobbes'un Sosyal Sözleşme Kuramının Analiz ve Yorumu". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral'a Armağan.** Cilt.LXXII, Sayı.1, 2014.

Moeller, Judith, Damian Trilling, Natali Helberger, Kristina Irion ve Claes De Vreese. "Shrinking core? Exploring the differential agenda setting power of traditional and personalized news media". **Digital Policy, Regulation and Governance**. Vol.18, No.6, 2016, ss.26-41.

Morris, Carwyn, Andy Hanlun Li ve Lotus Ruan, "Covid origins, nationalism, and diasporic heterogeneity: China, Chineseness, and Covid-19", Michael Butter ve Peter Knight (Ed.). **Covid Conspiracy Theories in Global Perspective** içinde. London: Routledge, 2023, ss.43-57.

Mueller, Milton L. **Networks and States: The Global Politics of Internet Governance**. Massachusetts: MIT Press, 2010.

Mutlu, Muhammet Sefa. **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**. İstanbul: Adalet, 2020.

Nagan, Winston P. ve Craig Hammer, "The Changing Character of Sovereignty in International Law and International Relations", **Columbia Journal of Transnational Law**. Vol.39, 2004.

Nal, Sabahattin. "Karşılaştırmalı Hukukta Enformasyon Hakkı". **Prof. Dr. Necip Kocayusufpaşaoğlu için Armağan**. Ankara: Seçkin Yayınları, 2004.

Negro, Gianluigi. "China and Global Internet Governance ITU, ICANN, and the World Internet Conference", Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers, 2023, ss.153-170.

Nomer, Ergin. “Türk Vatandaşlık Hukukunun Genel İlkeleri”, **Cumhuriyetin 75. Yılı Armağanı** içinde, İstanbul: İstanbul Üniversitesi Yayınevi, 1999.

Ocelík, Václav, Ans Kolk ve Kristina Irion. “Shifting battlegrounds: Corporate Political Activity in the General Data Protection Regulation”. **Business & Society**.

Okandan, Recai Galip. “Devletin İktidar Unsurunun Vasıfları ve Bu Hususta Sürülen Doktrinler”. **Journal of Istanbul University Law Faculty**. Vol.16, No.3-4, 2011.

Okandan, Recai. “Devletin Beşerî Unsuru”. **İstanbul Hukuk Mecmuası**. Cilt.13, Sayı.4, 1947.

Okandan, Recai. “Devletin Fiziki Unsuru”. **Journal of Istanbul University Law Faculty**. Cilt.14, Sayı.1-2, Eylül 2011.

Okandan, Recai. “Devletin Tarihi Menşeini Kuvvet ve Mücadelede Bulan Muhtelif Görüşler”, **İstanbul Hukuk Mecmuası**. Cilt.9, Sayı.3, 1944, ss. 495-515.

Oostveen, Manon ve Kristina Irion. “The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?” Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?** içinde. Springer Nature, 2018, ss.7-26.

Ozan Özparlak, Başak. **Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme**. İstanbul: On İki Levha, 2021.

Önay Koçoğlu, Fatma ve Çiğdem Selçukcan Erol. “Algoritma”, Nilgün Bozbuğa ve Sevinç Gülseçen (Ed.) **Tıp Bilişimi** içinde. İstanbul: İstanbul Üniversitesi Yayınları, 2021, (Bölüm 13).

Özcan, Mehmet Tevfik. "Hukuk Olgusunun Sosyolojik Elemanları", **Mahmut R. Belik'e Armağan** içinde. İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Yayını, (1993).

Özdemir, Ali Murat, Muammer Ketizmen, Abdurrahman Saygılı, Hamdi Gökçe Zabunoğlu, Ebubekir Aykut, Göksu Uğurlu, Aynur Demirli, Ezgi Nur Türkoğlu Karacaova ve Ozan Giray Şahin. **Genel Kamu Hukuku: Kuramsal Yaklaşımlar**. 2. Baskı, Ankara: İmge Kitabevi, 2020.

Özdemir, Berceste Gülçin. "Yürümek Bir Devrimdir: Henry David Thoreau'nun Yürümeye Dair Felsefesi ile Heraklitos'un Ateşe Atfettikleri Bağlamında The Way Filmi". **SineFilozofi**. Cilt.7, Özel Sayı.4.

Özdemir, Şebnem. "Post-Panoptikon Çağı: Gözetimin Dijitalleşmesi ve Çevrimiçi Kimliğin Gizliliği Üzerine Bir Analiz". **Anadolu Üniversitesi Sosyal Bilimler Dergisi**. Cilt.20, Sayı.3, 2020.

Özen, Tuğçe. "Dijital Çağın Yarattığı Yeni Bir Fenomen: Dijital Şiddetin Türü Olarak Israrlı Takip". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Özkan, Zeynep Aslı. "Üretken Yapay Zekâ Çıktılarının Fikrî Mülkiyet Hukuku Kapsamında Değerlendirilmesi: Güncel Kararlar Işığında Bir İnceleme", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**. Cilt.2025, Sayı.2, 2025.

Özlem, Doğan. "Ahlakta, Hukukta ve Siyasette Özgürlük Kavramı Üstüne", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. Vecdi Aral'a Armağan,** Cilt.LXXII Sayı.1, 2014.

Özyiğit, Sinem ve Bengi Baydan. "Telif Hukuku Ekseninde Deepfake", Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde. Ankara:Adalet Yayınevi, 2023, ss.567-582.

Papagianneas, Straton ve Adam Knight, "The Stumbling Smart State Fragmented Policy Experimentatio and Dubious Consolidation", Rogier J.E.H. Creemers, Straton

Papagianneas ve Adam D. Knight (Ed.), **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers., 2023, ss.35-52.

Parviainen, Päivi, Maarit Tihinen, Jukka Kääriäinen ve Susanna Teppola. "Tackling the Digitalization Challenge: How to Benefit From Digitalization in Practice", **International Journal of Information Systems and Project Management**. Vol.5, No.1, 2017, ss.63-77.

Pasquale, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information**. Cambridge: Harvard University Press, 2016.

Penrose, Roger. **Bilgisayar ve Zekâ: Kralın Yeni Usu, Cilt 1**. Tekin Dereli (çev.). Ankara: Gökçe Ofset, 1997.

Pierson, Christopher. **Modern Devlet**. Burcu Erdoğan (çev.), Ankara: Chiviyazıları Yayınevi, 2015.

Pohle, Julia ve Thorsten Thiel, "Digital Sovereignty", **Internet Policy Review**. Vol.9, No.4, 2020.

Polat, Mehmet Bahadır. "Blokzincir Üzerinde Bulunan 'Mixer' Protokollerinde Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Fiili Bağlamında Objektif İsnadiyet Değerlendirmesi". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Purtova, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law", **Law, Innovation and Technology**. Vol.10, No.1, 2018.

Reed, Chris. "Information 'Ownership' in the Cloud", Queen Mary School of Law Legal Studies, Research Paper No. 45/2010, 2010, https://ssrn.com/abstract=1562461 (1 Ocak 2026).

Reidenberg, Joel R. "Lex Informatica: The Formulation of Information Policy Rules through Technology", **Texas Law Review**. Vol.76, 1997.

Reidenberg, Joel R. “Yahoo and Democracy on the Internet”. **Jurimetrics**. Vol.42, No.261, (2001-2002).

Reinicke, Wolfgang H. **Global Public Policy: Governing without Government?** Washington, D.C.: Brookings Institution Press, 1998.

Renan, Ernest. **Ulus Nedir?** Gökçe Yavaş (çev.), İstanbul: Pinhan Yayıncılık, 2016.

Roberts, Huw, Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo ve Luciano Floridi. “Safeguarding European Values with Digital Sovereignty: an Analysis of Statements and Policies”, **Internet Policy Review**. Vol.10, No.3, 2021.

Rousseau, Jean Jacques. **Bilimler ve Sanatlar Üzerine Söylev**. İstanbul: Türkiye İş Bankası Kültür Yayınları, 2007.

Rousseau, Jean Jacques. **Toplum Sözleşmesi**. İstanbul: Türkiye İş Bankası Kültür Yayınları, 2012.

Rouvroy, Antoinette ve Thomas Berns. “Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships?” **Réseaux**. Cilt.2013/1, No.177, 2013.

Rühlig, Tim. “China: A Technical Standardisation Power?”, Rogier J.E.H. Creemers, Straton Papagianneas ve Adam D. Knight (Ed.). **The Emergence of China's Smart State** içinde. Maryland: Rowman & Littlefield Publishers., 2023, ss.103-122.

Saka, Erkan. “Polislik Algoritmaları Bağlamında Öngörücü Algoritmalara (Predictive Algorithms) Eleştirel Bir Yaklaşım”, Oğuz Kuş (Ed.), **Algoritmaların Gölgesinde Toplum ve İletişim** içinde., Ankara: Alternatif Bilişim Derneği, 2021, ss.81-98.

Sala, Bedir. “Dijital Çağda Devlet Egemenliğini Tartışmak: Dijital Feodalizm”, **SDE Akademi Dergisi**. Cilt.5, Sayı.3, ss.373-399.

Sarıgül, Ali Tanju. “Kişisel Verilerin Korunmasına Yönelik Suçlarla Korunan Hukuki Değer”. Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.). **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.501-512.

Saygılı, Abdurrahman. “Jean Bodin'in Egemenlik Anlayışı Çerçevesinde Kralın İki Bedeni Kuramına Kısa Bir Bakış”. **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.63, Sayı.1, 2014.

Saygılı, Abdurrahman. “Modern Devlet’in Beden İdeolojisi Üzerine Kısa Bir Deneme”. **Ankara Üniversitesi Hukuk Fakültesi Dergisi.** Cilt.54, Sayı.3, 2005.

Saygılı, Abdurrahman. **Kutsal Canavar Devlet**. Ankara: Yetkin Yayınları, 2021.

Schmitt, Carl. **Political Theology, Four Chapters on the Concept of Sovereignty**. George Schwab (çev.). Chicago: University of Chicago Press, 2005.

Schmitt, Carl. **Siyasi İlahiyat Egemenlik Kuramı Üzerine Dört Bölüm**. A. Emre Zeybekoğlu(çev.), Ankara: Dost Kitabevi, 2005.

Schneider, Florian A “Communication and censorship”, Chris Shei ve Qing Cao (Ed.), **Chinese studies: Chinese media, communication and technology** içinde London: Routledge, 2023.

Schneider, Florian A. “Digital smartness, rethinking communities and citizenship in the face of ‘smart’ technology”. **Asiascape: Digital Asia**. Leiden, Vol.6, No.3, 2019.

Schneider, Florian A. “Nationalisms on China’s evolving internet”. **Communication and the Public**. Vol.9, No.4, 2024.

Schneider, Florian A. “Searching for ‘Digital Asia’ in its Networks: Where the Spatial Turn Meets the Digital Turn”. **Asiascape: Digital Asia**, Vol.2, No.1-2, 2015.

Schneider, Florian A. “The cultural governance of China's mass media events: how the PRC manages discourses in complex media environments”, Chris Shei (Ed.),

The Routledge handbook of Chinese discourse analysis içinde. London/New York: Routledge, 2019, ss.458-469.

Schneider, Florian A. "The Cultural Governance of Mass Media in Contemporary China", Michael Keane (Ed.), **The Handbook of Cultural and Creative Industries in China: Handbook of Research on Contemporary China** içinde. Cheltenham & Northampton (MA): Edward Elgar. 2016, ss.189-206.

Schneider, Florian A. **China's Digital Nationalism**. New York: Oxford University Press, 2018.

Schneider, Florian. "Reality Decoupling: Rumours, Disinformation, and Studying the Politics of Truth in Digital Asia", **Asiascape: Digital Asia**, Vol.10, No.1-2, 2023.

Schwartz, Paul M. ve Daniel J. Solovei "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", **New York University Law Review**. Vol.86, December 2011.

Shapiro, Andrew L. **The Control Revolution: How The Internet is Putting Individuals in Charge and Changing The World We Know**. New York: PublicAffairs, 1999.

Shoker, Ali. "Digital Sovereignty Strategies for Every Nation". **Applied Cybersecurity & Internet Governance.** Vol.1, No.1, 2022.

Sırma Gezer, Özge. "Koruma Tedbirleri Bakımından Dijitalleşme". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Smuha, Nathalie A. "Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective", Gavin Barrett, Peter-Christian Müller-Graff, Jean-Philippe Rageade ve Viktor Vadasz (ed.) **European Sovereignty: The Legal Dimension** içinde. Springer, 2024, ss.19-28.

Soyaslan, Doğan. “Hukuk Devletin ve Güvenlik”, **Prof. Dr. Sabih Arkan’a Armağan**. İstanbul: On İki Levha Yayıncılık, 2019.

Sökmen Güler, Ekin. “Uluslararası Özel Hukuk Boyutuyla Sınır Aşan NFT (Non-Fungible Token) Uyuşmazlıklarının Çözümünde Karşılaşılan Sorunlar ve Uyuşmazlık Çözüm Yöntemlerine İlişkin Öneriler”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Katip Çelebi Üniversitesi, 15-16 Aralık 2022.

Sözer, Ali Nazım. “Ceza Hukuku ve Sosyal Devlet”, **Prof. Dr. Kemal Oğuzman’a Armağan**. Ankara: İş Hukuku ve Sosyal Güvenlik Hukuku Türk Millî Komitesi Yayını, 1997.

Spiekermann, Kai, Adam Slavny, David V. Axelsen ve Holly Lawford-Smith. “Big Data Justice: A Case for Regulating the Global Information Commons”, **Journal of Politics**. Vol.83, No.2, 2019.

Subaşı, Zeynep Nur. “İnternette Unutulma ve Silme Hakkı”. Süleyman Yılmaz (Ed.). **Bilişim Hukuku Güncel Sorunlar** içinde. Ankara: Yetkin, 2020, ss.389-437.

Sunstein, Cass. **Republic.com**. Oxfordshire: Princeton University Press, 2001.

Supiot, Alain. **Homo Juridicus: Hukukun Antropolojik İşlevi Üzerine Bir deneme**. Bilge Açımuz Ünal (çev.) Ankara: Dost Kitabevi Yayınları, 2014.

Sütçü, Cem Sefa. “Önsöz”, **Algoritmaların Gölgesinde Toplum ve İletişim,** Oğuz Kuş (drl.), Ankara: Alternatif Bilişim Derneği, 2021.

Şahin, Bediha. “Ulusal Yapay Zekâ Stratejilerinin Eğitim Yönü: Çin ve Türkiye Örneği”, **Scientific Journal of Finance and Financial Law Studies.** Vol.3, No.2, 2023.

Şenel, Alaeddin. **Siyasal Düşünceler Tarihi: Tarih Öncesinde, İlkçağda, Ortaçağda ve Yeniçağda Toplum ve Siyasal Düşünüş.** 4. Basım, Ankara: Bilim ve Sanat, 1995.

Şimşek Öner, Altın Aslı. “Siber-Alanda Devlet Kudretine Bir Bakış: Dijital Egemenlik Kavramı”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Şimşek, Altın Aslı. “İnsan Hakları Hukuku ve İş Dünyası İlişkisi: Hukuki Yükümlü ile Kurumsal Sorumlu Arasında”. **Prof. Dr. Sabih Arkan’a Armağan**. İstanbul: On İki Levha Yayıncılık, 2019.

Tansuğ, Çağla. “Veriye Teknolojik ve Hukuki Yaklaşım Değişikliğinin Kamu Hizmeti Sunumu Alanındaki Etkileri”, Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar (Ed.), **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı** içinde. İstanbul: Adalet, 2021, ss.39-60.

Tevetoğlu, Mete. “DAO’nun Genel Olarak Hukuk Sistemine; Özel Olarak İse Ticaret Hukukuna Etkileri”. **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Thielmann, Tristan ve Christoph Borbach. “The Digital Leviathan: Medializing Sovereignty for Critical AI and Data Studies”. **communication+1**. vol.11, no.2, 2025.

Thorson, Kjerstin ve Chris Wells. “Curated flows: a framework for mapping media exposure in the digital age”. **Communication Theory**. Vol.26, No.3, 2015.

Thumfart, Johannes. “The Norm Development of Digital Sovereignty Between China, Russia, the EU and the US: From the Late 1990s to the Covid-Crisis 2020/21 as Catalytic Event”, Dara Hallinan, Paul de Hert ve Ronald Leenes (Ed.). **Data Protection and Privacy: Enforcing Rights in a Changing World** içinde. Oxford: Hart Publishing, 2021, ss.1-44.

Timmers, Paul. “Ethics of AI and Cybersecurity when Sovereignty is at Stake”, **Minds and Machines**. Vol.29, 2019.

Timmers, Paul. “Sovereignty in the Digital Age”, Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem ve Allison Stanger (Ed.) **Introduction to Digital Humanism** içinde. Springer, 2023, ss.571-592.

Tipper, David ve Prashant Krishnamurthy, “Digital Sovereignty and Resilience”, SSRN, 2022, https://ssrn.com/abstract=4178621 (22 Aralık 2024).

Tischbirek, Alexander. “Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems”. Thomas Wischmeyer ve Timo Rademacher (Ed.), **Regulating Artificial Intelligence** içinde. Springer, 2020, ss.103-122.

Topak, Süleyman. “Dokunmatik Ekran İmzası ile Oluşan Dijital Belgenin Delil Değeri”. **GSÜHFD**. Cilt.2025, Sayı.2, 2025.

Tretter, Max. “Sovereignty in the Digital and Contact Tracing Apps”. **Digital Society: Ethics, Socio-Legal and Governance of Digital Technology**. Vol.2, 2023.

Tufan Yeniçıktı, Nagihan. “İletişimsel Eylem ve Facebook: Gezi Parkı Olaylarında Sosyal Medyanın Gücü”. **Selçuk İletişim Dergisi**. Vol.8, 2014.

Turan, İsmail Bahadır. “Devlet Öğretisi Metodolojisi-Georg Jellinek (Allgemeine Staatslehre)”. **Kamu Hukuk ve Yönetim**. Cilt.1, Sayı.1, Temmuz 2024.

Ugan Çatalkaya, Deniz. “Dijitalleşmenin Çalışma İlişkileri Üzerinde Çift Yönlü Etkisi: ‘Görünürde’ Özgürlükler, ‘Gerçekte’ Daha Sıkı Bir Bağımlılık İlişkisi Lehine Gelişmeler ve Olası Riskler”. Cansu Atıcı, Kerem Batır ve Elif Çağla Yıldız (Ed.), **Dijital Çağda Hukuk** içinde. Ankara: Adalet Yayınevi, 2023, ss.285-304.

Ulu, Cansu. “İnsansız Hava Sistemleri ve Hedef Gözeterek Öldürme”, **Uluslararası Dijital Çağda Hukuk Sempozyumu.** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Uluk, Murat. “Veri Odaklı Kapitalizmin Ardındakiler: Aktörler, Değişen İş Modelleri ve Algoritmaların Rolü”. **Algoritmaların Gölgesinde Toplum ve İletişim**. Oğuz Kuş(drl.), Ankara: Alternatif Bilişim Derneği, 2021.

Ursic, Helena. “The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?”, Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt ve Gintarė Surblytė-Namavičienė (Ed.), **Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?**, içinde. Springer Nature, 2018, ss.55-83.

Uygun, Oktay. **Devlet Teorisi**. Gözden Geçirilmiş 8. Baskı, İstanbul: On İki Levha Yayıncılık, 2021.

Üskül Engin, Zeynep Özlem. “Birey Kavramının Gelişimi ve İnsan Hakları”. **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Prof. Dr. Vecdi Aral’a Armağan**. Cilt.LXXII, Sayı.1, 2014.

Üskül, Zeynep Özlem. “Ortaçağda Teologların Akılla Buluşmasının Bir Örneği: St. Thomas D’aquin”. **Prof. Dr. Necip Kocayusufpaşaoğlu İçin Armağan**. Ankara: Seçkin Yayınları, 2004.

van Dijck, Jose. “Datafiction, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Secular Belief”. **Surveillance & Society**. Vol.12, No.2, 2014, ss. 197-208.

Varoufakis, Yanis. **Kızımla Ekonomi Sohbetleri: Kapitalizmin Kısa Tarihi**. Sinan Arslaner (çev.). İstanbul: Epsilon Yayınevi, 2019.

Varoufakis, Yanis. **Technofeudalism: What Killed Capitalism**. London: The Bodley Head, 2023.

Voo, Julia ve Rogier J.E.H. Creemers “China’s role in digital standards for emerging technologies: impacts on the Netherlands and Europe”. Leiden: **Leiden Asia Centre** 2017.

Vural Dinçkol, Bihterin ve Alper Işık, “1924 Anayasası Döneminde Yurttaşlık Anlayışı”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.21, Sayı.1, 2015.

Vural Dinçkol, Bihterin ve Alper Işık, "Katılımcı Demokrasi ve Online Karar Alma Bağlamında E-Oy ve Estonya Örneği". **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. Cilt.25, Sayı.2, 2019.

Vural Dinçkol, Bihterin. "Çoğulcu Demokrasilerde Siyasal Partiler ve Kanaatler". **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**. Vol.1, No.2, 2002.

Vural Dinçkol, Bihterin. "Yurttaşlık ve Seçilme Hakkı Üzerine Bir Değerlendirme". **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.19, Sayı.2, 2013.

Vural Dinçkol, Bihterin: "Laiklik, Aydınlanma, Modernleşme ve Türkiye Modeli". **Prof. Dr. Tankut Centel'e Armağan** içinde. İstanbul: İstanbul Üniversitesi Hukuk Fakültesi Yayınları, 2011, ss.653-662.

Weymouth, Stephen. **Digital Globalization Politics, Policy, and a Governance Paradox**. Cambridge: Cambridge University Press, 2023.

Wiener, Norbert. **Cybernetics: or Control and Communication in the Animal and the Machine**. 2. Baskı, Massachusetts: The MIT Press, 1961.

Xin, Ge ve Yiting Wang, "The Algorithmic Leviathan and the Digital Polis: A Review of Global Digital Governance Dilemmas and Pathways". **Chinese Journal of International Review**. Vol.7, No.2, 2025.

Yağmur Sümer, Seda. "'Compas' Örneği Çerçevesinde Yapay Zekalı Risk Değerlendirme Araçları ve Ceza Muhakemesine Hâkim Olan İlkeler". **Uluslararası Dijital Çağda Hukuk Sempozyumu.** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Yakovleva, Svetlana ve Kristina Irion, "Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade", **International Data Privacy Law.** Vol.10, No.3, 2020.

Yalçın, Cemre Edip. **Klasik Kamusal Alandan Sanal Kamusal Alana: Demokrasi ve İnsan Hakları İdeali İçin Normatif Bir Değerlendirme**. İstanbul: On İki Levha Yayıncılık, 2022.

Yankın, Fahri Bilal. "Dijital Dönüşüm Sürecinde Çalışma Yaşamı". **Trakya Üniversitesi İktisadi ve İdari Bilimler Fakültesi E-Dergi**. Cilt.7, Sayı.2, Aralık 2018.

Yavuz Yayla, Ebru. "Anayasa'nın 41/4. maddesi Kapsamında Çocukların Dijital Ortamda Cinsel İstismara Karşı Korunması". **Uluslararası Dijital Çağda Hukuk Sempozyumu**. İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Yeniad, Mustafa. "Sosyal Ağlar ve Siber Güvenlik". İbrahim Demir (Ed.), **Mühendislik, Hukuk, İletişim & İktisat Perspektifinden Siber Güvenlik & Sosyal Medya** içinde. Ankara: Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, Vol.Ocak, Sayı.9, 2021, ss.18-20.

Yeşilkaya, Nazan. "Ölümcül Otonom Silah Sistemleri, Savaş Etiği ve Hukuk". **Uluslararası Dijital Çağda Hukuk Sempozyumu.** İzmir: İzmir Kâtip Çelebi Üniversitesi, 15-16 Aralık 2022.

Yıldırım, Engin. "Meta Gözetim Kurulu: Meta'nın 'Anayasa Yargısı' mı, Anayasacılığın Metalaşması mı?" **GSÜHFD**. Cilt.2025, No.2, 2025.

Zabunoğlu, Yahya Kazım, Maksut Mumcuoğlu, Abdurrahman Saygılı ve Hamdi Gökçe Zabunoğlu **Devletin Genel Kuramı Dersleri: Cilt I**. Ankara: Yetkin Yayınları, 2021.

Zhang, Eric Siyi ve Rogier J.E.H. Creemers. "Russian perspectives on China as an actor in cyberspace", Leiden: **Leiden Asia Centre**, 2021.

Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", **Journal of Information Technology**. Vol.30, No.1, 2015.

Zuboff, Shoshana. **Gözetleme Kapitalizmi Çağı: Ürünün "Sen" Olduğu Çağda İnsanın Geleceği için Savaş**. Tolga Uzunçelebi (çev.). İstanbul: Okuyan Us Yayınevi, 2021.

Zuboff, Shoshana. **The Age of Surveillance Capitalism**. New York: Public Affairs, 2019.

Zuckerman, Ethan. "New Media, New Civics?", **Policy and Internet**. Cilt.6, No.2, June 2014.

Zuiderveen Borgesius, Frederik J., Judith Möller, Sanne Kruikemeier, Ronan Ó Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo ve Claes de Vreese. "Online Political Microtargeting: Promises and Threats for Democracy". **Utrecht Law Review**, Cilt.14, No1., 2018, ss.82-96.

II. Belge, Görüş, Araştırma, Rapor ve Haberler

Adrian Shahbaz, Allie Funk, Andrea Hackl, "User Privacy or Cyber Sovereignty?", Freedom House, Special Report, 2020, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sover-eignty (1 Şubat 2026).

AFFRT, "A New Digital Dawn: The Rise, Role and Relevance of the Digital Yuan", AFFRT, https://www.affrt.com/tr/a-new-digital-dawn-the-rise-role-and-relevance-of-the-digital-yuan.html (1 Şubat 2026).

African Union, Convention on Cyber Security and Personal Data Protection, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (14 Aralık 2024).

Ahmed, Shazeda, "Cashless Society, Cached Data: Security Considerations for a Chinese Social Credit System", Citizen Lab, 2017,

https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system (31 Ocak 2026).

Albeniz, Ziyahan, "IT Sistemleri 'Mavi Ekran' Verdi, Dünya Sanal Olarak Çöktü", Serbestiyet, https://serbestiyet.com/featured/dunyaya-kuresel-siber-kesintinin-sokunda-174927/ (1 Şubat 2026).

All Tech Is Human, AI and Human Rights: Building a Tech Future Aligned With the Public Interest, 2022, https://alltechishuman.org/ai-human-rights-report (1 Şubat 2026).

American Civil Liberties Union (ACLU), "Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress", ACLU, https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress (1 Şubat 2026).

Amnesty International, "The Pegasus Project: Unmasking the NSO Group's Spyware", Amnesty International, 18 Temmuz 2021, https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/ (1 Şubat 2026).

Anadolu Ajansı, "Almanya'da Kamuya Ait Veri Ağlarına Siber Saldırı", Anadolu Ajansı, 28 Şubat 2018, https://www.aa.com.tr/tr/dunya/almanyada-kamuya-ait-veri-aglarina-siber-saldiri/1076539 (1 Şubat 2026).

Anadolu Ajansı, "Küresel 'Restart': Dünya Çapında İşletmeleri Etkileyen Büyük Bir Yazılım Sorunu Yaşanıyor", Anadolu Ajansı, https://www.aa.com.tr/tr/dunya/kuresel-restart-dunya-capinda-isletmeleri-etkileyen-buyuk-bir-yazilim-sorunu-yasaniyor/3279453 (1 Şubat 2026).

Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework (2015), APEC, 2015, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (14 Aralık 2024).

Avrupa Birliği Başkanlığı, Ocak 2022 Bülteni, https://www.ab.gov.tr/siteimages/birimler/mib/programlama/bulten/pdf/ocak_2022.pdf (1 Şubat 2026).

Avrupa Konseyi, Convention on Cybercrime (Budapest Convention), 23 Kasım 2001, ETS No. 185, https://rm.coe.int/1680081561 (1 Şubat 2026).

Avrupa Konseyi, İnternet ve Daha Geniş Dijital Dünyada Hukukun Üstünlüğü, Avrupa Konseyi, 2014, https://rm.coe.int/internet-ve-daha-genis-dijital-dunyada-hukukun-ustunlugu-avrupa-konsey/16806daa33 (1 Şubat 2026).

Banco Central do Brasil, Resolution CMN nº 4.656 of April 26, 2018, https://www.bcb.gov.br/content/financialstability/fintechs_docs/Resolution%204656.pdf (1 Şubat 2026).

Bayart, Bertille, Martin, Jacques-Olivier, "Thierry Breton: «C'est aux GAFAM de s'adapter à nos règles, pas l'inverse»", Le Figaro, 10 Nisan 2018, https://www.lefigaro.fr/secteur/high-tech/2018/04/06/32001-20180406ARTFIG00280-thierry-breton-c-est-aux-gafa-de-s-adapter-a-nos-regles-pas-l-inverse.php (1 Şubat 2026).

BBC News Türkçe, "Birimi ilan eden ilk ülke oldu", BBC News Türkçe, 9 Haziran 2021, https://www.bbc.com/turkce/haberler-dunya-57415131 (1 Şubat 2026).

BBC News Türkçe, "Orta Afrika Cumhuriyeti, El Salvador'dan sonra…", BBC News Türkçe, https://www.bbc.com/turkce/haberler-dunya-61252871 (1 Şubat 2026).

BBC News, "Cambridge Analytica: UK Watchdog Fines Facebook £500,000", BBC News, https://www.bbc.com/news/uk-politics-54457407 (2 Şubat 2026).

BBC News, "Facebook Settles Facial-Recognition Privacy Lawsuit", BBC News, 30 Ocak 2020, https://www.bbc.com/news/technology-51309186 (2 Şubat 2026).

Birleşmiş Milletler Internet Governance Forum, The Charter of Human Rights and Principles for the Internet, 2014, http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet_Turkish_final.pdf (2 Şubat 2026).

Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (UNCTAD), Digital Economy Report 2019: Value Creation and Capture, UNCTAD, 2019.

Birleşmiş Milletler, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015, https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf (15 Aralık 2024).

Bradley, Karen, UK Digital Strategy 2017, gov.uk, 11 Eylül 2023, https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy (27 Temmuz 2025).

Business Insider, "Google Search Event Live 2010", Business Insider, 2010, https://www.businessinsider.com/google-search-event-live-2010-9?r=US&IR=T (2 Şubat 2026).

California Privacy Protection Agency (CPPA), California Consumer Privacy Act (CCPA), 2020, https://cppa.ca.gov/regulations/pdf/cppa_act.pdf (14 Aralık 2024).

Canada, Protecting Canadians from Online Crime Act, S.C. 2014, c. 31, https://laws-lois.justice.gc.ca/PDF/2014_31.pdf (1 Şubat 2026).

Cerulus, Laurens, "Europe's Litmus Test over Cloud Computing Push", Politico, 28 Temmuz 2020, https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/ (1 Şubat 2026).

Cerulus, Laurens, "French Cyber Czar Promotes European Tech Sovereignty", Politico, 2021, https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/ (1 Şubat 2026).

Cerulus, Laurens, Jacopo Barigazzi, “Chinese Foreign Minister Warns of US ‘Interference’ on Europe Tour”, Politico, 25 Ağustos 2020, https://www.politico.eu/article/chinese-foreign-minister-warns-of-us-interference-on-europe-tour/ (1 Şubat 2026).

Chazan, Guy, “Angela Merkel Urges EU to Seize Control of Data from US Tech Titans”, Financial Times, 12 Kasım 2019, https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca (1 Şubat 2026).

Clarifying Lawful Overseas Use of Data Act (CLOUD Act), U.S. Department of Justice, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (1 Şubat 2026).

CMS (Expert Guides), CMS Expert Guide to Digital Litigation: France, CMS, https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-litigation/france (1 Şubat 2026).

Commission Nationale de l’Informatique et des Libertés (CNIL), “The CNIL Creates an Artificial Intelligence Department and Begins to Work on Learning Databases”, 26 Ocak 2023, https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases (1 Şubat 2026).

Commonwealth of Australia, Online Safety Act 2021 (Consolidated Text), https://www.legislation.gov.au/C2021A00076/latest/text (1 Şubat 2026).

Commonwealth of Australia, Online Safety Act 2021, https://www.legislation.gov.au/Details/C2021A00076 (1 Şubat 2026).

Commonwealth of Australia, Social Services Act 2018 (Cth), https://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/socia2018398/ (1 Şubat 2026).

Computer Ethics Institute, The Ten Commandments of Computer Ethics, Computer Ethics Institute, 2011, http://cpsr.org/issues/ethics/cei/ (13 Aralık 2024).

Congressional Research Service, Cryptocurrency: Selected Policy Issues, CRS Report R47425, https://crsreports.congress.gov/product/pdf/R/R47425 (1 Şubat 2026).

Conseil d'État (France), Décision n° 453763 (Coyote System), 5e–6e chambres réunies, 6 Mart 2024, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-03-06/453763 (2 Şubat 2026).

Conseil d'État (France), Décision n° 453763 (Coyote System), 6 Mart 2024, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-03-06/453763 (2 Şubat 2026).

Conseil d'État (France), Questions préjudicielles à la Cour de justice de l'Union européenne (CJUE), https://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/socia2018398/ (1 Şubat 2026).

Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, 23 Kasım 2001, https://rm.coe.int/1680081561 (1 Şubat 2026).

Council of Europe, Guidelines on Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, Strasbourg, 1–2 Nisan 2008, https://rm.coe.int/16802fe14d (1 Şubat 2026).

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, 2019, https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/ (1 Şubat 2026).

Cybersecurity and Infrastructure Security Agency (CISA), "ICS Alert: IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure", 20 Temmuz 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (1 Şubat 2026).

Cybersecurity and Infrastructure Security Agency (CISA), "National Cybersecurity Protection System (NCPS)", CISA, https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system (1 Şubat 2026).

Dastin, Jeffrey, “Insight: Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women”, Reuters, 11 Ekim 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (1 Şubat 2026).

Department of Industrial Policy and Promotion (India), Action Plan, 2016, https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/Action__Plan.pdf (27 Temmuz 2025).

Deutsche Welle, “How Taiwan Is Countering Chinese Disinformation”, Deutsche Welle, 25 Ağustos 2022, https://www.dw.com/en/how-taiwan-is-countering-chinese-disinformation/a-62931086 (1 Şubat 2026).

Diken, “İFÖD'den ‘Siber Güvenlik Kanunu’ Uyarısı: Tehlikenin Farkında mısınız?”, Diken, 16 Ocak 2025, https://www.diken.com.tr/ifodden-siber-guvenlik-kanunu-uyarisi-tehlikenin-farkinda-misiniz/ (1 Şubat 2026).

Diken, “Siber Güvenlik Kanunu Teklifi Meclis'te kabul edildi”, Diken, 15 Ocak 2025, https://www.diken.com.tr/siber-guvenlik-kanunu-teklifi-mecliste-kabul-edildi/ (1 Şubat 2026).

e-Estonia, “Artificial Intelligence as the New Reality of e-Justice”, e-Estonia, https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (1 Şubat 2026).

eSafety Commissioner (Australia), “eSafety Statement: National Age Restrictions for Digital Platforms”, eSafety Commissioner, https://www.esafety.gov.au/newsroom/media-releases/esafety-statement-national-age-restrictions-for-digital-platforms (1 Şubat 2026).

Etter, Lauren, “How Duterte Turned Facebook into a Weapon: With Help from Facebook”, Bloomberg Businessweek, 7 Aralık 2017, https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook (1 Şubat 2026).

EuroHPC Joint Undertaking, "Our Supercomputers", EuroHPC, https://eurohpc-ju.europa.eu/supercomputers/our-supercomputers_en (1 Şubat 2026).

European Commission, "The Digital Europe Programme", European Commission, https://digital-strategy.ec.europa.eu/en/activities/digital-programme (14 Aralık 2025).

European Commission, A European Strategy for Data (COM (2020) 66), 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066 (1 Şubat 2026).

European Commission, Commission Decision on Open Source Licensing and Reuse of Commission Software (2021/C 495 I/01), 8 Aralık 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D1209(01) (1 Şubat 2026).

European Commission, European Chips Act, 2022, https://digital-strategy.ec.europa.eu/en/policies/european-chips-act (1 Şubat 2026).

European Commission, European Declaration on Digital Rights and Principles, 2022, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles (1 Şubat 2026).

European Commission, Proposal on European Production and Preservation Orders for Electronic Evidence, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN (14 Aralık 2024).

European Commission, Shaping Europe's Digital Future, European Commission, 2020, https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260 (15 Aralık 2025).

European Commission, Two Years of Application of the GDPR (COM (2020) 264 final), 24 Haziran 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264 (1 Şubat 2026).

European Commission: Futurium, “Cloud Computing Services: European Alliance for Industrial Data, Edge and Cloud”, Digital Compass Library (Video), https://futurium.ec.europa.eu/en/digital-compass/digital-businesses/library-video/cloud-computing-services-european-alliance-industrial-data-edge-and-cloud (1 Şubat 2026).

European Council, “Digital Single Market for Europe”, European Council, 2015, https://www.consilium.europa.eu/en/policies/digital-single-market/ (1 Şubat 2026).

European Council, “Digital Sovereignty Is Central to European Strategic Autonomy: Speech by President Charles Michel”, European Council, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/ (15 Aralık 2025).

European Council, “The Digital in a Fractious World: Europe’s Way – Speech by President Charles Michel at the FT-ETNO Forum”, 29 Eylül 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/pdf (1 Şubat 2026).

European Council, Special Meeting of the European Council (1 and 2 October 2020) – Conclusions, 2020, https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf (15 Aralık 2024).

European Parliament, Compromise Amendments to the Draft Report on “A New Industrial Strategy for Europe”, 15 Ekim 2020, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2020/10-15/CAs_Industrial_Strategy_EN.pdf (1 Şubat 2026).

European Parliament, Draft Report on a European Strategy for Data, 2020, https://www.europarl.europa.eu/doceo/document/ITRE-PR-657163_EN.pdf (1 Şubat 2026).

European Parliamentary Research Service, Digital Sovereignty for Europe, EPRS, 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (15 Aralık 2024).

European Parliamentary Research Service, EU Strategic Autonomy 2013–2023: From Concept to Capacity, EPRS, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf (15 Aralık 2024).

European Parliamentary Research Service, Tackling Deepfakes in European Policy, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf (1 Şubat 2026).

European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689), 2024, https://data.europa.eu/eli/reg/2024/1689/oj (2 Şubat 2026).

European Union, Commission Delegated Regulation (EU) 2022/265, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (1 Şubat 2026).

European Union, Cybersecurity Act (Regulation (EU) 2019/881), Official Journal of the European Union L 151/15, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (1 Şubat 2026).

European Union, Directive (EU) 2015/2366 on Payment Services in the Internal Market (PSD2), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366 (1 Şubat 2026).

European Union, Directive (EU) 2016/1148 (NIS Directive), 2016, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf (1 Şubat 2026).

European Union, EU Cybersecurity Strategy for the Digital Decade (JOIN (2020) 18 final), 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018 (1 Şubat 2026).

European Union, General Data Protection Regulation (Regulation (EU) 2016/679), 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (1 Şubat 2026).

European Union, Regulation (EU) 2019/881 (Cybersecurity Act), Official Journal L 151/15, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (1 Şubat 2026).

Europol, "Crime Areas: Cybercrime", Europol, https://www.europol.europa.eu/crime-areas/cybercrime (1 Şubat 2026).

Europol, Crime Areas: Cybercrime, https://www.europol.europa.eu/crime-areas/cybercrime (1 Şubat 2026).

Federal Antimonopoly Service of the Russian Federation, Federal Law No. 44-FZ on the Contract System in Public Procurement (English Translation), https://en.fas.gov.ru/netcat_files/File/44-FZ%20eng.pdf (1 Şubat 2026).

Federal Budget IQ, "DoD's FY24 Cyber Budget", Federal Budget IQ, https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/ (1 Şubat 2026).

Federal Ministry of the Interior and Community (Germany), "Better Protection for Critical Infrastructure", 28 Temmuz 2023, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2023/07/ge-kritis.html (1 Şubat 2026).

Federal Register of Legislation (Australia), Privacy Act 1988, https://www.legislation.gov.au/C2004A03712/latest/text (14 Aralık 2024).

Federal Risk and Authorization Management Program (FedRAMP), "FedRAMP Program Basics", FedRAMP, https://www.fedramp.gov/program-basics (1 Şubat 2026).

Financial Times, "EU Digital Protectionism Risks Damaging Ties with the US", Financial Times, 2 Ağustos 2020, https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103 (1 Şubat 2026).

Freedom House, Saudi Arabia: Freedom on the Net 2021 Country Report, https://www.freedomhouse.org/country/saudi-arabia/freedom-net/2021 (1 Şubat 2026).

GDPR, Avrupa Birliği Genel Veri Koruma Tüzüğü (Regulation (EU) 2016/679) Türkçe Çeviri, https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf (1 Şubat 2026).

Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector, 2020, https://www.globaldataalliance.org/downloads/GDAeverysector.pdf (1 Şubat 2026).

Gobierno de España, Carta de Derechos Digitales, 2021, https://portal.mineco.gob.es/recursosarticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/sediacartaderechosdigitales.pdf (14 Aralık 2024).

Government of Canada, "Joint Statement from Founding Members of the Global Partnership on Artificial Intelligence", 2020, https://www.canada.ca/en/innovation-science-economic-development/news/2020/06/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence.html (1 Şubat 2026).

Görgülü, Eymen, "İnternetin Öyküsü: Geçmişten Günümüze", Bilişim Dergisi, https://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/internetin-oykusu-gecmisten-gunumuze.html (2 Şubat 2026).

Greenwald, Glenn – MacAskill, Ewen, "NSA Prism Program Taps In to User Data of Apple, Google and Others", The Guardian, 7 Haziran 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (1 Şubat 2026).

Heavnn University, "Russia Approves Cryptocurrency Framework: A New Era for Digital Assets Amid Sanctions and Tax Reform", https://university.heavnn.io/russia-approves-cryptocurrency-framework-a-new-era-for-digital-assets-amid-sanctions-and-tax-reform/ (1 Şubat 2026).

Hollis, Duncan B., "A Brief Primer on International Law and Cyberspace", Carnegie Endowment for International Peace, 14 Haziran 2021, https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace (1 Şubat 2026).

Houben, Robby, Snyers, Alexander, "Crypto-assets: Key Developments, Regulatory Concerns and Responses", European Parliament, 2020.

Human Rights Watch, "Questions and Answers: Turkey's Control of the Internet and Upcoming Election", Human Rights Watch, 10 Mayıs 2023, https://www.hrw.org/news/2023/05/10/questions-and-answers-turkeys-control-internet-and-upcoming-election (1 Şubat 2026).

Human Rights Watch, "Submission to the Human Rights Committee: Russian Federation", Human Rights Watch, 15 Şubat 2022, https://www.hrw.org/news/2022/02/15/submission-human-rights-watch-russia-human-rights-committee (1 Şubat 2026).

Independent Türkçe, "Scarlett Johansson, Sesini Kullanan Yapay Zekâ Şirketine Yasal İşlem Başlattı", Independent Türkçe, https://www.indyturk.com/node/671376/yasam/scarlett-johansson-sesini-kullanan-yapay-zeka-sirketine-yasal-islem-baslatti (1 Şubat 2026).

International Committee of the Red Cross (ICRC), “Martens Clause (Glossary)”, ICRC, 2024, https://casebook.icrc.org/a_to_z/glossary/martens-clause (14 Aralık 2024).

International Telecommunication Union (ITU), “Our Members”, ITU, https://www.itu.int/hub/membership/our-members/ (1 Şubat 2026).

International Telecommunication Union (ITU), WSIS Declaration of Principles: Building the Information Society, 12 Aralık 2003, https://www.itu.int/net/wsis/docs/geneva/official/dop.html (1 Şubat 2026).

Internet Corporation for Assigned Names and Numbers (ICANN)-U.S. Department of Commerce, Memorandum of Understanding, 31 Aralık 1999, https://www.icann.org/en/governance/documents/memorandum-of-understanding-between-the-us-department-of-commerce-and-icann-31-12-1999-en (1 Şubat 2026).

Internet Society, “Internet Society Statement on U.S. Clean Network Program”, Internet Society, 2020, https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/ (1 Şubat 2026).

Interoperable Europe Portal – Open Source Observatory (OSOR), “MIMO: A Working Group of French Ministries to Certify a LibreOffice Release”, European Commission, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/mimo-working-group-french-ministries-certify-libreoffice-release (1 Şubat 2026).

Japanese Law Translation, Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers, 2005, https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en (14 Aralık 2024).

Japanese Law Translation, Act on the Protection of Personal Information, 2003, https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (14 Aralık 2024).

Johnson, Bobbie, “Privacy No Longer a Social Norm, Says Facebook Founder”, The Guardian, 11 Ocak 2010, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (2 Şubat 2026).

Klimburg, Alexander, The Internet Yalta, Center for a New American Security, Washington D.C., 2013.

Komaitis, Konstantinos, Sherman, Justin, “The ITU Election Pitted the United States and Russia Against Each Other for the Future of the Internet”, Atlantic Council, 29 Eylül 2022, https://www.atlanticcouncil.org/uncategorized/the-itu-election-and-the-future-of-the-internet/ (1 Şubat 2026).

Kundra, Vivek, Federal Cloud Computing Strategy, The White House, Washington D.C., 2011.

Kuo, Mercy A., “China’s Digital Nationalism and Activism: Insights from Florian Schneider”, The Diplomat, 17 Ağustos 2017, https://thediplomat.com/2021/08/chinas-digital-nationalism-and-activism/ (2 Şubat 2026).

Laidler, John, “High Tech Is Watching You: In New Book, Business School Professor Emerita Says Surveillance Capitalism Undermines Autonomy — and Democracy (Q&A with Shoshana Zuboff)”, Harvard Gazette, 4 Mart 2019, https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy (14 Aralık 2024).

LGPD Brasil, Brazilian General Data Protection Law (LGPD) – English Version, 2020, https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf (14 Aralık 2024).

Manancourt, Vincent, “Europe’s Data Grab”, Politico, 19 Şubat 2020, https://www.politico.eu/article/europe-data-grab-protection-privacy/ (1 Şubat 2026).

Margolin, Jack, "Russia, China, and the Push for 'Digital Sovereignty'", Global Voices, 2 Aralık 2016, https://tr.globalvoices.org/2016/12/rusya-cin-ve-dijital-egemenlik-ihtiyaci/ (1 Şubat 2026).

McCarthy, John, "What Is Artificial Intelligence?", Stanford University Computer Science Department, 2007, https://www-formal.stanford.edu/jmc/whatisai.pdf (14 Aralık 2024).

McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, McKinsey & Company, 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx (28 Ocak 2026).

MIT News, "Report: CHIPS Act Is Just First Step to Addressing Threats to U.S. Leadership in Advanced Computing", MIT News, 28 Şubat 2023, https://news.mit.edu/2023/report-chips-act-just-first-step-addressing-threats-us-leadership-advanced-computing-0228 (1 Şubat 2026).

Milliyet, "Oğlunun Sesini Taklit Eden Yapay Zekâ ile 25 Bin Dolar Dolandırdılar", Milliyet, https://www.milliyet.com.tr/dunya/oglunun-sesini-taklit-eden-yapay-zeka-ile-25-bin-dolar-dolandirdilar-7213403 (1 Şubat 2026).

Ministry of Science and ICT (South Korea), The Digital New Deal Is to Lead Digital Transition in the World After COVID-19, 2021, https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&mId=4&mPid=2&nttSeqNo=443 (14 Aralık 2024).

National People's Congress of the People's Republic of China, Personal Information Protection Law, 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (14 Aralık 2024).

National Security Agency (NSA), "How NSA, U.S. Cyber Command Are Defending Midterm Elections: One Team, One Fight", 25 Ağustos 2022,

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight/ (1 Şubat 2026).

New York Post, "Scammers Swindle Elderly California Man out of $25K by Using AI Voice Technology…", New York Post, 18 Ekim 2024, https://nypost.com/2024/10/18/us-news/scammers-swindle-elderly-california-man-out-of-25k-by-using-ai-voice-technology-to-claim-his-son-was-in-horrible-accident-needed-money-for-bail-absolutely-his-voice/ (1 Şubat 2026).

North Atlantic Treaty Organization (NATO), Cyber Defence Pledge, https://www.nato.int/cps/en/natohq/official_texts_133177.htm (1 Şubat 2026).

OECD, "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, 2019, http://dx.doi.org/10.1787/b2023a47-en (1 Şubat 2026).

OECD, Going Digital: Shaping Policies, Improving Lives, OECD Publishing, 2019, https://www.oecd.org/en/publications/going-digital-shaping-policies-improving-lives_9789264312012-en.html (13 Aralık 2024).

OECD, OECD Digital Economy Outlook 2024 (Vol. 1): Embracing the Technology Frontier, OECD Publishing, 2024, https://doi.org/10.1787/a1689dc5-en (1 Şubat 2026).

OECD, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, OECD Publishing, 2011, http://dx.doi.org/10.1787/5kgf09z90c31-en (1 Şubat 2026).

Office of Management and Budget (OMB), Memorandum M-16-21: Federal Information Security Modernization Act (FISMA) Reporting Requirements for Executive Agencies, The White House, 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf (1 Şubat 2026).

Organisation for Economic Co-operation and Development (OECD), OECD AI Principles, 2018, https://oecd.ai/en/ai-principles (1 Şubat 2026).

Ölmez, Yasir, "Almanya, İlk Kuantum Bilgisayarını Tanıttı", Kuantum Türkiye, https://kuantumturkiye.org/almanya-ilk-kuantum-bilgisayarini-tanitti/ (1 Şubat 2026).

Özkan, Yusuf, "Avrupa Adalet Divanı, Google'a 2,4 Milyar Avroluk Rekor Cezayı Onayladı", BBC News Türkçe, https://www.bbc.com/turkce/articles/c20rqkee2ldo (1 Şubat 2026).

Patnaik, Subrat, Michael Msika, "iPhone Maker Apple's Market Value Approaches That of French Stock Market", Business Standard, 14 Aralık 2023, https://www.business-standard.com/world-news/iphone-maker-apple-s-market-value-approaches-that-of-french-stock-market-123121400586_1.html (1 Şubat 2026).

People's Republic of China, Anti-Monopoly Law, https://www.icao.int/sustainability/Compendium/Documents/China/download-antimonopoly-law-in-china-63824%20(3).pdf (1 Şubat 2026).

Politico Europe, "Cambridge Analytica, Leave.EU, UKIP, Brexit and Facebook", Politico Europe, https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/ (2 Şubat 2026).

Politico, "Google, Facebook, Amazon Regulation: Europe vs Washington on Privacy, Competition and Tax", Politico, https://www.politico.eu/article/google-facebook-amazon-regulation-europe-washington-brussels-privacy-competition-tax-vestager (1 Şubat 2026).

Publications Office of the European Union, Algorithmic Discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1 (1 Şubat 2026).

Roberts, Paul, "China's Great Firewall Being Turned Against Facebook, Google, and Twitter", Threatpost, 18 Kasım 2011, https://threatpost.com/chinas-great-firewall-being-turned-against-facebook-google-and-twitter-111811/75912/ (1 Şubat 2026).

Schmitt, Michael N. (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge: Cambridge University Press, 2017, https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf (1 Şubat 2026).

Schulze, Elizabeth, "Tech: Russia Just Brought in a Law to Try to Disconnect Its Internet from the Rest of the World", CNBC, 1 Ekim 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html (1 Şubat 2026).

Sermaye Piyasası Kurulu, "Kripto Varlık Hizmet Sağlayıcılara İlişkin Duyuru", SPK, https://www.spk.gov.tr/duyurular/basin-duyurulari/2024/kripto-varlik-hizmet-saglayicilara-iliskin-duyuru_02072024 (1 Şubat 2026).

Singapore Infocomm Media Development Authority (IMDA), Digital Economy Framework for Action Singapore, 2018, https://www.imda.gov.sg/-/media/imda/files/sg-digital/sgd-framework-for-action.pdf (27 Temmuz 2024).

Sözcü, "Cambridge Analytica Nedir? Cambridge Analytica Skandalı Nasıl Oldu?", Sözcü, https://www.sozcu.com.tr/cambridge-analytica-nedir-cambridge-analytica-skandali-nasil-oldu-wp7671806 (2 Şubat 2026).

Sözcü, "Ünlü Ekran Yüzünü Deepfake ile Porno Filminde Oynattılar", Sözcü, https://www.sozcu.com.tr/unlu-ekran-yuzunu-deepfake-ile-porno-filminde-oynattilar-p42725 (1 Şubat 2026).

Stanford University: DigiChina Project, Translation: Cybersecurity Law of the People's Republic of China, 2017, https://digichina.stanford.edu/work/translation-

cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (14 Aralık 2024).

Stanford University: DigiChina Project, Translation: Data Security Law of the People's Republic of China, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (14 Aralık 2024).

Stanford University: DigiChina Project, Translation: Personal Information Protection Law of the People's Republic of China (PIPL), 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (14 Aralık 2024).

Stanford University: WILMap, Federal Law No. 425-FZ on Mandatory Pre-Installation of Russian Software, 2 Aralık 2019, https://wilmap.stanford.edu/entries/federal-law-no-425-fz-amending-article-4-federal-law-consumer-rights-protection-december-2 (1 Şubat 2026).

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ulusal Yapay Zekâ Stratejisi 2021–2025, 2021, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZekaStratejisi2021-2025.pdf (10 Eylül 2025).

The Economist, "The EU Wants to Set the Rules for the World of Technology", The Economist, 20 Şubat 2020, https://www.economist.com/business/2020/02/20/the-eu-wants-to-set-the-rules-for-the-world-of-technology (1 Şubat 2026).

The Guardian, "China's Internet Censorship Uses Distraction as Well as Repression", The Guardian, 22 Ocak 2017, https://www.theguardian.com/commentisfree/2017/jan/22/chinese-internet-censorship-uses-distraction (1 Şubat 2026).

The Independent, "NSO: Who Are the Spyware Makers at the Centre of the Pegasus Scandal?", The Independent, https://www.independent.co.uk/news/world/nso-who-spyware-pegasus-b1886786.html (1 Şubat 2026).

The Spectator, “Were There Any Links Between Cambridge Analytica, Russia and Brexit?”, The Spectator, https://www.spectator.co.uk/article/were-there-any-links-between-cambridge-analytica-russia-and-brexit/ (2 Şubat 2026).

The White House, 2024 Report on the Cybersecurity Posture of the United States, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (1 Şubat 2026).

Toronto Declaration, The Toronto Declaration, 2018, https://www.torontodeclaration.org (1 Şubat 2026).

Türkiye Büyük Millet Meclisi, Siber Güvenlik Kanunu Gerekçesi (Genel Gerekçe), https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf (1 Şubat 2026).

Türkiye Büyük Millet Meclisi, Siber Güvenlik Kanunu Gerekçesi, Genel Gerekçe, https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf (1 Şubat 2026).

Türkiye Cumhuriyet Merkez Bankası, Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, 16 Nisan 2021 tarihli ve 31456 sayılı Resmî Gazete, https://www.tcmb.gov.tr/wps/wcm/connect/6937855a-7c29-4d08-a26e-51ef3273c022/%C3%96demelerde%2BKripto%2BVarl%C4%B1klar%C4%B1n%2BKullan%C4%B1lmamas%C4%B1na%2BDair%2BY%C3%B6netmelik.pdf (1 Şubat 2026).

U.S. Department of Commerce, National Institute of Standards and Technology, The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (1 Şubat 2026).

U.S. Department of State, “The Clean Network”, U.S. Department of State, https://2017-2021.state.gov/the-clean-network/ (15 Aralık 2024).

UK Home Office, Police Survey 2022: Use of Overt Surveillance Camera Systems, UK Government, https://www.gov.uk/government/publications/police-survey-2022-responses-and-key-findings/the-use-of-overt-surveillance-camera-systems-in-public-places-by-police-forces-in-england-and-wales-an-assessment-of-compliance-with-the-protection-o (1 Şubat 2026).

UNCTAD, Digital Economy Report 2019: Value Creation and Capture, UNCTAD, 2019.

UNCTAD, Digital Economy Report, UNCTAD, 2021, https://unctad.org/system/files/official-document/der2021_en.pdf (1 Şubat 2026).

UNESCO, Preliminary Study on the Ethics of Artificial Intelligence, 2019, https://unesdoc.unesco.org/ark:/48223/pf0000367823 (14 Aralık 2024).

United Kingdom Parliament, Data Protection Act 2018, c. 30, https://www.legislation.gov.uk/ukpga/2018/12/contents (1 Şubat 2026).

United Kingdom Parliament, Financial Services Act 2021, https://www.legislation.gov.uk/ukpga/2021/22 (1 Şubat 2026).

United Kingdom Parliament, Investigatory Powers Act 2016, c. 25, https://www.legislation.gov.uk/ukpga/2016/25/contents (1 Şubat 2026).

United Nations Department of Economic and Social Affairs (UNDESA), United Nations E-Government Survey 2014: E-Government for the Future We Want, 2014, https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf (1 Şubat 2026).

United Nations Development Programme (UNDP), Guiding Principles on Business and Human Rights (Turkish Edition), 2023, https://www.undp.org/sites/g/files/zskgke326/files/2023-06/bhr_ungp_rehberilkelerrapor.29.05.23_web.pdf (1 Şubat 2026).

United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/78/237, 22 Aralık 2023, https://docs.un.org/en/a/res/78/237 (1 Şubat 2026).

United Nations Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/39/29, 3 Ağustos 2018, https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf (1 Şubat 2026).

United Nations Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/48/31, 2021, https://docs.un.org/en/A/HRC/48/31 (1 Şubat 2026).

United Nations Office for Disarmament Affairs, Open-Ended Working Group on ICT Security, https://meetings.unoda.org/open-ended-working-group/ (1 Şubat 2026).

United Nations Security Council, Open Debate on Cyber Security – Concept Note, 29 Haziran 2021, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf (1 Şubat 2026).

United Nations, Resolution 59(I), 14 Aralık 1946, https://digitallibrary.un.org/record/209774?v=pdf (2 Şubat 2026).

United States Code of Federal Regulations, Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5, https://www.ecfr.gov/current/title-16/section-312.5 (1 Şubat 2026).

United States Congress, Children's Online Privacy Protection Act (COPPA), 1998, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 (1 Şubat 2026).

United States Congress, Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (1 Şubat 2026).

United States Congress, Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (1 Şubat 2026).

United States Congress, Cybersecurity and Infrastructure Security Agency Act of 2018 (CISA Act), Pub. L. 115-278, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf (1 Şubat 2026).

United States Congress, Sherman Act, https://www.govinfo.gov/content/pkg/COMPS-3055/pdf/COMPS-3055.pdf (1 Şubat 2026).

Wakefield, Jane, "Russia 'Successfully Tests' Its Unplugged Internet", BBC, 24 Aralık 2019, https://www.bbc.com/news/technology-50902496 (1 Şubat 2026).

Wilson Center, "European Chips Act: A Vital Step in the Right Direction", Wilson Center, https://www.wilsoncenter.org/article/european-chips-act-vital-step-right-direction (1 Şubat 2026).

Wired.me, "UAE Alternatives to Banned Skype Calls", Wired.me, https://wired.me/technology/uae-alternatives-banned-skype-calls/ (1 Şubat 2026).

Wolff, Guntram, "Europe May Be the World's AI Referee, but Referees Don't Win", Politico, 17 Şubat 2020, https://www.politico.eu/article/europe-may-be-the-worlds-ai-referee-but-referees-dont-win-margrethe-vestager/ (1 Şubat 2026).

Working Group on Internet Governance (WGIG), Report of the Working Group on Internet Governance, Haziran 2005, https://www.wgig.org/docs/WGIGREPORT.pdf (1 Şubat 2026).

World Economic Forum, Data Free Flow with Trust, 2021, https://www.weforum.org/publications/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows/ (14 Aralık 2024).

World Economic Forum, Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows, WEF, 2021, https://www.weforum.org/publications/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows/ (14 Aralık 2024).

World Trade Organization (WTO), On Information, Information Technologies and the Protection of Information (WT/ACCR/RUS58/LEG/369), 2006, https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf (1 Şubat 2026).

World Trade Organization (WTO), World Trade Report 2018: The Future of World Trade, WTO, 2018, https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (1 Şubat 2026).

World Trade Organization (WTO), WT/ACC/RUS58/LEG/369 – Accession of the Russian Federation, 2006, https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf (14 Aralık 2024).

Yirmidort.tv, "Çağın Dijital Atom Bombası", Yirmidort.tv, 22 Kasım 2024, https://www.yirmidort.tv/gundem/cagin-dijital-atom-bombasi-210490 (1 Şubat 2026).

III. Tezler

Altaş, Alkan. "Özgürlük ve Egemenlik Arasında 'Bölünmüş İnternet'", **Yayınlanmamış Yüksek Lisans Tezi**. İstanbul Medeniyet Üniversitesi Lisansüstü Eğitim Enstitüsü, 2024.

Bulut, Serkan. "Çokluk Mekânı Olarak Dijital Medya ile Egemenlik Çerçevesinde Bilginin Kontrolü ve Yapısal Dönüşümü", **Yayınlanmamış Doktora Tezi**. İstanbul Üniversitesi SBE, 2019.

Demirkan, Gürol. “Blokzincir Teknolojisi ve Teknolojik Determinizm Çerçevesinde Toplumsal Değişime Etkileri”, **Yayınlanmamış Yüksek Lisans Tezi**. İstanbul Medipol Üniversitesi SBE, 2021.

Özdemir, Gloria. “Artificial Intelligence ‘Arms Dynamics’: The Case of the United States and China Rivalry”, **Yayınlanmamış Doktora Tezi,** Ankara Yıldırım Beyazıt Üniversitesi SBE, 2024.

Pehlivan, Hatice Kübra. “Türk Anayasalarında Millî Devlet, Ülke ve Vatandaşlık Kavramları”, **Yayınlanmamış Yüksek Lisans Tezi**. Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü, 2006.

IV. İnternet Siteleri

http://ec.europa.eu

http://eur-lex.europa.eu

http://www.apec.org

http://www.cnbc.com

http://www.dildernegi.org.tr

http://ww.echr.coe.int

http://www.ilo.org

http://www.mevzuat.gov.tr

http://www.oecd.org

http://www.ohchr.org

http://www.tdk.gov.tr

http://www.who.int

http://www.xinhuanet.com

https://ansiklopedi.tubitak.gov.tr

https://cbddo.gov.tr

https://cryptocurrency.law

https://curia.europa.eu (Avrupa Adalet Divanı kararları için)

https://dictionary.cambridge.org

https://finlandeducationhub.com

https://hudoc.echr.coe.int (AİHM kararları için)

https://iapp.org

https://iclalturan.medium.com

https://journo.com.tr

https://law.justia.com (ABD Temyiz Mahkemesi kararları için)

https://medium.com

https://ninjanews.io

https://protectkidsonline.ca

https://schneider-group.com

https://sozluk.gov.tr

https://technode.com

https://www.bollettinoadapt.it

https://www.boomlive.in

https://www.businessinsider.com

https://www.chinalawtranslate.com

https://www.chip.com.tr

https://www.citizensadvice.org.uk

https://www.cnet.com

https://www.coe.int

https://www.dataguidance.com

https://www.differencebetween.net

https://www.disputeresolutiongermany.com

https://www.economist.com

https://www.endustri40.com

https://www.ericsson.com

https://www.fdd.org

https://www.forbes.com

https://www.fransizcasozluk.net

https://www.gzt.com

https://www.ifj.org

https://www.kosgeb.gov.tr

https://www.lexology.com

https://www.linkedin.com

https://www.lsd.law

https://www.merriam-webster.com

https://www.moxytongue.com

https://www.msb.gov.tr

https://www.nisanyansozluk.com

https://www.online-latin-dictionary.com

https://www.oxfordlearnersdictionaries.com

https://www.resmigazete.gov.tr

https://www.straitstimes.com

https://www.tbmm.gov.tr

https://www.thetimes.co.uk

https://www.turkiye.gov.tr

https://www.turkiyehukuk.org

https://www.viettan.org

https://www.wired.com

https://www.womeninidentity.org

https://www.youtube.com

www.anayasa.gov.tr (Anayasa Mahkemesi kararları için)

www.yargitay.gov.tr (Yargıtay kararları için)