

## Dijital Egemenlik ve Ulus Devletin Dönüşümü: Teknoloji Devlerinin Yükselişi, Algoritmik Yönetişim ve Küresel Güç Dengeleri

Esin ÖZÇELİK\* Şevki IŞIKLI\*\*

\*Muğla Sıtkı Koçman  
Üniversitesi Sosyal Bilimler  
Enstitüsü  
esinozcelik@gmail.com  
 <https://orcid.org/0000-0001-9516-4363>

\*\*Marmara Üniversitesi,  
Visiting Scholar at Florida  
Gulf Coast University  
sisikli@fgcu.edu  
 <https://orcid.org/0000-0002-8075-9177>

**Anahtar Sözcükler**  
Dijital Egemenlik, Finansal  
Egemenlik, Teknoloji  
Devleri, Siyasi Otorite

**Key Words**  
Digital Sovereignty,  
Financial Sovereignty,  
Technology Giants, Political  
Authority.

**Atıf/Citation**  
Özçelik, E., Işıklı, Ş. (2024).  
Dijital Egemenlik ve Ulus  
Devletin Dönüşümü:  
Teknoloji Devlerinin  
Yükselişi, Algoritmik  
Yönetişim ve Küresel  
Güç Dengeleri. ISophos:  
Uluslararası Bilişim,  
Teknoloji ve Felsefe Dergisi,  
Cilt 7, Sayı 13,  
ss: 17-33

### Özet

Bu makale, teknoloji devlerinin küresel sistemdeki yükselişini ulus devlet egemenliğinin dönüşümü bağlamında incelemektedir. Dijital platformların ekonomik büyüklükleri, altyapısal tahakkümleri ve algoritmik yönetim pratikleri; geleneksel devlet otoritesinin mali, siyasi ve güvenlik alanlarındaki tekeli sarsmaktadır. Çalışmada, 2025 yılı verileri ışığında teknoloji şirketlerinin piyasa değerleri ile G7 ülkelerinin GSYİH rakamları kıyaslanarak "finansal egemenlik" kayması analiz edilmektedir. Ayrıca, stablecoinlerin ve platform merkezli ödeme sistemlerinin para politikası üzerindeki etkileri, bulut bilişimdeki altyapı bağımlılığı ve Avrupa Birliği'nin regülasyon stratejileri ele alınmaktadır. Çalışmada, teknoloji devlerinin mali, altyapısal ve algoritmik kapasiteleriyle devletlerin geleneksel egemenlik alanlarını fiilen paylaştığı ve de facto yönetsel otoriteler haline geldiği sonucuna varılmıştır. Bu dönüşüm karşısında ulus devletlerin dijital özerkliklerini korumak adına "Milli Dijital Kamu Altyapıları" geliştirmeleri ve bölgesel iş birlikleri kurmaları stratejik bir zorunluluk olarak vurgulanmaktadır ve elde edilen bulgular doğrultusunda, devletlerin dijital özerkliklerini korumaları için bölgesel iş birlikleri geliştirmeleri gerektiğini savunmaktadır.

### Abstract

#### Digital Sovereignty and the Transformation of the Nation-State: The Rise of Tech Giants, Algorithmic Governance, and Global Power Dynamics

This article examines the rise of technology giants within the global system in the context of the transformation of nation-state sovereignty. The economic scale of digital platforms, their infrastructural dominance, and their practices of algorithmic governance are challenging the traditional monopoly of state authority in fiscal, political, and security domains. In light of 2025 data, the study analyzes the shift in "financial sovereignty" by comparing the market capitalizations of major technology companies with the GDP figures of G7 countries. It also addresses the impact of stablecoins and platform-centered payment systems on monetary policy, infrastructural dependence in cloud computing, and the regulatory strategies of the European Union. The study concludes that, through their financial, infrastructural, and algorithmic capacities, technology giants are effectively sharing the traditional domains of state sovereignty and have become de facto

governing authorities. In response to this transformation, it emphasizes that developing “National Digital Public Infrastructures” and establishing regional cooperation frameworks constitute a strategic imperative for nation-states seeking to preserve their digital autonomy. Based on the findings, the article argues that states must strengthen regional collaboration to safeguard their digital sovereignty.

### Giriş: Platform Egemenliği Tartışması

21. yüzyılın ikinci çeyreğine girerken uluslararası sistem, Westphalia düzeninden bu yana en köklü otorite kaymalarından birine tanık olmaktadır. Geleneksel ulus devlet, fiziki sınırlar ve hukuk tekeli üzerine kurulu egemenlik kapasitesini, küresel ölçekte faaliyet gösteren teknoloji devlerine (Big Tech) karşı savunmak durumundadır. Dijitalleşme hem teknik düzeyde hem de verinin, altyapının ve algoritmaların kontrolü üzerinde yeni bir iktidar alanı yaratmaktadır.

Teknoloji Devleri (Tekno-devler), örneğin Google, Apple, Microsoft, Amazon ve Meta gibi şirketler olarak tanımlanır. Bu şirketler sadece ürün ve hizmet sunan ticari aktörler değil, global dijital ekosistemde merkezi konuma sahip, büyük kullanıcı ağları, altyapılar, veri ve ekonomik güç üzerinden toplumun geniş alanlarında etkili aktörlerdir. Kavram, bu şirketlerin sahip oldukları ekonomik büyüklük, altyapısal kontrol (ör. bulut hizmetleri, işletim sistemleri) ve algoritmik gücün devletlerin karar alma ve düzenleme süreçlerini etkileyebilmesiyle ilişkilendirilir. Böylece bu aktörler, devletlerin egemenlik alanlarına doğrudan müdahale edebilir veya onu yeniden biçimlendirebilir. Yani tekno-dev olarak adlandırılan bu şirketler, devletlerle karşılaştırılabilir güç ve etkiye ulaşmış özel şirketlerdir (Işıklı, 2024). Bu bağlamda dijital egemenlik kavramı, devletlerin kendi dijital varlıklarını ve altyapılarını yabancı kurumsal aktörlerden bağımsız olarak yönetme kapasitesi olarak kristalize olmaktadır (Qelichi vd., 2025). Teknolojik determinizmden uzak bir yaklaşımla, bu yeni egemenlik biçimi paylaşılmış ve parçalı bir yapıya evrilmektedir. Ulus devletlerin karar alma yetkileri, platformların teknik standartları ve küresel veri akışı üzerindeki kontrolü tarafından fiilen sınırlandırılmaktadır (Işıklı, 2024).

Geleneksel ulus devlet anlayışı, belirli bir toprak parçası üzerinde mutlak otoriteyi ve dış müdahalelerden bağımsız karar alma kapasitesini temsil eder. Ancak dijital dönüşüm, bu otoritenin temel dayanaklarını sarsan akışkan bir yapı sunmaktadır. Fiziksel sınırların anlamsızlaştığı siber uzayda, devletlerin denetim kapasitesi algoritmik duvarlar ve kapalı ekosistemler tarafından engellenmektedir. Egemenlik artık tek merkezli olmaktan çıkarak mali, altyapısal, veri odaklı ve normatif boyutlara bölünmüş parçalı bir yapıya dönüşmüştür (Hamadeh ve Amin, 2025). Bu makale, küresel ekonomik güç odağı haline gelen dijital platformların aynı zamanda yönetsel otorite haline geliş sürecini analitik bir perspektifle ele almakta; bu platformlar ile ulus devletler arasındaki etkileşimleri; mali güç, altyapı bağımlılığı ve regülatif reaksiyonlar boyutunda incelemektedir. Realist yaklaşımlar, devlet egemenliğini, ulusal sınırlar içerisindeki mutlak karar alma yetkisi olarak tanımlar (Hamadeh ve Amin, 2025). Fakat dijital çağda bu otorite, platformların teknik standartları tarafından kısıtlanmaktadır. Devletler, vatandaşlarının dijital yaşamlarını kontrol etmek istediklerinde, karşılarında devlet benzeri kapasitelere sahip teknoloji platformlarını bulmaktadır. Bu durum, egemenliğin "fiziki kontrolden" "algoritmik denetime" kaydığı bir süreci tetiklemektedir.

Tekno-devler, sundukları platform yönetişimi pratikleri aracılığıyla devletlerin geleneksel egemenlik alanlarını fiilen paylaşmaya hatta bazı kritik alanlarda bu rolleri ikame etmeye başlamıştır (Işıklı, 2024). Bu devasa şirketler hem kâr peşinde koşan ekonomik yapılar aynı zamanda norm belirleyici, güvenlik sağlayıcı ve kamuoyu şekillendirici aktörler olarak "de facto/fiili" politik güç kazanmışlardır. Beş büyük küresel aktör (Apple, Microsoft, Google, Amazon ve Meta), dijital evrenin hem fiziksel hem de mantıksal katmanını kontrol ederek (Işıklı, 2024) bir tür "platform devleti" simülasyonu yaratmaktadır. 2025 yılı itibarıyla

dijital egemenlik tartışmaları, devlet ile platformun iç içe geçtiği hibrit ve çatışmalı bir yönetim modeline odaklanmaktadır. Platformlar, kendi kural setlerini ve ekosistem sınırlarını belirleyerek devletlerin hukuk düzenine paralel birer "teknolojik hukuk" alanı inşa etmektedir. Bu süreç, uluslararası ilişkilerde devlet dışı aktörlerin ağırlığının daha önce hiç olmadığı kadar hissedilmesine neden olan sistemik bir dönüşümü temsil etmektedir (Korte, 2025).

### 1. Giriş: Ulus Devletler ile Tekno-devler Arasındaki Gerilime Dair Teorik Tartışmalar

Platform Egemenliği ve Ulus Devletin Dönüşümü yüzyılın ikinci çeyreğine girerken uluslararası sistem, Westphalia düzeninin ortaya koyduğu klasik egemenlik paradigmasından belirgin bir uzaklaşma sürecine girmiştir. Ulus devletin fiziksel sınırlar, hukuk tekeli ve zor kullanma yetkisi üzerine inşa edilmiş egemenlik modeli; küresel ölçekte faaliyet gösteren tekno-devlerin—(Apple, Microsoft, Google, Amazon, Meta gibi küresel altyapıyı, veriyi ve algoritmik ekosistemi kontrol eden şirketler) (Işıklı, 2024)—altyapısal, ekonomik ve algoritmik kapasitesi karşısında yeniden tanımlanmaktadır. Dijitalleşme, kamusal otoritenin ve yönetme erkinin kaynağına, işleyişine ve kurumsal sınırlarına dair devrimsel bir kırılmadır. Dijital hegemonyanın ana kategorileri aşağıda ifade edilmiştir.

Klasik egemenlik teorileri ve dijital çağın yarattığı gerilim: Uluslararası ilişkiler literatüründe egemenlik, genellikle devletin kendi toprakları üzerindeki mutlak ve bölünmez otoritesi olarak tanımlanır (Krasner, 1999; Lake, 2003). Realist yaklaşımlar devletin karar alma yetkisini dış müdahalelerden bağımsız bir güç olarak yorumlarken bu çerçeve iki varsayıma dayanır: (1) Sınırlar kontrol edilebilir, (2) Kamu otoritesi yalnızca devlet tarafından uygulanabilir. Dijital çağ bu iki varsayımı da geçersiz kılmıştır. Sınırlar siber uzayda geçirgen hale gelirken, kamu otoritesi işlevlerinin önemli bir kısmı artık platform altyapıları ve algoritmik ekosistemler tarafından yürütülmektedir. Böylece klasik egemenlik, teknik standartlar ve platform politikaları tarafından fiilen sınırlandırılan bir forma dönüşmektedir.

Ağ yönetimi yaklaşımı ve çok merkezli egemenlik: Ağ yönetimi teorileri, küresel dijital sistemin çok aktörlü ve yatay bir yapıya sahip olduğunu savunur (Slaughter, 2004; Nye, 2011). Bu modele göre egemenlik artık tek bir merkezde toplanmamaktadır; dijital altyapılar ulus devletlerin değil, özel şirketlerin mülkiyetindedir; veri akışı ve algoritmik kararlar devletlerden bağımsız işlemektedir. Bu nedenle dijital çağda egemenlik, mali, altyapısal, veri odaklı ve algoritmik olmak üzere birden fazla alt kategoriye bölünmüş durumdadır (DeNardis, 2014). Ulus devlet ile tekno-dev arasındaki güç çatışması, bu parçalı ve paylaşılmış egemenlik alanları üzerinde gerçekleşmektedir.

Dijital emperyalizm ve platform kapitalizmi: Eleştirel sosyal teori literatürü, platformların yükselişini yeni bir dijital emperyalizm biçimi olarak görür (Zuboff, 2019; Srnicek, 2016; Couldry & Mejias, 2019). Bu yaklaşıma göre veri yeni bir sermaye türüdür. Platformlar kamu işlevlerini özelleştirmekte, kullanıcı davranışları algoritmik gözetimle yönlendirilmektedir. Dijital altyapı özel şirketlerin elinde toplandıkça devlet dışı aktörler "fiili egemenlik" alanları oluşturmaktadır. Bu bakış açısı tekno-devlerin hem bir ekonomik aktör hem de norm koyucu ve kamu gücü üreten altyapısal operatörler olduğunu vurgular.

Algoritmik egemenlik: Lessig'in (1999) "code is law" yaklaşımı, dijital çağda hukuki düzenin yalnızca yasalarla değil, kod mimarisi ile şekillendiğini savunur. Bir platformun algoritması: Hangi içeriğin görünür olacağını, Kimin hangi hizmete erişebileceğini, Ekonomik işlemlerin nasıl gerçekleşeceğini devlet düzenlemesinden bağımsız biçimde belirleyebilir. Bu nedenle egemenlik artık yalnızca normatif hukukta değil, algoritmik tasarımda ve veri akışının kontrolünde somutlaşmaktadır (Yeung, 2018; Pasquale, 2015). Egemenliğin bu "kod tabanlı" niteliği, devlet ile platform arasındaki gerilimin temelini oluşturmaktadır.

Altyapıda dijital iktidar: Plantin, Lagoze ve Edwards (2018), dijital altyapıyı modern çağın yeni jeopolitik kaynağı olarak tanımlar. Bulut sistemleri, fiber ağlar, veri merkezleri, işletim sistemleri ve ödeme altyapıları üzerinde kontrol sahibi olan aktörler; bilgi akışının yönünü,

ekonomik ilişkilerin aracılığını, kamu hizmetlerinin işleyişini, güvenlik süreçlerini belirleme gücüne sahiptir. Dolayısıyla tekno-devler hem küresel entegrasyonu sağlar hem de küresel sistemde altyapısal iktidarın taşıyıcıları haline gelir.

Bu çalışma, dijital çağda egemenlik meselesini ele alan literatürdeki üç temel yaklaşımın kesişim noktasında konumlanmaktadır: Realist kuramların savunduğu mutlak ve bölünmez devlet egemenliğinin dijital ortamda sürdürülemez hale gelişi; ağ yönetişimi yaklaşımlarının işaret ettiği çok merkezli ve parçalı egemenlik modelinin yükselişi; ve eleştirel dijital ekonomi literatürünün tekno-devleri, altyapısal ve algoritmik iktidar kapasiteleri nedeniyle yeni tür “özel egemenler” olarak konumlandırması. Bu kuramsal çerçeve ışığında makale, tekno-devlerin mali güçleri, veri üzerindeki hakimiyetleri ve dijital altyapı üzerindeki tekelleşmeleri arttıkça, ulus devletlerin mali egemenlikten siyasi otoriteye, kamuoyu oluşturma kapasitesinden ulusal güvenliğe uzanan geniş bir alanda görece güç kaybına uğradığı yönündeki temel hipotezi benimsemektedir. Söz konusu hipotezi sınamak için tekno-devlerin fiili yönetsel otoriteler hâline geliş sürecini çok katmanlı bir analitik çerçeveye incelenmektedir. Çalışmada, mali egemenlik kaybı, altyapı bağımlılığı, veri mülkiyeti, algoritmik denetim, regülasyon rekabeti ve dijital sömürgecilik gibi temalar hem gelişmiş ekonomilerin düzenleyici stratejileri hem de gelişmekte olan ülkelerin dijital bağımlılığa karşı geliştirdikleri direnç mekanizmaları üzerinden değerlendirilmektedir. Bu amaçla 2025 yılı verileri kullanılarak küresel teknoloji şirketlerinin piyasa kapitalizasyonları devlet hazineleriyle karşılaştırılmış; para politikası üzerindeki platform etkileri, bulut altyapısı bağımlılığı, stablecoin ekosistemi, algoritmik yönetim ve platform merkezli kamu hizmeti ikameleri gibi yeni nüfuz alanları ayrıntılı biçimde analiz edilmiştir.

Bu kapsamlı analizler, makalenin sonraki bölümlerinde geliştirilen mali egemenlik tartışmalarına, altyapısal kırılganlık değerlendirmelerine ve ulus devletlerin düzenleyici egemenlik arayışına ilişkin politika önerilerine kuramsal ve ampirik bir temel oluşturmaktadır.

## 2. Mali Egemenlik ve Ekonomik Güç

Teknoloji şirketlerinin likidite kapasiteleri ve pazar kapitalizasyonları, orta ölçekli birçok devletin GSYİH'sini geride bırakarak küresel finansal sistemin ana taşıyıcıları haline gelmiştir. 2025 yılı verileri, tekno-devlerin ekonomik büyüklüğünün G7 ülkeleriyle doğrudan yarışır düzeye ulaştığını teyit etmektedir. Nvidia'nın 2025 ortası itibarıyla ulaştığı yaklaşık 4,57 trilyonluk dolarlık piyasa değeri, şirketi tek başına dünyanın en büyük dördüncü ekonomisi konumuna taşımıştır. Bu durumun en çarpıcı yönü, yalnızca 36.000 çalışanı olan bir şirketin, 124 milyon nüfuslu Japonya'nın yıllık ekonomik üretiminden daha fazla piyasa değerine sahip olabilmesidir (Girginov, 2026). Bu durum, ulus devletlerin egemenliğinin en somut dayanağı olan mali güç kategorisinde, tekno-devlerin devasa bütçeleri karşısında oransal bir gerileme yaşadığını göstermektedir.

**Tablo 1: Tekno-Devler vs. Devlet Ekonomileri**

| Ülke/Şirket | GSYİH/Piyasa Değeri (Trilyon USD) | Personel/Nüfus Ölçeği |
|-------------|-----------------------------------|-----------------------|
| ABD         | 30,61                             | 343 milyon            |
| Çin         | 19,39                             | 1,42 milyar           |
| Almanya     | 5,01                              | 84,5 milyon           |
| Nvidia      | 4,57                              | 36 bin                |
| Japonya     | 4,28                              | 124 milyon            |
| Hindistan   | 4,12                              | 1,43 milyar           |
| Microsoft   | 3,85                              | 220 bin               |
| Apple       | 3,78                              | 160 bin               |

Kaynak: Girginov, 2026; Frawley, 2026.

Tablo 1’de görülmekte olan şirket verileri Eylül 2025 piyasa kapitalizasyonunu, ülke verileri nominal GSYİH’yi temsil etmektedir. Bu veriler, ekonomik gücün emeğe dayalı üretimden, Yapay Zekâ çiplerine ve algoritmik sermayeye kaydığını göstermektedir. S&P 500 Endeksi’ndeki en büyük 10 şirketin, endeksin toplam ağırlığının %41’ini oluşturması, tarihin en yüksek piyasa yoğunlaşmasına işaret etmektedir (Frawley, 2026).

Tekno-devlerin küresel faaliyetleri, ulus devletlerin vergi toplama kapasitesini sistematik olarak aşındırmaktadır. Şirketler, fiziksel varlıklarının bulunmadığı ancak milyonlarca kullanıcıya sahip oldukları ülkelerden elde ettikleri kârları, düşük vergi oranlı bölgelere transfer edebilmektedir. Küresel ölçekte vergi adaletini sağlamak ve devletlerin vergi gelir kaybını azaltmak için geliştirilen kapsamlı bir uluslararası vergi düzenleme amacı taşıyan OECD’nin BEPS Projesi, bu boşlukları kapatmayı hedeflese de karmaşık fikri mülkiyet modelleri devletlerin somut egemenlik kaybını derinleştirmektedir. Bu durum, devletlerin kamu hizmetlerini finanse etme yeteneğini doğrudan tehdit eden bir bütçe krizine yol açmaktadır. ABD’nin kendi tekno-devlerini koruma refleksi ile Avrupa Birliği’nin dijital hizmet vergisi konusundaki ısrarı, mali egemenlik savaşının jeopolitik bir kriz haline dönüştüğünü göstermektedir. Vergi adaletsizliği, devletlerin sosyal kontratlarını zayıflatmakta ve halk nezdinde meşruiyet tartışmalarına yol açmaktadır (Bhatti, 2026).

Tekno-devler artık yalnızca ticaret platformları değil, aynı zamanda küresel finansal sistemin alternatif operatörleridir. Apple Pay’ın 2025 yılı itibarıyla yıllık 10 trilyon dolarlık işlem hacmine ulaşması, geleneksel bankacılık aracılığını devre dışı bırakmaktadır. Bu durum, bankaların mevduat kaybetmesine ve merkez bankalarının para politikası aktarım mekanizmalarının zayıflamasına yol açmaktadır (Radage, 2025). Öte yandan kripto paraların yüksek fiyat oynaklığını azaltmayı, kripto teknolojisini kullanırken fiyat istikrarı sağlamayı hedefleyen ve çoğu 1:1 oranında dolar gibi bir rezerv varlıkla desteklenen stablecoin (sabitkoin) kullanımı, bu dijital varlıkların "para" fonksiyonlarını üstlendiği yeni bir dönem başlatmıştır. 2025 yılı sonu itibarıyla stablecoin pazarının 300 milyar doları aşması ve yıllık işlem hacminin 10 trilyon dolara yaklaşması, devletlerin sermaye kontrollerini aşan bir likidite alanı yaratmaktadır. IMF ve ECB raporları, bu gelişmenin "dolarizasyon" riskini artırdığına dair ciddi uyarılar içermektedir (Adrian vd., 2025).

**Tablo 2: Dijital Finansal Ekosistem Metrikleri**

| Gösterge                        | Değer (USD) | Stratejik Etki                               |
|---------------------------------|-------------|----------------------------------------------|
| Apple Pay Yıllık İşlem Hacmi    | 10 Trilyon  | Bankacılık dışı likidite akışı               |
| Stablecoin Toplam Market Cap    | 300+ Milyar | Para politikası bağımsızlığı riski           |
| Stablecoin Yıllık İşlem Hacmi   | 10 Trilyon  | Sınır ötesi ödemelerde SWIFT alternatifi     |
| Dijital Cüzdan Kullanıcı Sayısı | 5,2 Milyar  | Finansal kapsayıcılık vs. Şirket bağımlılığı |

Kaynak: Clearly Payments, 2025; Deutsche Bundesbank, 2025; Dey, 2025; Adrian vd., 2025; Heaton, 2025.

Yukarıda görüleceği üzere Tablo 2, Tekno-devlerin salt birer ticari platformlar olmaktan çıktığını, ulus devletlerin temel egemenlik araçlarından biri olan "para basma ve finansal akışları kontrol etme" gücü kazandıklarını da göstermektedir. Apple Pay ve Stablecoin’lerin her biri, yıllık yaklaşık 10 trilyon dolarlık işlem hacmine ulaştığında, bu platformlar artık geleneksel bankacılık sisteminin birer eklentisi olmaktan çıkıp ona rakip birer paralel altyapı haline gelmiş oldular. Bu rakam, dünyanın en büyük ekonomisi olan ABD’nin yıllık GSYİH’sinin yaklaşık üçte birine tekabül eden bir ekonomik aktivitenin, devletlerin doğrudan denetimi dışındaki dijital kanallardan aktığını göstermektedir (Clearly Payments, 2025; ElectrolQ, 2025). Stablecoin pazarının 300 milyar doları aşması ve mevduatların bankalardan bu dijital varlıklara kayması, merkez bankalarının faiz oranları aracılığıyla ekonomiyi soğutma veya canlandırma yeteneğini zayıflatmaktadır. Bu yönüyle Tablo 2, "para politikası bağımsızlığı riski" notuyla devletlerin ekonomik kriz anlarında kullanabileceği en



güçlü araçların, platform bazlı bu yeni ekosistemler tarafından aşındırıldığını da ifade eder.

Siyasi bir silah olarak swift alternatifi, Stablecoin'lerin sınır ötesi ödemelerde bir SWIFT alternatifi olarak konumlanması, devletlerin finansal yaptırımlar ve sermaye kontrolleri üzerindeki egemenliğini sarsmaktadır. Özellikle Güneydoğu Asya'da B2B ödemelerin %43'ünün (Riseworks, 2025) bu kanallara kayması, devletlerin uluslararası para trafiğini izleme ve gerektiğinde bloke etme kapasitesinin "kod tabanlı" sistemlere devredildiğini kanıtlamaktadır. Ayrıca Tablo 2'nin son satırında görüleceği üzere; 5,2 milyar insanın dijital cüzdan kullanıcısı haline gelmesi, küresel nüfusun büyük bir kısmının günlük yaşamını sürdürmek için özel şirketlerin mülkiyetindeki yazılımlara bağımlı olduğunu göstermektedir. Bu durum, kamu hizmeti olması gereken finansal erişimin şirket inisiyatifine geçmesi riskini doğurarak devlet ile vatandaş arasındaki toplumsal sözleşmeyi, platform ile kullanıcı arasındaki hizmet şartları sözleşmesiyle ikame etmektedir. Özetle Tablo 2; mali egemenliğin artık fiziksel sınırlarla veya ulusal para birimleriyle değil, dijital ağların hızı ve kullanıcı derinliğiyle ölçüldüğü yeni bir dönemin başladığı şeklinde yorumlanmalıdır.

### 3. Dijital Egemenlik ve Siyasal Otorite

Dijital platformlar, vatandaşların bilgiye erişim kanallarını kontrol ederek devletlerin kamuoyu oluşturma tekelini ellerinden almıştır. Algoritmik yönetim, dikkat ekonomisi üzerinden rıza inşa eden modern bir iktidar biçimidir. Aşağıdaki tablo, bu şirketlerin 2025 mali yılı verilerine dayanarak hazırlanan yaklaşık kullanıcı sayılarını ve yıllık gelirlerini içermektedir.

**Tablo 3: 2025 Yılı Teknoloji Devleri Performans Tablosu**

| Platform/<br>Şirket              | Yaklaşık Kullanıcı Sayısı<br>(2025) | 2025 Yıllık Geliri<br>(Milyar \$) | Ana Gelir Kaynağı          |
|----------------------------------|-------------------------------------|-----------------------------------|----------------------------|
| Google<br>(Alphabet)             | 4 Milyar+ (Aktif Kullanıcı)         | ~403 Milyar \$                    | Reklam ve Bulut Hizmetleri |
| Amazon                           | 310 Milyon+ (Aktif Müşteri)         | ~637 Milyar \$                    | E-ticaret ve AWS (Bulut)   |
| Meta<br>(Facebook/<br>Instagram) | 4.1 Milyar (Günlük Aktif)           | ~201 Milyar \$                    | Dijital Reklamcılık        |
| Microsoft                        | 1.5 Milyar+ (Windows/<br>Office)    | ~282 Milyar \$                    | Azure Bulut ve Yazılım     |
| Apple                            | 2.4 Milyar+ (Aktif Cihaz)           | ~391 Milyar \$                    | iPhone ve Hizmetler        |

Kaynak: Amazon.com Inc., 2025; Meta Platforms, 2025; Alphabet Inc., 2025; Apple Inc., 2025.

Yukarıdaki Tablo 3'de görüleceği üzere, gelir lideri Amazon, özellikle perakende operasyonlarının devasa hacmi ve AWS (Amazon Web Services) bulut biriminin yüksek kârlılığı sayesinde toplam gelirden rakiplerine fark attığı görülmekte, 2025'te 600 milyar dolar barajını aşan ilk teknoloji devi olma yolunda ilerlemektedir (Amazon.com Inc., 2025). Sosyal medya tarafında ise Meta, günlük aktif kullanıcı sayısını 4,1 milyara ulaştırarak küresel erişim gücünü kanıtlamış ve reklam gelirlerini 201 milyar dolar seviyesine taşımıştır (Meta Platforms, 2025). Arama motoru ve bulut hizmetleri rekabetinde Alphabet (Google), 400 milyar dolar sınırını aşan geliriyle dijital reklamcılıktaki dominasyonunu korurken (Alphabet Inc., 2025); Microsoft, Azure bulut platformundaki büyüme sayesinde 282 milyar dolar gelir elde etmiştir (Microsoft Corporation, 2025). Donanım ve servis odaklı büyümesini sürdüren Apple ise, 2,4 milyardan fazla aktif cihaz ekosistemi üzerinden 391 milyar dolar gelir yaratarak karlılığını maksimize etmiştir (Apple Inc., 2025).

Algoritmalar, bireylerin neyi göreceğine karar veren modern "enformasyon eşik bekçileri"dir.

Google ve Meta, 2025 yılı itibarıyla küresel dijital reklam pazarının %55,8'ini kontrol ederek bilginin hiyerarşisini belirlemektedir. Bu güç konsantrasyonu, enformasyonun ticari ve siyasi amaçlarla manipüle edilmesine olanak tanıyan devasa bir kapasite sunmaktadır (Rodrigues, 2025). Diğer yandan yankı odaları, toplumsal kutuplaşmayı derinleştirirken demokratik müzakere ortamını zayıflatmaktadır (Advanced Television 2025). Algoritmik öneri sistemleri, seçim davranışlarını ve siyasi eğilimleri şekillendirerek "psiko-politik" bir egemenlik aracı olarak kullanılmaktadır (EU Digital Services Act, 2025). Bu süreçte karanlık desenler gibi manipülatif ara-yüz tasarımları, kullanıcıların rızasını platform çıkarları doğrultusunda yönlendirmektedir (Digital Services Act, 2025).

### 3.1. Veri Mülkiyeti: Devletin İstihbarat Kapasitesi ve Şirket Gizliliği Çatışması

Dijital egemenlik tartışmalarının en çetin cephesi veri mülkiyeti ve kontrolüdür. Veri, dijital egemenliğin temel yakıtıdır ve kontrolü devletler ile şirketler arasında çatışma yaratmaktadır. Devletler ulusal güvenlik gerekçesiyle verilere erişim talep ederken, şirketler uçtan uca şifrelemeyi bir "kurumsal egemenlik alanı" olarak savunmaktadır. Bir devletin vatandaşının verisine erişememesi, o devletin kendi yargı alanındaki asayiş kapasitesinin fiilen felç olması anlamına gelir (Rice, 2022).

Veri mülkiyeti tartışması, artık bireysel gizlilik sınırlarını aşarak devletin istihbarat kapasitesi ile şirketlerin teknik özerkliği arasındaki bir egemenlik mücadelesine evrilmiştir. 2025 yılında; Çin, Rusya, BAE, Suudi Arabistan, Vietnam, Endonezya ve Hindistan gibi ülkelerde en net şekilde görülen veri yerelleştirme yasaları verinin nerede saklandığının coğrafi egemenlik ile eşdeğer görüldüğünü göstermektedir. Avrupa Birliği ve Birleşik Krallık gibi bölgelerde ise dolaylı regülasyonlar bu trendi desteklemektedir (Trust Act, 2025). Veri mülkiyeti tartışması, artık bireysel gizlilikten ziyade devletin istihbarat kapasitesi ile teknoloji şirketlerinin teknik özerkliği arasındaki bir güç mücadelesidir. Bu durum, siber uzayda hukuki egemenliğin sınırlarını yeniden tanımlamayı zorunlu kılmaktadır (Shaikh, 2025). Bu noktada, teknoloji devlerinin veri üzerindeki hakimiyeti sadece ticari bir üstünlük değil, aynı zamanda politik bir güç gösterisine dönüşmüştür. Işıklı tarafından belirtildiği üzere: "Teknoloji devleri, sahip oldukları devasa veri havuzlarını ve bu veriyi işleme kapasitelerini kullanarak, devletlerin geleneksel olarak tekelinde bulundurduğu 'bilgiye dayalı yönetim' mekanizmalarına ortak olmaktadır. Veri mülkiyeti, platformların sadece ekonomik aktörler değil, aynı zamanda toplumun kılcal damarlarına sızan ve kamu otoritesini baypas edebilen de facto siyasi otoriteler haline gelmesini sağlamaktadır" (Işıklı, 2024). Teknoloji devlerinin sahip olduğu veri yönetimi gücü, hükümetleri etkilemede merkezi bir rol oynar çünkü yerel hükümetler, vatandaşlarına dair verilere ulaşma konusunda Tekno-devler ile iş birliği yapmak zorundadırlar. "Bu iş birliği, devletlerin teknoloji devlerine mecbur ve mahkûm olmalarıyla sonuçlanabilir" (Işıklı, 2024).

Devletlerin Tekno-devlerle iş birliği yapma mecburiyetinde kalması, devletlerin ulusal güvenlik yeteneğini doğrudan etkiler. Örneğin ABD, Hillary Clinton döneminde dış politika amaçları doğrultusunda çeşitli platformlardan yararlandığına dair iddialar gündeme gelmiştir. Örneğin "2011 yılında Arap Baharı patlak verdiğinde ABD Dış İşleri uzmanlarından bazıları Google'da çalışıyor, platformların ortak amaçlar doğrultusunda koordinasyonuna yardım ediyorlardı" (Işıklı, 2024). Bu durum, platformların sadece ekonomik aktörler değil, aynı zamanda egemen güçler tarafından dezenformasyon yaymak veya diğer ülkelerin iç siyasi süreçlerine müdahale etmek için kullanılan stratejik araçlar olduğunu göstermektedir. Veri mülkiyetinin bir siyasi silaha dönüştürülebileceğinin en net, Cambridge Analytica vakasıdır. Meta (Facebook), ABD başkanlık seçimleri sürecinde 146 milyon kullanıcının manipülatif ve yanlış bilgilere maruz kalmış olabileceğini kabul etmiştir. Bu noktada, veri mülkiyeti tartışması bireysel gizlilikten ziyade, devletin kamuoyu oluşturma tekeli ile platformların algoritmik rıza inşa etme kapasitesi arasındaki bir güç mücadelesine evrilmektedir (Işıklı, 2024).

Devletlerin vatandaş verilerine erişim talebi ile şirketlerin gizlilik politikaları arasındaki en büyük kırılma noktası uçtan uca şifrelemedir (E2EE). Hükümetler, şifrelemenin mahkeme kararıyla bile erişilemez bir alan yarattığını ve terörizm, çocuk istismarı gibi suçlarla mücadeleyi engellediğini iddia etmektedir. FBI gibi kurumlar, teknoloji şirketlerinden okunabilir içerik sağlamalarını talep ederken şirketler, sistemlerine eklenecek herhangi bir arka kapının genel siber güvenliği çökerteceğini ve kullanıcı güvenliğini yok edeceğini savunmaktadır. Bu çatışmanın en ikonik örneği olan Apple-FBI davasıdır. "FBI müfettişleri, San Bernardino saldırılarının failinde iPhone marka bir telefon ele geçirmişlerdi; telefon kilitli ve şifreliydi. Hükümet, Apple'a şifrenin çözülmesine yardımcı olmasını emretti fakat Apple bunu reddetti. Telefonun kilidini açmak için Apple'ın güvenlik yazılımına bir güvenlik açığı eklemesi gerekiyordu. Apple açısından bakıldığında, diğer tüm Apple cihazlarının güvenliğini ve dolayısıyla tüketici güvenliğini azaltacak tehlikeli bir girişimdi" (Işıklı, 2024). Bu olaydan sonra platformlar, kendilerini devlet müdahalesinden korumak adına teknik ve hukuki güvenliği artırmış, devletlerin sızamayacağı şifreli bağlantıları standart haline getirmişlerdir.

ABD'de 2025 yıl sonu verilerine göre, adli soruşturmalarda karşılaşılan şifreli içeriklerin %88'i kolluk kuvvetleri tarafından deşifre edilememektedir (Finlea, 2026). Bu durum, devletin kendi yargı alanındaki asayiş kapasitesinin fiilen felç olması ve egemenliğin "fiziki kontrolden" "algoritmik denetime" kayması anlamına gelmektedir.

#### 4. Şirket Odaklı Risk ve Avantaj Analizi

Tekno-devlerin her biri, dijital ekosistemin farklı bir katmanını domine ederek devletler üzerinde özgün bağımlılıklar yaratmaktadır.

##### 4.1. Altyapı Bağımlılığı: Microsoft ve Amazon Web Services (AWS) Örneği

Devletlerin e-devlet hizmetleri büyük ölçüde AWS ve Microsoft Azure gibi yabancı platformlara emanet edilmiştir. 2025 verilerine göre AWS pazarın %29-30'unu, Microsoft ise %20'sini kontrol etmektedir. Bu bağımlılık, "tek bir noktada toplanan hata" riskini ve stratejik bir kırılganlığı beraberinde getirmektedir (Haranas, 2025). Yani, bir devletin e-devlet hizmetlerinin %30'u AWS üzerinden sunuluyorsa, bu platformda yaşanacak teknik bir kesinti veya siber saldırı, devletin kamu hizmetlerini aynı anda felç ederek ulusal güvenlik krizi yaratabilir.

**Tablo 4: Küresel Bulut Altyapı Pazarı (Q3 2025)**

| Şirket          | Pazar Payı (%) | Temel Stratejik Alan                    |
|-----------------|----------------|-----------------------------------------|
| AWS (Amazon)    | 29 - 30%       | Kamu sektörü AI ve depolama             |
| Microsoft Azure | 20%            | Kurumsal yazılım ve devlet entegrasyonu |
| Google Cloud    | 13%            | Veri analitiği ve makine öğrenimi       |
| Diğerleri       | 37 - 38%       | Bölgesel ve niş sağlayıcılar            |

Kaynak: Haranas, 2025; Holori, 2025; Cargoson, 2025; HG Insights, 2025.

Küresel bulut pazarını izleyen Synergy Research Group ve Canalys gibi bağımsız kuruluşlarının 2025 yılı raporlarından derlenen Tablo 4'te sunulan pazar payı verileri, dijital dünyadaki otorite yoğunlaşmasının sadece ekonomik bir başarı değil, aynı zamanda devletlerin işleyişi üzerinde kurulan yapısal bir tahakküm olduğunu ortaya koymaktadır. Pazarın yarısından fazlasının iki şirket özelinde konsolide olması, ulus devletlerin dijital varlıklarını 'başkalarının mülkiyetindeki' topraklarda inşa etmesi sonucunu doğurmaktadır. Bu durum, istatistiksel bir veri olmanın ötesine geçerek, yabancı bir servis sağlayıcının hizmetini durdurması, bir devletin tüm kamu hizmetlerini felç edebilecek potansiyele sahiptir. Devletler, bu "bulut egemenliği" sorununu aşmak için kendi denetimlerindeki "Egemen Bulut" projelerine yönelmektedir (Fleming, 2025; European Commission, 2025).



Devlet kurumları, verilerini AWS veya Microsoft Azure gibi platformlara taşıdıklarında, kullanılan özel yazılım dilleri ve veri formatları nedeniyle başka bir sağlayıcıya geçmeleri imkânsız hale gelmektedir. Bu teknolojik hapis, devletlerin stratejik esnekliğini yok ederek onları platformun fiyat politikalarına ve teknik standartlarına kalıcı olarak mahkûm etmektedir (Işıklı, 2024). Geleneksel devlet otoritesi fiziki saldırılara karşı dirençli olsa da dijital altyapıdaki merkezi yoğunlaşma (Tablo 3'teki %50'lik pazar payı), yabancı bir şirketin hizmet şartlarını tek taraflı güncellemesi veya bir siber saldırı sonucu sistemlerini kapatması durumunda, devletin tüm vergi, sağlık ve güvenlik sistemlerinin saniyeler içinde çökmesine neden olabilir.

Altyapı mülkiyeti, jeopolitik krizlerde bir yaptırım aracına dönüşmektedir. Bir devletin siber savunma veya e-devlet sistemleri yabancı bir şirketin bulutunda saklanıyorsa, o devletin uluslararası ilişkilerde bağımsız karar alma kapasitesi, altyapıyı sağlayan şirketin merkez ülkesinin siyasi çıkarlarıyla sınırlandırılmaktadır. 2025 yılı itibarıyla devletlerin kendi yapay zekâ modellerini eğitmek için ihtiyaç duydukları yüksek hesaplama gücü, sadece bu dev şirketlerin veri merkezlerinde bulunmaktadır. Devletler, ulusal stratejilerini belirlemek için dahi bu şirketlerin hesaplama kaynaklarına "kira ödemek" ve onların algoritmik çerçevelerine uymak zorundadır. Devletlerin e-devlet hizmetleri, sağlık sistemleri ve savunma altyapıları bu platformlara derinlemesine entegre edilmiştir. Örneğin ABD Savunma Bakanlığı (DoD), NASA ve birçok Avrupa bakanlığı hassas verilerini AWS ve Microsoft Azure sunucularında barındırmaktadır. Bu durum, kamu hizmetlerinin yürütülmesini özel bir şirketin ticari kararlarına, güncellemelerine ve hizmet şartlarına bağımlı hale getirerek, devletin operasyonel özerkliğini zayıflatmaktadır (Marketing4Emmorce, 2025). Devletlerin bir bulut sağlayıcısından diğerine geçmesi teknik ve mali açıdan imkansıza yakın hale gelmiştir. Şirketlerin mülkiyetindeki kapalı API yapıları ve veriyi buluttan dışarı çıkarma maliyetleri, geçiş süreçlerini milyonlarca dolarlık bir yük haline getirmektedir. İngiltere Kabine Ofisi'nin (CDDO) raporları, kamu sektörünün önümüzdeki on yıl içinde adil fiyat pazarlığı yapma yeteneğini tamamen kaybedebileceği ve bu kilitlenme nedeniyle şirketlerin fiyatları tek taraflı belirleyeceği uyarısında bulunmaktadır (McKay, 2024).

Altyapı bağımlılığının en kritik boyutu, verinin fiziksel konumu ile hukuki aidiyeti arasındaki çatışmadır. ABD CLOUD Act uyarınca, veri fiziksel olarak Avrupa sunucularında olsa bile, servis sağlayıcı bir Amerikan şirketi olduğu sürece ABD hükümeti bu verilere erişim talep edebilmektedir. Bu durum, AB'nin GDPR (Genel Veri Koruma Yönetmeliği) kurallarıyla doğrudan çatışmakta ve devletleri vatandaşlarının verileri üzerinde tam denetim kuramaz hale getirmektedir (SoftwareSeni, 2025). Bu bağımlılığı kırmak için Avrupa Komisyonu, 2025 yılı sonunda 180 milyon avroluk bir "Sovereign Cloud" (Egemen Bulut) ihalesi açmış ve altyapıların tamamen AB yargı alanında, AB vatandaşı personel tarafından yönetilmesi şartını getirmiştir. Bu girişimler, devletlerin teknik altyapı üzerindeki kontrolü yeniden kazanarak "stratejik özerkliklerini" inşa etme çabasıdır (European Commission, 2025). Bu bağımlılık sarmalı, devlet ile vatandaş arasındaki "toplumsal sözleşmeyi" zayıflatarak, vatandaşın verisini ve güvenliğini devletin değil, bir şirketin insafına bırakmaktadır. Bu nedenle, "Milli Dijital Kamu Altyapıları" ve "Egemen Bulut" stratejileri, sadece bir teknoloji projesi değil, ulus devletin 21. yüzyılda hayatta kalma mücadelesidir.

#### 4.2. Bilgi Akışı Üzerinde Tekelleşme ve Algoritmik Denetim: Google ve Meta

Google ve Meta, dijital dünyanın "bilgi otoriteleri" olarak bilginin hiyerarşisini ve toplumsal etkileşimi yönetmektedir. Google arama pazarının %86'sına hükmederken Meta, sosyal medya etkileşiminin ana mecrası konumundadır. Bu şirketlerin algoritmik denetimi, hangi bilginin görünür kılınacağına dair mutlak bir otorite sunmaktadır (Advanced Television, 2025). Yapay zeka modelleri (Gemini ve Llama) aracılığıyla sunulan içerikler, platformların kendi değerlerini toplumlara empoze etmesine olanak tanır. Avrupa Komisyonu'nun bu platformlara yönelik "sistemik risk" soruşturmaları, bu etkinin devlet otoritesi için yarattığı tehditle ilişkilendirilmektedir (Pita vd., 2025). İnternetteki bilgi akışı üzerindeki otoritenin

bu denli tekelleşmesi, demokratik toplumlarda fikir çeşitliliğini ve tarafsız enformasyonu tehdit etmektedir.

Google ve Meta'nın kontrolü, yalnızca veriyi depolamanın ötesine geçerek enformasyonun üretim biçimini değiştiren "Ajan Yapay Zeka" (Agentic AI) evresine evrilmiştir (Review 2025). 2025 yılı itibarıyla Google, Gemini modelini doğrudan Chrome tarayıcısına ve Search ekosistemine entegre ederek, kullanıcıların bilgiye erişimini "tarafsız sonuç listelerinden" ziyade "algoritmik özetlere" (AI Overviews) dayalı bir modele dönüştürmüştür. Bu dönüşüm, OpenAI'nın Atlas ve Perplexity'nin Comet gibi yeni rakiplerine karşı atılmış stratejik bir hamle olmanın ötesinde, 650 milyondan fazla aktif kullanıcının neyi "doğru bilgi" olarak kabul edeceğini belirleyen teknolojik bir tekel yaratmaktadır (Keyword, 2025).

Meta ise dijital nüfuzunu, "Advantage+" reklam kampanyaları aracılığıyla öznelliğin tam otomasyonu üzerine kurmaktadır; şirket, 2026 yılı sonuna kadar tüm içerik üretim, hedefleme ve bütçe süreçlerini yapay zeka tarafından yönetilen bir sistem haline getirmeyi hedeflemektedir (Couldry ve Mejias, 2024). Bu süreç, Nick Couldry'nin "sembolik şiddet" olarak tanımladığı, bireylerin kendi arzularını platformun algoritmik sınıflandırmalarına göre yeniden yapılandığı bir egemenlik türünü tetiklemektedir. Meta'nın yalnızca Reels üzerinden yıllık 50 milyar dolarlık gelir elde etmesi, bu algoritmik yakalama mekanizmasının ne denli güçlü bir mali ve epistemik tahakküm aracı haline geldiğini doğrulamaktadır (Keyword 2025).

Algoritmik denetim ve yapay zeka entegrasyonu üzerinden kurulan bu otorite, dijital ekosistemin yazılımsal ve mantıksal katmanını mülkiyet altına almaktadır. Bu noktada, bilgi akışı üzerindeki bu esnek ve dinamik kontrol, dijital egemenliğin bir sonraki aşamasında yerini donanım ve yazılımın bütünleştiği daha katı ve geçirimsiz teknoloji duvarlarına bırakmaktadır.

#### 4.3. Teknoloji Duvarları: Apple'ın Kapalı Ekosistem ve Gizlilik Modeli

Apple, donanım ve yazılım arasında kurduğu "kapalı ekosistem" (walled garden) ile kullanıcılarını kendi dijital dünyasına hapsetmektedir (Chargeflow 2025; Clearly Payments, 2025). Apple Pay'in ABD'deki mobil debit cüzdan pazarında %92 paya sahip olması, şirketin bankacılık sistemine paralel dev bir güç odağı olduğunu kanıtlamaktadır (Emewulu, 2025). Ancak bu "teknoloji duvarları", ulus devletlerin denetim kapasitesini kısıtlayan birer "teknolojik sınır" haline gelmiş; özellikle uygulama mağazaları (App Store) üzerindeki mutlak kontrol, rekabetin engellenmesi ve verinin tekelleşmesi tartışmalarını beraberinde getirmiştir.

Avrupa Birliği, bu kapalı ekosistemlerin yarattığı piyasa tikanıklığını aşmak amacıyla Dijital Pazarlar Yasası (DMA) ile "kapı bekçisi" statüsündeki dev platformlara yönelik ex-ante kurallar getirmiştir. DMA uyarınca, 45 milyondan fazla kullanıcısı olan bu aktörler; kendi hizmetlerini kayırmama, üçüncü taraf uygulama mağazalarına izin verme ve mesajlaşma servislerinde birlikte çalışabilirliği sağlama gibi yükümlülöklere tabi kılınmıştır (Digital Watch, 2026). 2025 ve 2026 yıllarındaki uygulamalar, bu yasal duvarların somut sonuçlarını ortaya koymaktadır: Apple'ın iOS 26.3 sürümüyle ekosistemini üçüncü taraf aksesuarlara açması (Digital Watch, 2026), Google'a yönelik çevrim içi arama verisi paylaşımı (European Commision, 2025) ve Meta'nın AB kullanıcılarına kişiselleştirilmemiş reklam seçenekleri sunma taahhüdü, "ekosistem egemenliğinin" düzenleyici güç karşısındaki ilk büyük dönüşümünü simgelemektedir (European Commision, 2026).

Teknoloji devlerinin inşa ettiği bu kapalı ekosistemler ve ulus devletlerin bu yapılarla karşı geliştirdiği regülatif savunma mekanizmaları, dijital egemenlik mücadelesinin mikro ölçekteki tezahürleridir. Ancak, bu aktör odaklı dinamiklerin ötesinde, teknoloji platformlarının küresel sistemdeki varlığı, hem devlet kapasitesini artıran stratejik avantajlar hem de demokratik süreçleri ve ulusal güvenliği tehdit eden sistemik riskler arasında hassas bir denge yaratmaktadır

## 5. Küresel Risk - Avantaj Dengesi

Tekno-devlerin yükselişi, inovasyon hızı ile ulusal güvenlik dengesini sarsan bir "kazan-kaybet" senaryosu yaratmaktadır (Snyder, 2025).

### 5.1. Teknolojik İnovasyon ve Hızlı Çözüm Üretme Avantajı

Platformlar, hantal devlet bürokrasisinin aksine, devasa Ar-Ge bütçeleri sayesinde teknolojik sıçramaları tetiklemektedir (Işıklı, 2024). Tekno-devlerin piyasaya sunduğu Yapay Zekâ ve yüksek hesaplama gücü, sağlık bilimlerinden iklim değişikliğiyle mücadeleye kadar pek çok alanda devletlerin kapasitesini artırmaktadır. 2025 yılındaki AI patlaması, üretkenlikte yıllık %0,3'lük bir artış vaat ederek ekonomiye taze kan sağlamaktadır (European Central Bank, 2025). Teknolojik ivme, kamu hizmetlerinin dijitalleşmesini hızlandırarak verimli bir devlet yönetimi vaat etmektedir. Ancak bu avantaj, inovasyonun kontrolünün tamamen özel sektör elinde kalması riskini de beraberinde getirmektedir. Devletler, teknolojik gelişmeleri takip etmek için bu dev şirketlerle iş birliği yapmak zorunda kalırken yön belirleme yetkilerini kaybetmektedirler (OECD Digital Government Index, 2025).

Teknolojik inovasyonun hızı, teknoloji devlerinin devasa Ar-Ge bütçeleri ve çevik yapıları sayesinde devlet bürokrasisinin hantallığını etkisiz kılmaktadır. Evgeny Morozov (2013), bu durumu "teknolojik çözümçülük" (technological solutionism) kavramıyla ele alarak, Silikon Vadisi şirketlerinin devletin yetersiz kaldığı sosyal meseleler için pratik ve ucuz "anahtar teslim" dijital çözümler sunduğunu belirtmektedir. Bu süreçte devletler, kendi asli sorumluluklarını yerine getiremedikleri noktada teknoloji şirketlerinin sunduğu araçlara sığınmakta, bu da kamu otoritesinin teknik yetkinliğini yitirerek platformlara teslim olmasıyla sonuçlanmaktadır.

Marietje Schaaake (2024) ise "The Tech Coup" (Teknoloji Darbesi) adlı eserinde, demokratik hükümetlerin bu sorumlulukları özel sektöre devrederek kendi kapasitelerini "içini boşalttığını" savunmaktadır. Schaaake'ye göre devletler, AI ve siber güvenlik gibi kritik alanlarda teknoloji şirketlerinin hızı karşısında sindirilmiş ve "vergisini bile zamanında toplayamayan bir hantal yapı" karikatürüne hapsolmuştur. Nick Srnicek (2017) ise "Platform Kapitalizmi" eserinde, devletin bir zamanlar kendisinin finanse ettiği teknolojik inovasyonun artık tamamen özel platformların mülkiyetine geçtiğini ve bugün devletlerin bile bu şirketlerden altyapı kiralayan bağımlı aktörlere dönüştüğünü vurgulayarak, inovasyon avantajının devlet aleyhine kalıcı bir "operasyonel vesayet" yarattığını öne sürmektedir. Teknoloji devlerinin inovasyon hızı üzerinden kurduğu bu operasyonel vesayet, yalnızca sivil hizmetlerin işleyişini değil, devletin savunma ve güvenlik tekeli de doğrudan etkilemektedir. Bu bağlamda inovasyonun hızı, siber uzayın yeni savaş alanına dönüşmesiyle birlikte ulusal güvenliğin teknoloji şirketlerine devredilmesi riskini doğurmaktadır.

### 5.2. Siber Güvenlik ve Ulusal Güvenliğin Özelleşmesi Riski

Microsoft ve Google gibi şirketlerin siber güvenlik ağları, pek çok devletin istihbarat servisinde daha kapsamlıdır. Bu durum, ulusal güvenliğin özelleşmesi ve taşeronlaşması riskini doğurmaktadır (Latham ve Watkins, 2025). Geleneksel olarak devlet tekelinde olan güvenlik işlevleri, günümüzde teknoloji devlerine taşeronlaşma yoluyla devredilmektedir. Marietje Schaaake (2024), bu durumu "demokrasilerin siber güvenlik ve istihbarat gibi kritik alanlardaki sorumluluklarını özel sektöre devrederek kendi kapasitelerini içten içe boşaltması" olarak tanımlamaktadır. Schaaake'ye göre, şirketlerin kâr güdüsüyle hareket etmesi, kamu yararını ikincil plana iterek devletin siber uzaydaki otoritesini zayıflatmakta ve ulusal güvenliğin hesap verebilirliğini kurumsal yönetim kurullarının insafına bırakmaktadır. Kamu otoritesinin bu şekilde aşınması, sadece idari bir yetki devri değil, aynı zamanda siber savunma stratejilerinin kurumsal karlılık odaklı bir yapıya bürünmesi tehlikesini de beraberinde getirmektedir.

Bir devletin siber savunmasının yabancı bir şirkete bağımlı olması, egemenliğin teknik

bir vesayet altına girmesine yol açabilir. Bu özelleşme süreci, devletlerin siber savunma kapasitesini yabancı şirketlerin teknik standartlarına mahkûm ederek operasyonel egemenliğin kaybına yol açmaktadır. 2025 yılı verilerine göre, AWS ve Microsoft Azure gibi ABD merkezli sağlayıcıların Avrupa bulut pazarının %70'ini kontrol etmesi, siber savunmanın "altyapısal bağımlılığa" dönüştüğünü kanıtlamaktadır (Synergy Research Group, 2025). Francesca Bria'nın (2025) literatüre kazandırdığı "Otoriter Yığın" (Authoritarian Stack) kavramı; bulut platformları, yapay zekâ modelleri, finansal ağlar ve uydu sistemlerinin birleşerek devletin "fiili işletim sistemi" haline geldiği bu yeni kontrol mekanizmasını betimlemektedir. Bria'ya göre, ordular artık sadece yazılım satın almamakta, aksine hedefleme kararları ve istihbarat analizi gibi asli egemenlik yetkilerini kurumsal yönetim kurullarına devretmektedir; bu durum, devletin sistemden çıkışını imkânsız kılan teknik bir "altyapısal hapis" (infrastructural trap) senaryosu yaratmaktadır.

Ulusal güvenliğin bu şekilde özelleşmesi, kriz anlarında devletlerin bağımsız hareket kabiliyetini kısıtlamaktadır (Cyber Risk GmbH, 2025). Bu durumun yarattığı küresel asimetri, "Kuzey-Güney" meselesi olarak siber alanda dijital sömürgeciliğe dönüşmektedir. "Küresel Kuzey" (özellikle ABD ve Çin), altyapıyı ve algoritmik sermayeyi elinde tutan teknolojik hegemonlar olarak konumlanırken; "Küresel Güney" ülkeleri ise sadece ham veri üreten birer tarlaya indirgenmektedir. De Freitas'ın (2025) analiz ettiği üzere, verinin Güney ülkelerinden bedelsizce çekilip Kuzey'deki merkezlerde işlenmesi ve tekrar bu ülkelere hizmet olarak satılması, tarihsel sömürgeci bağımlılık ilişkilerini dijital çağda yeniden üretmekte ve geliştirmekte olan ülkelerin teknolojik özerkliğini imkânsız kılmaktadır.

Söz konusu bu dijital sömürgecilik düzeni, küresel sistemdeki aktörleri teknolojik kapasitelerine göre keskin sınırlarla birbirinden ayırarak yeni bir hiyerarşik yapı inşa etmektedir. Bu hiyerarşinin zirvesinde yer alan güçler, dijital ekosistemi kontrol etme yetenekleri sayesinde diğer uluslar üzerinde yapısal bir tahakküm kurmaktadır. İnternetin ABD, Çin ve AB blokları arasında bölünmesi (splinternet), küresel iletişimin evrenselliğini ihlal etmekte ve üçüncü dünya ülkelerine kapalı dijital adalar yaratmaktadır. Dijital ekosistemdeki tekelleşme, yalnızca ekonomik bir yoğunlaşma değil, Shoshana Zuboff'un (2019) "epistemik darbe" olarak tanımladığı toplumsal bir parçalanma sürecidir. Bu parçalanma, platformların tavsiye algoritmalarının kullanıcıları yankı odalarına hapsederek radikalleştirmesiyle gerçekleşmektedir. Algoritmalar, dikkat ekonomisinin gereği olarak en çok etkileşim alan—genellikle kutuplaştırıcı ve duygusal—içerikleri öne çıkararak toplumsal müzakere zeminini yok etmekte ve vatandaşları ortak bir gerçeklik algısından kopararak ideolojik "dijital gettolara" bölmektedir. Başka bir deyişle, bu parçalanma, küresel internet, artık tek bir ağ olmaktan çıkarak; Çin'in "Büyük Güvenlik Duvarı" ve Rusya'nın "Egemen İnternet" yasaları gibi ulusal bariyerlerle "dijital adalara" bölünmektedir. Dijital sömürgecilik altında ezilen toplumlar hem ekonomik hem de kültürel olarak küresel platformların normatif tahakkümü altına girmektedir (Nocetti, 2024). Asma Mhalla'nın (2025) vurguladığı üzere, bu siber alanlar, bilginin evrensel akışını engelleyerek her jeopolitik bloğun kendi kapalı enformasyon evrenini kurmasına yol açmakta; bu da küresel toplumsal bütünlüğü imkânsız kılan teknik ve ideolojik bir parçalanma yaratmaktadır.

Platformların yarattığı bu sistemik parçalanma ve egemenlik alanlarına yönelik algoritmik müdahaleler, ulus devletleri pasif birer izleyici olmaktan çıkararak aktif birer düzenleyici aktör olmaya zorlamaktadır. Tekno-devlerin kontrolsüz yükselişine karşı bir savunma refleksi geliştiren devletler, kaybettikleri otoriteyi hukuk ve denetim mekanizmaları aracılığıyla yeniden tesis etme arayışına girmişlerdir.

## 6. Ulus Devletlerin Reaksiyonu ve Regülasyonlar

Avrupa Birliği, teknoloji devlerini hukuk yoluyla evcilleştirmeyi hedefleyen en kapsamlı düzenleyici güç konumundadır. 2025 ve 2026 yıllarındaki uygulamalar, Dijital Pazarlar



Yasası (DMA) kapsamında "gatekeeper" statüsündeki platformlara yönelik müdahalelerin sonuçlarını somutlaştırmaktadır: AB Komisyonu, Apple'ı iOS ekosistemini üçüncü taraf aksesuarlara açmaya zorlamış, Google'a karşı çevrim içi arama verisi paylaşımı davaları açmış ve Meta'yı kullanıcılara kişiselleştirilmemiş reklam seçenekleri sunma konusunda taahhüt altına almıştır. Aynı zamanda Dijital Hizmetler Yasası (DSA) uyarınca, Elon Musk'ın Grok yapay zekâ sistemi ve X platformu üzerindeki tavsiye algoritmalarına yönelik "sistemik risk" soruşturmaları başlatılarak dezenformasyon üzerindeki platform denetimi, doğrudan devletin şeffaflık radarına sokulmuştur. Yapay zekâ alanında ise AB Yapay Zeka Yasası (AI Act), teknoloji devlerinin en güçlü modellerine karşı yeni bir sınır çekmiştir. Yasa, özellikle eğitiminde 1025 FLOPs hesaplama gücünden fazlasını kullanan modelleri "sistemik risk" kategorisine alarak çok sıkı denetimlere tabi tutmaktadır. Bu teknik eşik, egemenlik mücadelesinin artık sadece yasalarla değil, işlem gücü ve veri yığınları üzerinden kurulan bir "model egemenliği" savaşına dönüştüğünü kanıtlamaktadır.

ABD ve Çin'in stratejik yaklaşımları, dijital egemenliği birer jeopolitik güç yarışı olarak kurgulamaktadır. ABD, pazar odaklı "liberal" bir strateji izleyerek kendi tekno-devlerini şirketlerini küresel nüfuzun taşıyıcıları olarak korurken; ulusal güvenliğini tehdit eden yabancı platformlara karşı (örneğin TikTok) dağıtım ve güncelleme yasağı, internet barındırma hizmetlerinin kısıtlanması gibi sert yasaklar uygulamakta ve siber uzayı kendi şirketleri aracılığıyla denetlemeye çalışmaktadır. CHIPS Yasası ile donanım katmanında üretim egemenliğini geri kazanmayı hedeflemektedir (Tekin, 2025). Washington, bu yolla kendi özel şirketlerinin teknik kapasitesini devletin stratejik hedefleriyle uyumlu hale getirmeyi amaçlamaktadır. Çin ise "siber egemenlik" modeliyle devlet kontrolünü merkeze alan bir strateji izlemektedir. Made in China 2025 Planı ile dışa bağımlılığı azaltmayı, kendi yerli devlerini küresel standartlara taşımayı amaçlamaktadır. Çin, Dijital İpek Yolu Projesi ile kendi teknolojik standartlarını Küresel Güney'e yayarak ABD hegemonyasına alternatif bir blok inşa etmektedir (Wang, 2025).

Bu regülatif müdahaleler, teknoloji devlerinin operasyonel sınırlarını belirleyen ve ulus devletlerin hukuki egemenlik alanını yeniden inşa eden yaptırım gücü yüksek bir yol haritası sunmaktadır.

**Tablo 5: AB Dijital Regülasyon Çerçevesi (2025-2026)**

| Yasa / Kriter    | Hedef / Eşik                  | Temel Yükümlülük                                |
|------------------|-------------------------------|-------------------------------------------------|
| DSA              | Çok Büyük Platformlar (VLOPs) | Algoritma şeffaflığı, içerik moderasyonu        |
| DMA              | Eşik Bekçileri (Gatekeepers)  | Birlikte çalışabilirlik, veri taşınabilirliği   |
| AI Act           | GPAI Modelleri                | Risk analizi, telif haklarına uyum              |
| Systemic Risk AI | > 1025 FLOPs Compute          | Zorunlu model değerlendirmesi ve siber güvenlik |

Kaynak: Griffiths, 2025; European Union, 2025

Yukarıda bulunan Tablo 5, AB'nin tekno-devlerinin pazar ve veri hakimiyetini hukuk yoluyla sınırlamak için oluşturduğu dört ana sütunu özetlemektedir. Bu tablonun içeriği ve stratejik anlamı şu şekildedir: DSA, aylık 45 milyondan fazla kullanıcısı olan "Çok Büyük Çevrim İçi Platformları" (VLOPs) hedef almaktadır (Digital Watch 2025). Temel yükümlülüğü, platformların algoritmik şeffaflığını sağlamak ve yasadışı içeriğe karşı hızlı moderasyon yapmaktır. Kurallara uyulmaması durumunda teknoloji devleri, küresel cirolarının %6'sına kadar varan devasa para cezalarıyla karşı karşıya kalabilmektedir (European Commission, 2026). DMA, pazarın kapı bekçisi konumundaki Apple, Google ve Meta gibi aktörleri denetlemek amacıyla geliştirilmiştir. Kapı bekçisi şirketlerin kendi hizmetlerini kayırmamasını yasaklamakta; mesajlaşma servislerinde birlikte çalışabilirliği ve kullanıcıların verilerini taşıyabilmesini zorunlu kılmaktadır. Ağır ihlaller durumunda, AB'nin bu şirketlerin iş



kollarını ayırma yetkisi bulunmaktadır (GMFUS, 2025). AI Act, genel amaçlı yapay zeka (GPAI) modelleri geliştiren sağlayıcıları kapsamaktadır. Bu modellerin eğitim süreçlerinde telif haklarına uyum ve teknik dokümantasyon sunma gibi risk odaklı yükümlülükler getirmektedir (Artificialintelligence.eu, 2025). Sistemik Risk Taşıyan AI Modelleri, AI Act kapsamında, eğitiminde 1025 FLOPs ve üzerinde hesaplama gücü kullanılan modeller (Gemini veya GPT-5 gibi) en sıkı denetim katmanına alınmaktadır (Harwood, 2025). Bu eşiği aşan modeller, sistemik risk kategorisinde değerlendirilerek zorunlu siber güvenlik protokollerine ve bağımsız model değerlendirmelerine tabi tutulmaktadır (Artificialintelligence.eu, 2025). Özetle bu tablo, teknoloji devlerinin operasyonel sınırlarını belirleyen ve ulus devletlerin hukuki egemenlik alanını yeniden inşa eden yaptırım gücü yüksek bir yol haritasıdır. Bu çok kutuplu regülasyon ve strateji yarışı, teknoloji devlerinin sunduğu verimlilik ile devletlerin aradığı denetim arasındaki gerilimin küresel bir 'yeni normal' olduğunu tescil etmektedir. Geleceği dünyasında egemenlik, ulus devletlerin bu teknik ve idari araçları ne ölçüde kendi lehlerine dönüştürebileceklerine bağlıdır; bu durum ise çalışmanın sonuç kısmında ele alınan bütüncül politika yaklaşımlarını birer zorunluluk haline getirmektedir.

## 7. Sonuç ve Politika Önerileri

Geleceğin politika tasarımı için dijital egemenliğin tek boyutlu bir veri güvenliği meselesi olmaktan çıkarılıp, ölçülebilir bir çerçeveye oturtulması elzemdir. Rodriguez Pita vd. (2025) önerdiği model uyarınca egemenlik; teknolojik (endüstriyel kapasite), devlet (yasal denetim) ve sosyal (vatandaş hakları) olmak üzere üç ana katmanda takip edilmelidir. Bir ülkenin egemenlik seviyesi yalnızca koyduğu yasalarla değil, siber altyapısının yerlilik oranı, vatandaşlarının yabancı platformlara olan veri bağımlılığı ve kriz anlarında siber savunmasını kendi personeliyle yönetme kapasitesiyle ölçülmelidir. Devletlerin ve uluslararası blokların dijital özerkliklerini inşa edebilmeleri için şu somut adımları atmaları stratejik bir zorunluluktur:

Milli Dijital Kamu Altyapıları (DPI): Devletler, kritik sosyal ve ekonomik süreçleri teknoloji devlerinin insafından kurtarmak için "kamu yararı odaklı" altyapılar inşa etmelidir. Hindistan'ın Aadhaar/UPI ve Brezilya'nın PIX sistemleri, kamu eliyle yönetilen ama piyasa inovasyonuna açık "açık kaynak" altyapıların teknoloji devlerine olan finansal bağımlılığı nasıl azalttığına en somut örnekleridir (De Freitas, 2025).

Egemen Bulut ve Teknoloji Yatırım Fonları: "Altyapısal hapis" riskini kırmak için ulusal veya bölgesel "Egemen Bulut" girişimleri hayata geçirilmelidir. Avrupa Birliği'nin 180 milyon avroluk European Commission, 2025) ihale modeli ve önerilen €300 milyar değerindeki "Avrupa Egemen Teknoloji Fonu" (ESTF), yerli start-up'ların ve kritik teknoloji şirketlerinin (DeepMind veya ARM örneğinde olduğu gibi) yabancı tekeller tarafından yutulmasını önleyecek finansal bir kalkan görevi görmelidir (Bria vd., 2025).

Kolektif Regülasyon ve "Dijital Bandung" İttifakı: Küresel Güney ülkeleri, tek başlarına teknoloji devleri karşısında zayıf kalmaktadır. 20. yüzyılın siyasi bağımsızlık hareketlerinden ilham alan bir "Dijital Bandung" platformu kurulmalı; bu platform üzerinden veri mülkiyeti, dijital vergilendirme ve algoritmik şeffaflık konularında ortak pazarlık gücü oluşturulmalıdır (De Freitas, 2025).

Bağımsız Dijital Yönetişim Kurulları: Teknoloji devlerinin denetimi, hantal bürokratik yapılar yerine; operasyonel güce ve teknik uzmanlığa sahip, Avrupa Merkez Bankası modeline benzer özerk ve liyakatli "Dijital Yönetişim Kurulları" tarafından yürütülmelidir. Bu kurullar, platformların öneri algoritmalarını denetleyerek yankı odalarını kırmalı ve demokratik süreçlerin algoritmik manipülasyonuna karşı anlık müdahale kapasitesi geliştirmelidir.

Algoritmik Okuryazarlık ve Direnç Kapasitesi: Vatandaşların sadece "pasif kullanıcı" olmaktan çıkıp "aktif dijital vatandaşlara" dönüşmesi sağlanmalıdır. Eğitim müfredatları; algoritmik profil çıkarma, "karanlık desenler" ve dezenformasyon tekniklerine karşı

savunma mekanizmalarını içerecek şekilde güncellenmeli, toplumsal direnç kapasitesi bir ulusal güvenlik önceliği olarak kabul edilmelidir.

Geleceğin dünyasında egemenlik ne sadece devletlerin elindeki mühürde ne de sadece şirketlerin yazdığı kodda olacaktır. Bu iki güç arasındaki dinamik gerilimin yarattığı yeni yönetim mimarisi, insanlığın dijital kaderini tayin edecektir.

## 5. Kaynakça

- Adrian, T., Bains, P., Bechara, M., Cerutti, E., Forte, S., Grinberg, F., Gullo, A., Hengge, M., Jekabsone, A., Kao, K., Mancini Griffoli, T., Martinez Peria, S., Miccoli, M., Reuter, M., & Sugimoto, N. (2025). Understanding stablecoins. Washington, DC: International Monetary Fund.
- Alphabet Inc. (2025). Alphabet announces fourth quarter and fiscal year 2025 results. <https://www.abc.xyz/investor/> Erişim tarihi: 13.02.2026.
- Amazon.com Inc. (2025). Amazon.com announces fourth quarter results. <https://ir.aboutamazon.com/> Erişim tarihi: 13.02.2026.
- Amin, H., Cochrane, L., & AlKaabi, N. (2025). Globalization and national identity: A qualitative approach. National Identities.
- Apple Inc. (2025). Apple reports fourth quarter results. <https://www.apple.com/investor/> Erişim tarihi: 13.02.2026.
- Bofinger, P. (2025). Stablecoins and the future of money: Economic principles and policy implications. Hans-Böckler-Stiftung, Study No. 100.
- Bria, F. (2025). The Authoritarian Stack: Mapping Big Tech's capture of state power. Rosa Luxemburg Stiftung.
- Chargeflow. (2025). Apple Pay vs Google Pay statistics, adoption rates & market share.
- Clearly Payments. (2025). Payment stats that will blow your mind and change your strategy.
- Couldry, N., & Mejias, U. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
- Cyber Risk GmbH. (2025). European cyber defence policy and digital sovereignty report.
- De Freitas, M. V. (2025). Digital sovereignty and data colonialism: Shaping a just digital order for the Global South. Policy Center for the New South, PP-38/25.
- Dey, M. K., & Wang, C. (2022). Asymmetric volume volatility causality in dual listing H-shares. *Journal of Asset Management*, 23(5), 419-428.
- Digital Watch. (2026). Digital Governance Act as an instrument for strengthening the European Union's digital sovereignty.
- Emewulu, C. U. D. (2025). Apple Pay market share and mobile debit wallet transactions. Chargeflow Research.
- European Commission. (2025). Call for evidence for an impact assessment: EU Cloud and AI Development Act.
- Finklea, K. (2026, January 12). Law Enforcement and Technology: The "Lawful Access" Debate (CRS In Focus No. IF11769). Congressional Research Service. <https://www.congress.gov/crs-product/IF11769>
- Fleming, S. (2025). Europe's drive for digital sovereignty and sovereign cloud. World

- Economic Forum.
- Frawley, T. (2026). The “Great Narrowing”: S&P 500 concentration. RBC Wealth Management.
- Girginov, B. (2026). How Nvidia's market cap stacks up against entire countries. Visual Capitalist.
- Griffiths, T. L. (2025). AI agents should be regulated based on the extent of their autonomous operations. OpenReview.
- Hamadeh, S., & Amin, H. (2025). AI, education and digital sovereignty. *Frontiers in Education*, 10, 1677727.
- Haranas, M. (2025). Global cloud infrastructure market share report Q3 2025. CRN.
- Harwood, S. (2025). EU obligations on providers of GPAI models under the EU AI Act.
- Heaton, J., & Lucas, D. (1995). The importance of investor heterogeneity and financial market imperfections for the behavior of asset prices. *Carnegie-Rochester Conference Series on Public Policy*, 42(1), 1-32.
- HG Insights. (2025). Microsoft Azure market share & buyer landscape report.
- Işıklı, Ş. (2024). Teknoloji devleri vs. yerel devletler: Platformlar politikleşiyor mu? *Tarih Bilinci*, 44(44), 8–14.
- Korte, M. (2025). Digital sovereignty in 2025: The new frontier of tech independence. *Forbes Tech Council*.
- Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.
- Lake, D. A. (2003). *Hierarchy in international relations*. Cornell University Press.
- Latham & Watkins. (2025). China's CAC announces new cybersecurity incident reporting measures.
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Marketing4Ecommerce. (2025). Amazon, Google and Microsoft divide 60% of the global cloud.
- McKay, R. (2024). Keeping the door open: UK public sector and open-source AI models. *Cabinet Office*.
- Meta Platforms, Inc. (2025). Meta reports fourth quarter and full year 2025 results. <https://investor.fb.com/> Erişim tarihi: 13.02.2026.
- Mhalla, A. (2025). *Cyberpunk: The empire of compute and the new geopolitics of sovereignty*. Seuil.
- Microsoft Corporation. (2025). Earnings release FY25 Q4. <https://www.microsoft.com/en-us/investor/> Erişim tarihi: 13.02.2026.
- Nocetti, J. (2024). A splintered internet? Internet fragmentation and the strategies of China, Russia, India and the European Union. *Études de l'Ifri*.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Qelichi, M. M., Ghasemi, K., & Moradhasel, N. (2025). Strengthening digital sovereignty: A structural analysis of digital governance indicators. IGI Global.
- Radage, D. (2025). Apple Pay and other digital wallets market share in 2025. *Clearly Payments*.

- Review. (2025). Agentic AI: Autonomy, adaptability and goal-driven reasoning. MDPI.
- Rice, N. F. (2022). Data embassies, sovereignty and continuity for nation-states. Georgetown Security Studies Review.
- Riseworks. (2025). 2025 Crypto payroll report: Global adoption, market share, and compensation trends.
- Rodrigues, R. (2025). Motivations in the adoption and conversion of digital advertising services. *Review of Managerial Science*, 19(7), 2127-2148.
- Rodriguez Pita, M. P., Pérez Martínez, J. E., & Urueña López, A. (2025). From concept to method: A framework for measuring digital sovereignty. ITS 33rd European Conference.
- Schaake, M. (2024). *The Tech Coup: How to save democracy from Silicon Valley*. Princeton University Press.
- Shaikh, S. (2025). India's search for digital sovereignty and data localization. Tech Policy Press.
- SoftwareSeni. (2025). Navigating EU Data Act and Digital Markets Act cloud compliance.
- Snyder, J., & Lonergan, E. D. (2025). Cultural change in military organizations: Hackers and warriors in the US Army. *Texas National Security Review*, 8(3), 74-95.
- Srnicek, N. (2016). *Platform capitalism*. Polity Press.
- Tekin, F. (2025). The European Chips Act and defense industry supply chains. European Parliament Think Tank.
- TrustArc. (2025, Ekim 12). Data localization and global privacy laws: How to manage the regulatory patchwork. TrustArc. <https://trustarc.com/resource/data-localization-global-privacy-laws/>
- Wang, B. (2025). The Digital Silk Road: China's strategy for global technological leadership. *International Journal of Artificial Intelligence*.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.