

Dijital Dönüşüm Çağında **Veri Kapitalizmi, Modern Emperyalizm ve Teknofeodalizm**





DİJİTAL DÖNÜŞÜM ÇAĞINDA VERİ KAPİTALİZMİ, MODERN EMPERYALİZM ve TEKNOFEODALİZM

DİJİTAL DÖNÜŞÜM ÇAĞINDA VERİ KAPİTALİZMİ, MODERN EMPERYALİZM ve TEKNOFODALİZM

İmtiyaz Sahibi

Kalkınma Odaklı Stratejik Araştırmalar Merkezi adına
Lütfi Can BAŞARAN

Editör

Koray GÜÇLÜ

Hazırlayan

Feyzullah YEĞİN

Kapak

Nevzat PEKKARPUZ

Baskı Yeri, Yılı

Konya, 2026

E-ISBN

978-625-92621-5-4

KOSAM

Akabe Mah. Alaaddin Kap Cad.

No:130 42020 Karatay / Konya

www.kosam.org

KTO Karatay Üniversitesi Yayınları

Ocak 2026

Bu yayının tüm hakları KOSAM'a aittir. KOSAM'ın izni olmadan yayının tümünün veya bir kısmının elektronik veya mekanik (fotokopi, kayıt ve bilgi depolama vd.) yollarla basımı, yayımı, çoğaltılması veya dağıtımı yapılamaz. KTO Karatay Üniversitesi Bilimsel Araştırma Projeleri (BAP) kapsamında desteklenen bu çalışmadan, kaynak göstermek sureti ile alıntı yapılabilir.

ÖNSÖZ

Günümüzde, veri kapitalizmi, insanların internetteki verilerin düzenli olarak toplanması, incelenmesi ve bu veriler üzerinden ekonomik veya siyasi kazanç elde edilmesi süreciyle birlikte köklü bir dönüşümden geçmektedir. Bu dönüşüm sürecinde, büyük dijital platformların yükselişi, algoritmik tahakküm ve dijital sömürü gibi kavramlar, bilimsel, ekonomik, çevresel, sosyal ve etik açılardan dikkat çeken yeni bir araştırma alanı olarak öne çıkmaktadır. Dijital platformlar, iş yapış şekillerinden toplumsal eğilimlere kadar geniş bir alanda ekonomik ve sosyal etkiler oluşturarak, pazar kontrolünü ele geçirmiş ve tekelleşmeyi artırmıştır.

Kalkınma Odaklı Stratejik Araştırmalar Merkezi (KOSAM) olarak yürüttüğümüz bu rapor çalışmasında, veri kapitalizmi ve dijital egemenlik konusunu “her yönüyle” ele alarak, dijital ekonominin geleceğinde karşılaşılabilecek fırsatları, riskleri ve politika gereksinimlerini kapsamlı biçimde değerlendirdik. Rapor; veri toplama ve algoritmik işleme teknolojilerinden, ekonomik tekelleşmeye ve veri rantına, siber bağımlılık gibi sosyal ve zihinsel sağlık etkilerinden, etik ve toplumsal boyutlara (kişisel gizlilik ve sömürü), regülasyon modellerine (KVKK’nın GDPR ile uyum zorunluluğu) kadar pek çok başlığı bütüncül bir perspektifle analiz etmektedir. Bu analizde, platform devlerinin “dijital derebeyleri” rolünü üstlenmesiyle, kullanıcıların ve işletmelerin “dijital serfler” konumuna indirgendiği teknofeodalizm yaklaşımı da incelenmektedir.

Bu çalışma, yalnızca veri kapitalizminin işleyişini tanıtmakla kalmayıp, aynı zamanda algoritmaların KOBİ’ler ve çalışanlar üzerindeki yönetsel gücü, yerel girişimlerin küresel bulut hizmetlerine olan zorunlu bağımlılığı (vendor lock-in) gibi yapısal değişimleri de değerlendirmektedir. Rapor, ayrıca Türkiye’nin küresel veri sistemine veri üreterek destek olmasına rağmen, bu verileri ekonomik, teknolojik ve kültürel değere çevirme konusundaki sınırlı yeteneğini ve politika yapıcılarının önünde bulunan seçenekleri de değerlendirmektedir. Bilimsel verilere, uluslararası regülasyon örneklerine (GDPR) ve güncel sektör dinamiklerine dayanan bu rapor, teknolojiyi savunmak ya da reddetmek yerine, mevcut veriler üzerinden çok boyutlu ve dengeli bir analiz sunmaktadır.

KOSAM olarak, küresel veri adaleti tartışmalarına katkıda bulunulması, yerli ve açık kaynaklı dijital çözümlerin teşvik edilmesi ve etik duyarlılıklara (gizlilik hakkı, hesap verebilirlik, unutulma hakkı) dayalı bir kalkınma vizyonunun desteklenmesi yönündeki çalışmalarımıza devam ediyoruz. “**Dijital Dönüşüm Çağında Veri Kapitalizmi, Modern Emperyalizm ve Teknofeodalizm**” raporunun, akademi, kamu otoriteleri, özel sektör ve sivil toplum kuruluşları için dijital ekonomilerdeki dönüşüm sürecine dair yol gösterici bir kaynak olacağına inanıyoruz.

İÇİNDEKİLER

ÖNSÖZ	i
İÇİNDEKİLER	ii
TABLolar DİZİNİ.....	iv
YÖNETİCİ ÖZETİ	1
GİRİŞ	5
1. VERİ KAPİTALİZMİNİN KURAMSAL TEMELLERİ VE VERİ MÜLKİYETİ.....	7
1.1. Veri Kapitalizmi	7
1.2. Veri Üretiminde Mülkiyet	8
1.2.1. Veri Mülkiyetinin Belirsizliği.....	8
1.2.2. Veri Mülkiyetinde Yeni Yaklaşımlar ve Öneriler Nelerdir?	9
2. DİJİTAL EKONOMİ VE PLATFORM KAPİTALİZMİ.....	10
2.1. Dijital Platform Ekonomisinin Yapısı	10
2.1.1. Temel Bileşenler	11
2.1.2. Dijital Platform Ekonomisinin Etkileri	11
2.2. Büyük Teknoloji Şirketlerinin Ekonomik ve Siyasal Gücü	13
2.2.1. Dijital Platformların Ekonomik Güçleri	15
3. DİJİTAL DÜZENDE HAKLAR, MAHREMİYET VE RİSKLER	19
3.1. Bireysel Mahremiyet.....	19
3.2. Gözetim Toplumu	21
3.3. Dijital Haklar.....	22
3.4. Dijital Haklar Nasıl Korunur?	26
3.5. Kültürel ve Toplumsal Mücadele	26
4. YAPAY ZEKÂ VE ALGORİTMİK KARAR ALMA	28
4.1. Veri Kapitalizminde Algoritmik Kararlar	29
4.2. Siber Bağımlılık ve Dijital Altyapı Eşitsizlikleri	30
4.2.1. Dijital Bağımlılığın Psikolojik Nedenleri	30
4.3. Dijital Altyapı Eşitsizlikleri	32
4.3.1. Dijital Altyapı Eşitsizliğinin Boyutları.....	32
4.3.2. Dijital Altyapı Eşitsizliğinin Sonuçları ve Çözüm Önerileri	34

5. ULUSLARARASI VERİ POLİTİKALARI VE DİJİTAL EGEMENLİK.....	35
5.1. Uluslararası Veri Politikaları.....	35
5.1.1. Veri Politikalarının Kapsamı ve Kavramsal Çerçeve.....	35
5.1.2. Temel Uluslararası Yaklaşımlar	35
5.2. Veri Konusunda Uluslararası Çatışma ve İş Birliği Alanları	36
5.2.1. Çatışma Alanları	37
5.2.2. İş Birliği Alanları	38
5.3. Dijital Egemenlik	42
6. MODERN EMPERYALİZM ÇAĞINDA DİJİTAL SÖMÜRÜ DÜZENİ	44
6.1. Dijital Sömürünün Mekanizmaları	45
6.2. Dijital Sömürüye Direniş ve Alternatifler	46
6.3. Sonuç: Dijital Emperyalizme Karşı Yeni Bir Dayanışma.....	48
7. TEKNOFEODALİZM.....	50
7.1. Orta Çağ Avrupa'sıyla Günümüz Dijital Ortamındaki Benzerlikler	50
7.2. Teknofeodalizmi Ortaya Çıkaran Dinamikler	50
7.3. Günlük Yaşamda Teknofeodalizmin Etkileri	51
7.4. Teknofeodalizmin Türkiye'deki Durumu.....	51
8. TÜRKİYE'DE VERİ KAPİTALİZMİ VE DİJİTAL SÖMÜRÜYLE MÜCADELE	54
8.1. Türkiye'de Veri Kapitalizminin Temel Boyutları.....	54
8.2. Türkiye'nin Veri Kaynakları Üzerinden Sömürülme Riskleri	56
8.3. Türkiye'de Veri Kapitalizmine Dair Güncel Gelişmeler	56
8.4. Yasal ve Kurumsal Reformlar	57
8.5. Uluslararası İş Birlikleri.....	59
8.6. Türkiye İçin Dijital Egemenlik ve Direniş Yol Haritası.....	59
KAYNAKÇA	62

TABLolar DİZİNİ

Tablo 1: Veri Üzerindeki Hak Talepleri	8
Tablo 2: Dijital Platform Ekonomisinin Yapısı.....	10
Tablo 3: Pazar Hakimiyeti	15
Tablo 4: Dijital Platformların Ekonomik ve Siyasal Gücü	18
Tablo 5: Mahremiyetin Korunması için 3 Temel Aşama.....	20
Tablo 6: Dijital Sömürüye Direniş Alanları: Bireysel Düzeyde	47
Tablo 7: Dijital Sömürüye Direniş Alanları: Toplumsal Düzeyde	47
Tablo 8: Dijital Sömürüye Direniş Alanları: Politik ve Hukuki Düzeyde	48
Tablo 9: Türkiye’de Veri Kapitalizminin Görünümleri	54
Tablo 10: Algoritmik Yönlendirme	55
Tablo 11: Ekonomik Değerin Platformlarda Yoğunlaşması	55
Tablo 12: Veri Kapitalizmine Dair Gelişmeler	56
Tablo 13: Dijital Platformların Yerli ve Açık Kaynak Alternatifleri	58
Tablo 14: Dijital Hak Savunuculuğu	59

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

YÖNETİCİ ÖZETİ

Veri kapitalizmi, insanların internette ürettiği bilgilerin (verilerin) düzenli olarak toplanması, incelenmesi ve bu veriler sayesinde ekonomik veya siyasi kazanç elde edilmesi demektir. Bu süreçte veriler çoğunlukla gözlemlenerek toplanır; algoritmalarla işlenerek geleceğe yönelik tahminler yapılır ve bu tahminler, kişiye özel reklamlar, içerikler, fiyatlandırmalar veya hatta siyasi yönlendirmeler için kullanılır.

Dijital platformlar ise birden fazla grubu internet ortamında birleştiren ve bu etkileşimlerden ekonomik değer oluşturan aracı sistemlerdir. Bu platformlar, iş yapış şekillerinden tüketici alışkanlıklarına, piyasa hareketlerinden toplumsal ve siyasi eğilimlere kadar çok geniş bir alanda hem ekonomik hem de sosyal etkiler oluşturur. Büyük dijital platformlar artık sadece ekonomik değil, aynı zamanda siyasi güç de kazanmıştır. Ekonomik olarak, pazarın kontrolünü ele geçirmeleri, veriye dayalı zenginlik birikimiyle mali olarak güçlenmeleri ve bu durumun tekelleşmeyi artırması dikkat çeken noktalardır. Siyaset tarafında ise bu platformlar, lobi çalışmaları ve insanların fikirlerini yönlendirmeleriyle etkili olmakta; sahip oldukları dijital sistemler sayesinde bazı devlet hizmetlerinin yerine geçmeye başlamaktadır. Sosyal medya algoritmaları, toplumun konuşacağı konuların belirlenmesinde önemli bir rol oynamaktadır.

Dijital sömürü, insanların internetteki çabasının (emeğinin) ve dikkatlerinin paraya çevrilmesiyle ortaya çıkar. İnsanlar; sosyal medya, arama motorları ve çeşitli uygulamalar sayesinde hem bedava içerik üreten hem de isteyerek veri sağlayan kişi konumuna gelmiştir. Bu sömürü şekli, sadece dikkatin ticari bir mal haline getirilmesiyle sınırlı kalmaz; aynı zamanda kültürel içeriklerin parayla satılan eşyalara dönüştürülmesi, algoritmalarla insanların yönlendirilmesi ve veri sahipliğinin tek bir elde toplanması gibi şekillerde de görülmektedir. Veri kapitalizminin yapısı gereği, dijital platformlarda kişisel gizliliği (mahremiyeti) korumak en zor işlerden biridir. Çünkü bu sistem, toplayabileceği en çok kişisel veriyi toplayıp bunu paraya dönüştürmeyi hedefler. Kişisel gizliliğin korunması; yasal düzenlemeler, teknolojik araçların doğru kullanılması ve toplumun bu konudaki bilincinin yükseltilmesiyle mümkün olabilir. Dijital platformları kullananların sahip olduğu haklar; gizlilik hakkı, kişisel verileri koruma hakkı, ifade özgürlüğü, ağ tarafsızlığı, unutulma hakkı ve veriyi başka yere taşıyabilme hakkı gibi farklı başlıklar altında toplanır. Bu hakları korumak sadece yasalarla değil, aynı zamanda teknolojik çözümlerle ve sivil toplumun aktif mücadelesiyle de sağlanabilir.

Algoritmaların karar verme yöntemleri, Meta, Google ve Amazon gibi büyük dijital platformlara, kullanıcıların sadece şimdiki davranışlarını değil, gelecekteki eğilimlerini de tahmin etme ve onları yönlendirme yeteneği vermektedir. Veri kapitalizminin ulaştığı bu

noktada, dijital platformlar kullanıcıları sadece tanımakla yetinmeyip onları ikna etmek ve istedikleri yöne çekmek için planlar (stratejiler) geliştirmektedir. Bu durum, yapay zekâ (AI) ile desteklenen algoritmaları yeni bir güç aracı haline getirmektedir.

Siber bağımlılık, dijital çağın insanlar ve toplumlar üzerindeki en yaygın ancak aynı zamanda en zor fark edilen sorunlarından birisidir. Teknolojik gelişmeler hayatımızı kolaylaştırır da dijital araçların kontrolsüz ve sürekli kullanımı, insanların fiziksel, zihinsel ve sosyal sağlığını kötü etkilemektedir. Özellikle sürekli dopamin arayışı, gerçek hayattan kaçma isteği, sosyal medyada onaylanma ihtiyacı, özgüven eksikliği, yalnızlık duygusu ve diğer duygusal nedenler, insanlarda siber bağımlılığın oluşmasına yol açmaktadır.

Türkiye, küresel veri kapitalizmi sistemine çok fazla veri üreterek destek olsa da bu verileri ekonomik, teknolojik ve kültürel değere çevirme konusunda sınırlı bir yeteneğe sahiptir. Instagram ve TikTok gibi sosyal medya platformlarının algoritmaları, insanların dikkatini sömürmektedir. E-ticaret ve finans sektörlerinde çalışan dijital platformlar ise kullanıcıların davranışlarını, fiyatları sürekli değiştiren (dinamik) fiyatlandırma sistemlerinde kullanmaktadır.

Google ve Meta gibi büyük küresel dijital oyuncular, Türkiye'deki dijital reklam piyasasının neredeyse %70'ini kontrol etmektedir. Buna ek olarak, Kişisel Verilerin Korunması Kanunu'nun (KVKK) yetersiz kalması, herkese açık (açık kaynaklı) dijital sistemlerin eksikliği ve dijital okuryazarlık seviyesinin düşük olması, Türkiye'deki dijital sömürünün etkilerini daha da artırmaktadır. Veri kapitalizmine ve dijital sömürüye karşı Türkiye'nin atması gereken farklı adımlar mevcuttur. Hukuk alanında, Kişisel Verilerin Korunması Kanunu'nun (KVKK) Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile aynı seviyeye getirilmesi, dijital platformların tekelleşmesine karşı güçlü rekabet denetiminin yapılması ve Veri Koruma Kurumu'nun bağımsız, açık ve yeterli yetkiye sahip bir hale getirilmesi şarttır. Teknolojik altyapı konusunda ise, Pardus, TRCloud ve Jitsi gibi açık kaynak kodlu yerli dijital çözümler kamu kurumlarında daha çok kullanılmalı; yerli dijital girişimler ve veri kooperatifleri desteklenmelidir. Ek olarak, ülkeye ait yapay zekâ modelleri ve yerli veri kaynaklarının geliştirilmesi, stratejik olarak öncelikli bir konu olmalıdır.

Dijital sömürü ile mücadele sadece yasal ve teknolojik çözümlerle sınırlı kalmamalı, toplum genelinde de güçlü bir bilinç oluşturulmalıdır. Bu amaçla, dijital okuryazarlık eğitimi tüm okullarda ders programına eklenmeli; sivil toplum kuruluşları, belediyeler ve üniversiteler veri farkındalığını artırıcı halka yönelik kampanyalar yapmalıdır. Ayrıca, kültürel içerik üretenler yerli dijital platformlar üzerinden desteklenmeli; kendi hikayelerini anlatma hakkı ve kültürel olarak eşit temsil için yasal koruma yöntemleri geliştirilmelidir. Türkiye, dünya genelindeki veri adaleti ve dijital yönetim tartışmalarına

katkıda bulunmak için Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (UNCTAD), Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) ve G20 gibi uluslararası platformlardaki çalışmalara aktif olarak katılmalıdır. Bu süreçte, bölgesel dijital iş birlikleri çerçevesinde Türk Devletleri Teşkilatı ve İslam İşbirliği Teşkilatı gibi yapılar üzerinden ortak dijital egemenlik politikaları oluşturulmalıdır.

Dijital egemenlik sadece teknoloji üretmekle sınırlı değildir; aynı zamanda verinin kime ait olduğu, nasıl kullanıldığı ve kültürel hikayeler üzerindeki toplumsal ve siyasi kontrolün sağlanmasını da kapsar. Bu nedenle, Türkiye'nin dijital egemenliği için atacağı adımlar çok yönlü olmalıdır. Yasal olarak, KVKK'nın AB'nin Veri Koruma Tüzüğü ile uyumlu hale getirilmesi, dijital piyasalarda rekabeti koruyacak yeni bir dijital rekabet yasasının çıkarılması ve devletin dijital hizmetlerinde açık veri ve açık kaynak yazılımlarının kullanılması güvence altına alınmalıdır. Bu çerçevede, ülke çapında bir "Dijital Egemenlik Ulusal Politikası" oluşturulması çok önemlidir.

Teknofeodalizm kavramı, dijital çağda büyük teknoloji şirketlerinin ekonomik, politik ve sosyal yaşam üzerindeki gücünü, Orta Çağ feodal düzenindeki derebeylerine benzetmektedir. İlgili yaklaşım dahilinde, kapitalizm yeni bir evreye girmiştir; klasik piyasa mantığı yerine, platforma bağımlılık, veri mülkiyeti ve algoritmik tahakküm ilişkileri belirleyici olmaktadır. Bu çerçevede, platform devleri kritik dijital altyapının ve veri mülkiyetinin sahibi olarak "dijital derebeyleri" rolünü üstlenirken, kullanıcılar ve işletmeler dijital altyapılara erişim zorunluluğu nedeniyle "dijital serfler" konumuna indirgenmektedir. Dönüşümün temel dinamikleri arasında aşırı odaklı platformlaşma, kapalı veri tekelleri ve algoritmaların görünmez ancak güçlü yönetim mekanizması işlevi görmesi yer almaktadır. Söz konusu sistemde şirketler, üretime doğrudan katılmadan komisyon, reklam payı ve veri rantı gibi yöntemlerle gelir elde etmekte; neticede ekonomik değer üretiminin merkezileşmesine ve toplumun algoritmik manipülasyona açık hale gelmesine yol açmaktadır.

Teknofeodalizmin Türkiye bağlamındaki etkileri; pazarın platform merkezli örgütlenmesi, KOBİ'ler ile çalışanların algoritmik ekosistemlere bağımlılığı ve veri mülkiyetinin aşırı merkezileşmesi eksenlerinde yoğunlaşmaktadır. Ülkedeki küçük işletmeler (KOBİ'ler), satış hacmi ve görünürlük elde etmek için e-ticaret platformlarına zorunlu olarak girmekte; komisyon oranları ve algoritmik sıralama kriterleri gibi tek taraflı belirlenen kurallara uymak zorunda kalmaktadır. Öte yandan, yemek ve kurye ekonomisinde çalışanların gelir, rota ve performans ölçümü tamamen kapalı algoritmalar tarafından yönetilmektedir; bahsi geçen durum, feodal sistemdeki "toprağa bağlılık" ilişkisinin "uygulama ekosistemine bağlanma" şeklinde tezahür etmesini sağlamaktadır. Ayrıca, yerli girişimler

ve büyük şirketler, dijital altyapının mülkiyetinin küresel platformlarda toplanması nedeniyle küresel bulut hizmetlerine (dijital toprak) hem teknik hem de mali açıdan zorlayıcı bir bağımlılık (vendor lock-in) yaşamaktadır. Fintek ve bankacılık sektöründe ise, merkezi veri havuzlarında biriken finansal davranış verileri, algoritmik değerlendirme yoluyla ekonomik katılım üzerinde yönetsel güç edinilmesine neden olmakta, böylece yeni aktörlerin rekabeti kısıtlanmaktadır. Nihayetinde, üretim ve dağıtım karar merkezinin ekonomik aktörlerin elinden çıkıp dijital altyapı sahiplerine kaydığı görülmektedir.

Toplumsal düzeyde veri hakları, algoritmaların yaptıklarından sorumlu tutulması (hesap verebilirlik) ve kişisel gizlilik gibi konular, dijital okuryazarlık eğitimleriyle geniş kitlelere öğretilmelidir. Veri sahipliğini ortak bir yapıya taşıyan veri kooperatifleri desteklenmeli; yerli ve farklı dijital platformlar devlet teşvikleriyle güçlendirilmelidir. Ayrıca, kültürel zenginliği ve kendi hikayesini anlatma hakkını koruyan bir ulusal dijital medya sisteminin kurulması, kültürel bağımsızlık açısından hayati öneme sahiptir. Bu amaçlara ulaşmak için dijital egemenlik politikaları kısa, orta ve uzun vadeli bir plan dâhilinde düzenlenmeli, bu politikaların uygulanması ise sürekli takip edilmeli ve değerlendirilmelidir.

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

GİRİŞ

Amerikalı sanayici ve iş insanı Henry Ford'un, Ford Motor Company'nin kurucusu ve seri üretimin montaj hattı tekniğinin baş geliştiricisi olarak, Model T'lerin (1919–1925) rengiyle ilgili söylediği “Müşteri, istediği herhangi bir rengi seçebilir; yeter ki siyah olsun.” sözü üzerinden yaklaşık 100 yıl geçti.

Ticaret, üretim kapasitesi ve sürecine odaklanan bir dönemden, müşterinin merkeze alındığı bir anlayışa evrildi. Çünkü artık birçok ürün yeterince, hatta fazlasıyla üretilebiliyor ve pek çok alanda seri üretime geçilebiliyordu. Bu durum, müşterilere daha fazla seçenek sunulmasına yol açtı. Müşteri açısından temel soru da “Bu ürünü alabilecek miyim?” sorusundan, “Hangi ürün benim isteklerimi daha iyi karşılar?” sorusuna dönüştü.

Teknolojinin ilerlemesi, piyasaya daha fazla rakibin girmesini sağladı. Müşteri ihtiyaçlarını daha iyi analiz edebilen Toyota gibi Japon üreticiler, 1960'larda Ford gibi Amerikan otomobil üreticilerini kendi pazarlarında bile geride bırakmaya başladı. Bu gelişme, öncelikle üretim hattındaki aksaklıkların giderilmesini ve daha yüksek üretim kapasitesine ulaşılmasını sağladı. Ancak ekonomik refahın arttığı bir dönemde firmalar açısından asıl soru, giderek “Müşteri ne istiyor?” haline geldi. Firmalar, müşterilerini daha yakından tanımaya yönelik veri toplamaya başladılar. Başlangıçta bu veri toplama süreci, satış elemanlarının kişisel deneyimlerine ve anket gibi basit yöntemlere dayanıyordu. Zamanla bu süreç daha sistematik bir yapıya kavuştu. Çünkü müşterilerin zaman içinde değişen eğilimlerini tanımadan, bir firmanın pazarda varlığını sürdürebilmesi mümkün değildi.

Örneğin, 1970'lerde yaşanan petrol krizi, otomobil tercihlerini kökten değiştirdi. Tüketiciler, daha az yakıt tüketen modelleri tercih etmeye başladı. Bu özellikleri öne çıkaran modeller ise reklamlarında bu farkı vurgulayarak daha yüksek satış rakamlarına ulaştı.

Önceleri, genel müşteri isteklerini daha iyi anlayabilmek için saha araştırmaları ve yüz yüze yöntemler uygulanıyordu. Oysa günümüzde müşteri profilleri, bireysel düzeylere kadar indirgenebiliyor ve firmalar müşterilerini artık onların kendilerinden bile daha iyi tanıyabiliyorlar. Yapay zekâ ve algoritmalar sayesinde firmalar artık müşterilerin farkında bile olmadıkları ya da bilinçaltılarında yatan isteklerine ulaşabilir hâle geldiler.

Verinin bu denli merkezi bir konuma yerleşmesi, günümüzde yalnızca pazarlama stratejilerini değil, aynı zamanda küresel ekonomik dengeleri ve güç ilişkilerini de şekillendirmektedir. Artık veriye sahip olan şirketler ve devletler, yalnızca bireylerin tüketim alışkanlıklarını değil, aynı zamanda düşünce kalıplarını, yönelimlerini ve davranış biçimlerini de etkileyebilecek güce sahiptir. Bu durum, veri kapitalizmi adı verilen yeni bir ekonomik düzenin kapılarını aralarken; birey mahremiyetinin ötesinde, irade ve tercih

özgürlüğüne doğrudan müdahale edebilen bir sistemin de habercisidir. İşte bu rapor, dijital dönüşüm çağında verinin nasıl bir sermaye biçimine dönüştüğünü, şirketlerin ve devletlerin bu gücü nasıl kullandığını ve yeni yapının modern emperyalizmin günümüzdeki tezahürü olup olmadığını tartışacaktır.

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

1. VERİ KAPİTALİZMİNİN KURAMSAL TEMELLERİ VE VERİ MÜLKİYETİ

1.1. Veri Kapitalizmi

Veri kapitalizmi, ekonomik ve toplumsal değer üretim merkezine verinin yerleştirildiği, dijital çağın üretim biçimini tanımlar. Geleneksel kapitalizmde emek, hammadde ve fiziksel sermaye ön plandayken, veri kapitalizminde kişisel veriler, davranışsal bilgiler ve algoritmik çıkarımlar temel kaynaklar haline gelmiştir. Veri kapitalizmi, bireylerin dijital izlerinden elde edilen davranışsal verilerin toplanması, işlenmesi ve bu veriler aracılığıyla tahmin, yönlendirme ve kâr üretiminin sağlanması esasına dayanır. Kullanıcı verileri; reklam, algoritma geliştirme ve ürün tasarımı gibi amaçlarla kullanılmaktadır. Bu veriler artık bireye değil, onları toplayan dijital platformların mülkiyetinde sayılmaktadır. Ayrıca, değer kaynağının emekten veriye kaydığı yeni bir ekonomik düzeni tanımlamaktadır.

Veri Kapitalizminin Temel Özellikleri

- **Veri kapitalizminde, veri yeni sermayedir.** Dijital platformlar başta olmak üzere şirketler, kullanıcıların her tıklamasını, aramasını, konum bilgisini hatta duygusal tepkilerini veri olarak toplamakta ve bu veriler üzerinden gelir üretmektedir.
- **Veri kapitalizminde gözetim temelli işleyiş (gözetim kapitalizmi) söz konusudur.** Shoshana Zuboff'un tanımıyla bu sistem, gözetimi ekonomik bir mantık hâline getirmiştir. Kullanıcılar çoğu zaman verilerinin toplandığından habersizdir ya da bu süreç üzerinde herhangi bir denetim gücüne sahip değildir.
- **Veri kapitalizminde platform ekonomisi vardır.** Google, Facebook (Meta), Amazon gibi küresel dijital platformlar, kullanıcı verilerini analiz ederek hedefli reklamlar, kişiselleştirilmiş ürün önerileri ve pazar tahminleriyle ciddi gelirler elde etmektedir.
- **Veri kapitalizminde, algoritmik güç ve tahakküm vardır.** Dijital platformlar tarafından toplanan veriler, algoritmalar tarafından işlenerek bireylerin ne göreceği ne satın alacağı hatta nasıl düşüneceği yönünde müdahalelere neden olabilmektedir.
- **Veri kapitalizminde, emek başka bir formata dönüşmüştür.** Veri kapitalizmi bağlamında emek, geleneksel biçiminden farklılaşmıştır. Kullanıcılar, herhangi bir içerik üretmeseler bile yalnızca dijital platformları kullanarak (örneğin Google'da bir arama yapmak ya da YouTube'da video izlemek) veri sağlayarak "gizli emek" üretmiş sayılmaktadır.

1.2. Veri Üretiminde Mülkiyet

Veri üretiminde mülkiyet kavramı, günümüzde sıkça tartışılan ancak hâlâ belirsizliğini koruyan konulardan biridir. Geleneksel anlamda mülkiyet; fiziksel bir nesneye sahip olmayı ve bu nesne üzerinde kullanma, satma, kiralama ya da yok etme gibi hakları içerir. Ancak veri, fiziksel olmayan; çoğaltılabilir, kopyalanabilir, dağıtılabilir ve anonimleştirilebilir bir yapıya sahiptir. Bu durum, “Veri kime aittir?” sorusunu oldukça karmaşık bir hâle getirir.

1.2.1. Veri Mülkiyetinin Belirsizliği

Veriye ilişkin mülkiyet meselesi üç temel boyutta ele alınabilir:

Verinin Kime Ait Olduğu: Kullanıcıların tıkladığı, yazdığı, görüntülediği ya da gezindiği her dijital temas, kişisel veri üretir. Bu veriler doğrudan kullanıcıya ait gibi görünse de genellikle dijital platformların sunucularında toplanır, depolanır ve işlenir. Bu da mülkiyetin kullanıcıdan çok platformlara geçtiği bir yapıyı ortaya çıkarır.

Veriyi Üretenin Kim Olduğu: Kullanıcı, herhangi bir içerik üretmese bile dijital ortamdaki her etkileşimiyle veri üretir. Ancak bu verinin ekonomik olarak değerli hâle gelmesi, ancak bir şirketin sunucusunda işlenmesiyle mümkündür. Dolayısıyla veri, kullanıcı tarafından üretilse bile, ekonomik değer platformların işleme kapasitesiyle ortaya çıkar.

Veriyi Sahiplenenin Kim Olduğu: Hukuki düzenlemelere bakıldığında, birçok ülkede veri, mülkiyet temelli değil; daha çok koruma temelli bir anlayışla düzenlenmektedir. Bu bağlamda yasal metinlerde “Kullanıcı verileri kullanıcıya aittir” ifadesinden çok, “Kullanıcı verileri korunmalıdır” vurgusu ön plandadır. Bu durum, verinin fiilî mülkiyetini belirsizleştirmekte ve platformların veri üzerindeki hâkimiyetini meşrulaştıran gri alanlara neden olmaktadır.

Tablo 1: Veri Üzerindeki Hak Talepleri

Aktör	Talep Ettiği Haklar	Gerekçe
Kullanıcı	Sahiplik, kontrol, silme hakkı	Verinin kaynağı olması
Şirket	Erişim, kullanım, analiz, satma	Altyapıyı ve hizmeti sağlaması
Devlet	Düzenleme, denetleme, erişim hakkı	Kamu yararı, güvenlik, vergi gibi nedenler

1.2.2. Veri Mülkiyetinde Yeni Yaklaşımlar ve Öneriler Nelerdir?

Veri Kooperatifleri / Veri Ortaklıkları

Veri kooperatifleri, kullanıcıların verilerini bir araya getirerek kolektif biçimde yönettiği alternatif yapılardır. Veri kapitalizminin, bireysel verileri merkezî şirketlerde toplaması ve bu veriler üzerinden tek taraflı kazanç sağlaması karşısında; veri kooperatifleri daha adil, şeffaf ve kullanıcı odaklı bir sistem önermektedir. Bu yapılar, kullanıcıların verileri üzerindeki kontrolünü artırmayı ve veri üreticilerini sürecin pasif öznesi olmaktan çıkararak kolektif fayda üretiminin parçası hâline getirmeyi amaçlar.

Veri Temelli Temel Haklar

Veriyle ilişkili temel haklar, bireylerin dijital dünyada kişisel verileri üzerindeki yasal ve etik güvencelerini ifade eder. Bu haklar; mahremiyetin korunması, şeffaflık, veriye erişim, veri üzerinde kontrol gibi temel ilkeleri kapsar. Avrupa Birliği'nin (AB) GDPR ve Türkiye'deki KVKK gibi düzenlemeler, bu hakların yasal çerçevesini oluşturmaktadır. Bu kapsamda bireylere tanınan başlıca haklar şunlardır:

- Mahremiyet hakkı
- Veri koruma hakkı
- Veri güvenliği hakkı
- Veriye erişim hakkı
- Unutulma hakkı
- Veri taşınabilirliği
- İşleme itiraz hakkı

Veri Emek-Ücret İlişkisi

Bazı düşünürler, bireylerin sundukları veriler karşılığında maddi bir karşılık almaları gerektiğini savunmaktadır. Bu yaklaşıma göre, veriye dayalı olarak ciddi ekonomik değer ve servet üretiliyorsa, bu değer bir kısmı veri sağlayan bireylere dönmelidir.

Veri Mülkiyeti Ne Durumda?

Günümüzde veri mülkiyeti, büyük ölçüde dijital platformların ve şirketlerin fiilî egemenliği altındadır. Kullanıcılar ise yalnızca sınırlı ölçüde onay verme veya itiraz etme hakkına sahiptir. Güncel tartışmalarda, hukuki anlamda mülkiyetten çok, “veri üzerinde kontrol hakkı” kavramı öne çıkmaktadır. Ancak gelecekte veri mülkiyetinin; bireysel, kolektif ve kamusal haklar ekseninde yeniden tanımlanması ve düzenlenmesi yönünde teorik ve politik eğilimler giderek güçlenmektedir.

2. DİJİTAL EKONOMİ VE PLATFORM KAPİTALİZMİ

2.1. Dijital Platform Ekonomisinin Yapısı

Dijital platformlar, çok taraflı pazarları dijital altyapı üzerinden bir araya getiren ve bu etkileşimlerden değer üreten aracı sistemlerdir. Srnicek, platformları veri toplayarak ekonomik değer elde eden yeni sermaye yapıları olarak tanımlamaktadır. Platformları beş ana kategoriye ayırır: bulut platformları (örneğin AWS), reklam platformları (Google), endüstriyel platformlar (General Electric), ürün platformları (Apple) ve yalın platformlar (Uber) (Srnicek, 2016).

OECD ise dijital platformları, internet vasıtasıyla iletişimi ve veri iletimini kolaylaştıran dijital servisler olarak tanımlar. Bu tanım, platformların temel bileşenlerini ve işleyişini anlamada önemli bir çerçeve sunmaktadır (OECD,2019).

Tablo 2: Dijital Platform Ekonomisinin Yapısı

Bileşen	Açıklama
Platform Temelli Altyapı	Platformlar, klasik üretim araçları yerine dijital altyapı sağlayıcısı rolünü üstlenir. Mal veya hizmet üretmezler, üretim ve tüketim arasındaki aracı yapıyı kontrol ederler.
Çok Taraflı Pazar	Platformlar üretici (arz), tüketici (talep) ve bazen reklamcılar gibi birden fazla tarafı bir araya getirir. Değer, bu taraflar arasındaki etkileşimden doğar. (Örnek: Uber, Airbnb)
Ağ Etkisi	Kullanıcı sayısı arttıkça platformun değeri katlanarak artar. Ağ etkisi, platformların pazar liderliğini sağlamlaştırır ve rakip girişleri engeller.
Veri Akışı ve Kontrolü	Kullanıcıların her tıklaması, araması, beğenisi veri olarak toplanır. Bu veriler analiz edilerek kâr amaçlı kullanılır: reklam hedefleme, içerik yönlendirme, fiyatlandırma vb.
Algoritmalar	Platformlar kullanıcı davranışını yönlendirmek için algoritmalar kullanır. Bu şekilde, ne izleyeceğimize YouTube karar verir. Ne satın alacağımızı Amazon önerir. Böylece platformlar sadece aracı değil, karar verici hâle gelir.
Kapalı Ekosistemler	Büyük platformlar (Apple, Google, Amazon) sadece tek bir hizmet değil, tam bir dijital ekosistem sunar. Kendi ödeme sistemlerini, reklam ağlarını, bulut hizmetlerini kurarak her kullanıcı hareketini içselleştirir. Örneğin; Apple → iPhone + App Store + iCloud + Apple Pay Amazon → Marketplace + AWS + Prime + Reklam.
Emek Yapısı	Platform kapitalizmi, çalışanları doğrudan istihdam etmez, “bağımsız iş ortakları” modeli uygular. Bu model, iş güvencesi ve sosyal hakları büyük ölçüde zayıflatır. Örneğin; Yemeksepeti kurye modeli, Uber sürücüler, Upwork/TaskRabbit emekçileri.
Pazar Tekelleri	Veriye sahip olan kazanır. Platformlar daha fazla kullanıcı, veri ve kaynak çekerek aşırı merkezileşmeye neden olur. Bu durum, küçük girişimlerin, yerli şirketlerin ve bireylerin sistem dışına itilmesine ve küresel ölçekte dijital tekelleşmenin güçlenmesine yol açar.

2.1.1. Temel Bileşenler

Platform iş modeli, iki veya daha fazla farklı kullanıcı grubunun etkileşimini kolaylaştırarak ekonomik değer üretmeye dayanır. Bu model, dijital teknolojilerden önce de çeşitli biçimlerde mevcuttu; örneğin, basılı gazetelerdeki ilan sayfaları, sınıflandırılmış reklamlarla arz ve talep taraflarını bir araya getiriyordu. Ancak dijitalleşmenin etkisiyle birlikte, bu model daha sofistike ve yaygın bir form kazanmıştır. Günümüzde dijital platformlar, çok taraflı pazar yapısı sayesinde milyarlarca dolarlık değerlemelere ulaşabilmekte, ancak aynı zamanda birçok girişim rekabet baskısı ve sürdürülebilirlik sorunları nedeniyle başarısız olabilmektedir (Evans, 2016).

Platform temelli işletmelerin geleneksel iş modellerinden temel farkı, doğrudan mal veya hizmet satışı yerine kullanıcı gruplarını birbirine bağlamaya odaklanmalarıdır. Geleneksel bir taksi şirketi, doğrudan ulaşım hizmeti sunarken; Uber gibi platform işletmeleri, sürücüler ve yolcular arasında bir aracı olarak konumlanır (Morozov, 2015).

Platform ekonomisinin bir diğer dikkat çekici yönü, ağ etkilerine duyduğu yüksek bağımlılıktır. Platformlar, kullanıcı sayısı arttıkça daha fazla değer üretir. Bu doğrultuda, genellikle bir kullanıcı grubuna ücretsiz veya düşük maliyetli hizmetler sunularak daha büyük bir kullanıcı tabanı oluşturulması hedeflenir. Bu strateji, reklam verenler gibi gelir getiren tarafların ilgisini çekmekte ve platformun sürdürülebilirliğini desteklemektedir (Evans, 2016).

2.1.2. Dijital Platform Ekonomisinin Etkileri

2.1.2.1. İstihdam Üzerindeki Etkiler

Platform temelli ekonomi, istihdam yapısında iki ana iş türünü öne çıkarmıştır: birincisi, temizlik, kurye hizmeti veya ulaşım gibi fiziksel ortamda gerçekleştirilen “talep üzerine işler”; ikincisi ise veri girişi, içerik üretimi gibi çevrim içi olarak yürütülen dijital görevlerdir. Platform ekonomisinin savunucuları, bu iş biçimlerinin düşük giriş engelleri, esnek çalışma imkânı ve geniş kitleler için erişilebilirlik sunduğunu vurgulamaktadır.

Platform çalışanları sıklıkla bağımsız yüklenici ya da kendi hesabına çalışan statüsünde sınıflandırılmakta; bu durum, onları asgari ücret, hastalık izni ve sosyal güvenlik gibi geleneksel iş güvencesi standartlarından mahrum bırakmaktadır. Esneklik bazı çalışanlar için avantaj sağlasa da genel eğilim düşük kazanç, düzensiz gelir ve istikrarsız çalışma koşulları yönündedir. Birçok geçici iş ekonomisi çalışanı ortalamanın altında gelir elde etmekte ve bu durum, gelir eşitsizliğini daha da derinleştirmektedir (Kenney Martin, 2016).

2.1.2.2. Tüketici ve Toplumsal Riskler Üzerindeki Etkiler

Dijital platformlar, geleneksel sektörlerdeki işleyişi köklü biçimde dönüştürmektedir. Uber gibi ulaşım hizmetleri ya da Airbnb gibi konaklama platformları, taksicilik ve otelcilik gibi geleneksel hizmet sağlayıcıların yerini alırken, daha önce kayıt dışı olan ekonomik faaliyetlerin resmiyet kazanmasına da aracılık etmektedir. Ancak bu dönüşüm, aynı zamanda değer üretiminin ve kârın platform sahiplerinin elinde yoğunlaşmasına yol açmaktadır (Gray, 2019).

Egemen konumdaki platformlar, kullanıcılar ve hizmet sağlayıcılar arasında çeşitli bağlayıcılık anlaşmaları yoluyla pazarı denetim altında tutmaktadır. Bu tür uygulamalar platformların kârlılığını artırmakla birlikte, tüketici tercihini sınırlamakta, piyasa rekabetini zayıflatmakta ve yapısal verimsizlikler doğurmaktadır. Eleştirmenler, bu durumun hem tüketiciler hem de küçük ölçekli üreticiler açısından sömürüye açık bir zemin hazırladığını ileri sürmektedir (Star & Strauss, 1999).

Platform ekonomisinin savunucuları ise, kullanılmayan kaynakların (boş oda, özel araç vb.) etkin kullanımını sağlayarak girişimciliği demokratikleştirdiklerini ve ekonomik katılımı artırdıklarını savunmaktadır. Ancak karşıt görüşe göre, platformlar oluşturulan değer dağılımında eşitsizliği artırmakta; servetin ve piyasa gücünün belli başlı şirketlerde yoğunlaşmasına neden olmaktadır. Özellikle e-ticaret ve yemek teslimatı gibi sektörlerde uygulanan katı bağlılık sözleşmeleri, rekabeti sınırlayarak toplumsal refahın azalmasına yol açabilmektedir (Gray, 2019).

2.1.2.3. Piyasalar Üzerindeki Etkiler

Platformlar, yerleşik hizmet sağlayıcıları devre dışı bırakarak ve pazar yapısını yeniden şekillendirerek geleneksel piyasa işleyişini bozmaktadır. Örneğin, yolculuk paylaşımı ve kısa süreli konaklama sağlayan dijital platformlar, geleneksel ulaşım ve konaklama sektörlerine doğrudan rakip haline gelmiş; böylece, yerel üreticilerin elde ettiği ekonomik değeri küresel platformlara yönlendirmiştir.

Bu süreçte egemen platformlar hem kullanıcılar hem de hizmet sağlayıcılar üzerinde kontrol kurmak adına bağlayıcı sözleşmeler ve platforma özel koşullar uygulamaktadır. Bu stratejiler, tüketici tercihlerini daraltmakta ve piyasa içi rekabeti baskılamaktadır. Sonuç olarak, kaynakların etkin dağılımı sektöre uğramakta; verimsizlikler yapısal bir nitelik kazanmaktadır. Her ne kadar platformlar daha verimli kaynak kullanımını ve bireysel girişimciliği desteklediklerini öne sürseler de, eleştirmenler sistemin ekonomik fırsatlara erişimi sınırladığını, piyasa gücünü belli başlı aktörlerde topladığını ve özellikle yemek teslimatı ve çevrim içi perakende gibi sektörlerde gelir eşitsizliğini derinleştirdiğini ifade etmektedir (Star & Strauss, 1999).

2.1.2.4. Sosyopolitik Etkiler

Sosyal platformların geleneksel iş modellerinden en büyük farkı, kullanıcılarının davranışlarını sürekli olarak takip edip analiz etmeleri ve bu analizler sonucunda kullanıcıları istedikleri şekilde yönlendirebilmeleridir. Bu durum, platformlar açısından önemli bir güvenlik açığı oluşturmakta; zira toplanan veriler sosyal mühendislik uygulamaları ya da seçim manipülasyonları gibi amaçlarla kullanılabilir. Örneğin Cambridge Analytica skandalında, şirketin 2014 yılından itibaren toplamaya başladığı yaklaşık 50 milyon Facebook kullanıcısının kişisel olarak tanımlanabilir bilgilerini, ABD seçimlerini etkilemek için kullanıldığı iddia edilmiştir. Platform kullanıcıları, kararlarını özgür iradeleriyle verdiklerini düşünseler de bilinçaltına yönelik pek çok yönlendirmeye farkında olmaksızın maruz kalmaktadırlar (Zuboff, 2019).

Dijital platformların bir diğer önemli olumsuz etkisi, düşük kaliteli içeriklerin sıradanlaştırılması ve yaygınlaştırılmasıdır. Örneğin TikTok gibi platformlar bazı ülkelerde yasaklama tedbirleriyle karşı karşıya kalmıştır. Kullanıcıların hangi içeriği göreceğini ve hangi bilgilerle karşılaşacağını belirleyen algoritmalar, bireysel özgürlüğü zayıflatabilmektedir. Bu platformlar, dopamin etkisinden yararlanarak özellikle küçük yaşlardaki kullanıcılarda bağımlılık yapmakta; büyüme sürecinde olan çocuk ve gençlerin beyin gelişimini olumsuz yönde etkilemektedir. Dikkat çekmek ve dikkati sürekli kılmak amacıyla kullanılan ses ve görüntü efektleriyle birlikte, toplumsal açıdan kabul edilemez davranışlar bilinçsiz kullanıcılar tarafından sergilenmekte; benzer içeriklere uzun süre maruz kalan bireyler ise zamanla bu davranışları normalleştirmeye başlamaktadır. Böylece dijital platformlar yalnızca birer teknoloji aracı değil; aynı zamanda kültürel sansür, norm belirleme ve güç üretme araçlarıdır (Gillespie, 2018).

2.2. Büyük Teknoloji Şirketlerinin Ekonomik ve Siyasal Gücü

Büyük teknoloji şirketlerinin (Big Tech: Google/Alphabet, Apple, Amazon, Meta/Facebook, Microsoft vb.) sahip olduğu ekonomik ve siyasal güç, 21. yüzyıl kapitalizminin en kritik dönüşüm alanlarından birini oluşturmaktadır. Bu şirketler yalnızca piyasa dinamikleri üzerinde değil; aynı zamanda kamu politikaları, seçim süreçleri, uluslararası ilişkiler ve kültürel normlar üzerinde de doğrudan etkili hale gelmiştir.

ABD Başkan Yardımcısı JD Vance'in CBS News'e verdiği röportajda, büyük teknoloji şirketlerinin çok fazla güce sahip olduğunu ve bu şirketlerin ya Amerika'nın anayasal haklarına saygı duyacağını ve sansürü bırakacağını ya da Başkan Trump liderliğinin onlara karşı hoşgörülü olmayacağını söylemiştir. Ağustos ayında da benzer bir açıklama yapan Vance, Google gibi şirketlerin Amerikan halkının bilgilerini sansürlediğini ve "ifade

özgürlüğü üzerinde tekel kurduğunu” öne sürerek, bu tekellerin parçalanması gerektiğini savunmuştur.

Google, yakın zamanda büyük bir antitröst davasını kaybetmiştir. Virginia’da bir federal yargıç, 17 Nisan 2025 tarihinde, Google’ın çevrimiçi reklamcılık pazarında yasa dışı şekilde tekel oluşturduğuna ve mevcut konumunu daha fazla gelir elde etmek ve rakiplerini bastırmak için kullandığına karar vermiştir. Davayı Adalet Bakanlığı öncülüğünde birden fazla eyalet birlikte yürütmüş ve nihayetinde Google’ın parçalanması çağrısında bulunulmuştur. Açık Piyasalar Enstitüsü’nün yöneticisi Barry Lynn, “Mahkeme, Google’ın tekel gücünü yayıncıları sisteme kilitlemek ve reklam borsalarındaki rekabeti engellemek için kullandığını doğrulamıştır. Bu, dijital pazarlarımızın ve bilgi ortamımızın Google’ın kontrolü altına girdiğini gösteren açık bir yasa ihlalidir,” ifadelerini kullanmıştır (Estes, 2025).

Teknoloji devlerinin önemli güç kazanımlarının ardındaki nedenler uzun süredir tartışılmaktadır. Dijital şirketlerin tekelleşme süreci aslında yeni değildir. 1998 yılında Microsoft, Internet Explorer’ı Windows işletim sistemiyle birlikte sunarak önemli bir antitröst davasını kaybetmiş ve parçalanmanın eşiğine gelmiştir. Her ne kadar bu davadan çıkan sonuçlar şirketin bölünmesini engellemiş olsa da alınan kararlar tarayıcı piyasasında rekabeti artırmış ve Google Chrome’un yükselmesine zemin hazırlamıştır.

2010’lu yıllarda büyümeye başlayan dijital platformlar, en büyük sıçramayı Covid-19 pandemisi döneminde yaşamıştır. Salgın sürecinde uygulanan kapanma politikaları, sosyal medya kullanıcı sayısını dünya genelinde 4,5 milyarın üzerine çıkarmış ve bu rakam, küresel nüfusun yaklaşık %57’sine tekabül etmiştir. İnternette alışveriş ve kredi kartı kullanımı, 2019’a kıyasla iki kat artmış; dijital platformlar ve mobil uygulama kullanımı da bu dönemde belirgin biçimde yükselmiştir. Fiziksel alışverişin neredeyse durma noktasına geldiği bu süreçte, e-ticaret platformları rekor büyümeler gerçekleştirmiş ve küresel e-ticaret sektörü 5 yılda kat edeceği gelişimi sadece 5 ayda gerçekleştirmiştir (Tanrıkulu, 2022).

Uluslararası yardım kuruluşu Oxfam’ın yayımladığı “Eşitsizlik Öldürür” başlıklı raporda, dünyanın en zengin 10 kişinin — Elon Musk, Jeff Bezos, Bernard Arnault, Bill Gates, Larry Ellison, Larry Page, Sergey Brin, Mark Zuckerberg, Steve Ballmer ve Warren Buffet — toplam servetinin salgın sürecinde iki kat artarak 1,5 trilyon doları aştığı belirtilmektedir (Nabil, 2022).

2.2.1. Dijital Platformların Ekonomik Güçleri

2.2.1.1. Pazar Hakimiyeti ve Tekelleşme

Big Tech şirketleri; arama motorları (Google), dijital reklamcılık (Meta ve Google), e-ticaret (Amazon), mobil işletim sistemleri (Apple ve Android) ve bulut hizmetleri gibi alanlarda **duopol** ya da **tekel** yapılar oluşturmaktadır. Örneğin Google, küresel arama motoru pazarının yaklaşık %90'ını kontrol etmektedir. Amazon, ABD E-ticaret pazarının %40'ından fazlasına hâkimdir. Apple ve Google ise dünya mobil işletim sistemi pazarının neredeyse tamamını paylaşmaktadır (European Commission – *Digital Markets Act*, 2022; Statista – *Platform Market Shares*, 2024).

Tablo 3: Pazar Hakimiyeti

Sektör	Hâkim Platform	Pazar Payı
Arama Motoru	Google	%90+
E-Ticaret	Amazon	%40+ (ABD)
Sosyal Medya	Meta (Facebook + Instagram)	%70+

2.2.1.2. Veriye Dayalı Servet Birikimi

Kullanıcı verileriyle reklam, ürün geliştirme ve algoritmik yönlendirme yapan bu firmalar, **veriye dayalı kapitalizmin** merkezi haline gelmiş durumdadır (Zuboff, 2019). Artık yalnızca “emek” değil, “veri” üzerinden de değer üretilmektedir. Dijital platformlar, kullanıcıların her tıklamasını, kaydırmasını, beğenisini ve aramasını veriye dönüştürür. Bu veri yalnızca bir bilgi değil; aynı zamanda ekonomik değeri olan bir hammadde niteliğindedir (Cohen, 2019).

Örneğin Google, kullanıcıların arama geçmişini analiz ederek ilgi alanlarını belirlemekte ve buna göre kişiselleştirilmiş reklam hedeflemesi yapmaktadır. Toplanan veri, yapay zekâ ve algoritmalarla işlenerek kullanıcı davranışlarını tahmin edebilen modellere dönüştürülür. Burada temel hedef, kullanıcı henüz ne istediğini bilmeden, isteyebileceklerini ona göstermektir (Zuboff, 2019).

İşlenen veriler, reklam verenlere, finans kuruluşlarına, sigorta şirketlerine satılır ya da kullanıcıya gösterilecek içerik bu verilere göre belirlenir. Bu süreçten elde edilen gelir, platform kapitalistinin doğrudan kârına dönüşmektedir. Örneğin Meta, yalnızca kullanıcı ilgilerine göre kişiselleştirilmiş reklam satışıyla 2023 yılında 117 milyar dolar reklam geliri elde etmiştir (Meta, 2023).

Büyük veri havuzlarına sahip bu şirketler, yeni girişimlerin piyasaya girmesini neredeyse imkânsız hale getirmektedir. Artık veri, klasik sermaye birikiminden daha güçlü bir rekabet avantajı sunmaktadır. Örneğin Amazon, kullanıcı davranış verilerini kullanarak hangi

ürünlerin satılacağını önceden tahmin edebilmekte ve bu ürünleri kendi markasıyla piyasaya sürmektedir (UNCTAD, 2021).

Sonuçta servet birikimi yalnızca ekonomik değil; aynı zamanda toplumsal ve siyasal kontrol imkânı da oluşturmaktadır. Dijital platformlar, neyin görülüp görülmeyeceğini, neyin değerli olup olmadığını belirleyerek bir tür kültürel hegemonya üretmektedir (Cohen, 2019; Zuboff, 2019). Örneğin YouTube'un öneri algoritması, bir ülkenin gündemini şekillendirebilmekte ve halkın tercihlerine yön verebilmektedir (UNCTAD, 2021).

2.2.1.3. Finansal Güç

En büyük dijital platformlar, günümüzde dünyanın en değerli şirketleri haline gelmiştir. Örneğin, Apple'ın 2025 yılı için piyasa değeri yaklaşık 3 trilyon dolar civarındadır. Microsoft, Amazon, Alphabet (Google) ve Meta da yüz milyarlarca dolarlık piyasa değerine ulaşmıştır (Statista, 2024; Bloomberg Tech Valuations, 2024).

Dijital platformlar, klasik işletmeler gibi ölçek ekonomisi avantajından yararlanırlar. İlk yazılım altyapısını kurmak maliyetli olsa da bir kez büyük ölçekli sistem kurulduğunda daha fazla kullanıcıya düşük maliyetle hizmet verilebilir. Böylece platformların kâr marjı ciddi şekilde artar. Örneğin, Netflix'in içerik maliyetleri büyük oranda sabittir; bu nedenle abone sayısı arttıkça kârı da katlanarak artar (Srnicek, 2016).

Platformlar ayrıca reklamcılık sektörünü kökten dönüştürmüştür. Kişiselleştirilmiş reklamlar, dijital çağın temel gelir kaynaklarından biri haline gelmiştir. Örneğin, Meta'nın 2023 yılı reklam geliri 117 milyar dolar, Google'ın ise 240 milyar doları aşmıştır (Meta, 2023; UNCTAD, 2021).

Dijital platformların etkilediği bir diğer alan da finansal hizmetlerdir. Büyük teknoloji şirketleri, dijital cüzdan hizmetleri (Apple Pay, Google Pay), kredi sağlama (Amazon Lending) ve yatırım uygulamaları (Robinhood, Cash App) gibi alanlara da girmiştir. Ayrıca dijital platformlar, start-up'lara yatırım yaparak kendi ekosistemlerini oluşturmaktadırlar. Bu şirketler, platformlarında büyüttükleri firmaları satın alarak dikey birleşmelere yönelmişlerdir. Örneğin, Amazon'un Twitch ve Whole Foods'u, Google'ın ise YouTube ve Fitbit'i satın alması bu stratejinin örnekleridir (Srnicek, 2016).

Küresel çapta faaliyet gösteren bu platformlar, düşük vergilendirmeye sahip ülkelerde kayıt tutarak ve şirket içi fon transferlerini kullanarak vergi yükümlülüklerini minimize etmektedir. Böylece yüksek kârlarını düşük vergilerle koruyarak sermaye birikimlerini artırmaktadırlar (OECD, 2021; UNCTAD, 2021).

2.2.2. Dijital Platformların Siyasal Güçleri

Dijital platformlar, toplumları sadece ekonomik olarak değil; iktidarlari, seçimleri ve hatta demokrasiyi doğrudan etkileyen bir konuma gelmiştir. Dijital platformların siyasal gücü, özellikle bilgi akışını kontrol etme, lobicilik, platform regülasyonu ve algoritmik müdahaleler aracılığıyla kendini gösterir. Bu platformlar, kullanıcılara hangi içeriğin gösterilip gösterilmeyeceğine yapay zekâ araçlarıyla karar verir. Seçim dönemlerinde algoritmalar, siyasi içerikleri öne çıkararak seçim süreçlerini etkileyebilir ve bu durum platformları fiilen medya organı ve sansür makamı haline getirebilir. Örneğin, Facebook'un haber algoritmasının ABD seçimlerinde kutuplaşmayı artırdığı gözlemlenmiştir. Ayrıca, YouTube öneri sistemlerinin de radikalleştirici etkileri bulunmaktadır (Zuboff, 2019; Gillespie, 2018).

Günümüzde sosyal medya platformları, özellikle Twitter, botlar, troll orduları ve sponsorlu içeriklerle siyasi kampanyaların aracı haline gelmiştir. Botlar, çeşitli etiketler (hashtag) kullanarak istedikleri konuları sosyal medyada gündeme taşıyabilmektedir. Devlet dışı aktörlerin bile bu platformlar üzerinden bir ülkenin iç siyasetini etkilediği tespit edilmiştir. Örneğin, 2016 ABD seçimlerinde Cambridge Analytica, yaklaşık 50 milyon Facebook kullanıcısının kişisel olarak tanımlanabilir verilerini toplayarak seçmen profili oluşturmuş ve buna yönelik propaganda yapmıştır. Benzer şekilde, 2016'daki Brexit oylaması kampanyalarında da bu tür uygulamalar görülmüştür. Facebook, Twitter (X) ve YouTube gibi platformlar üzerinden dezenformasyon, manipülasyon ve siyasi propaganda yaygınlaşmıştır. Algoritmik sıralamalar, kamuoyunun neyi görüp neyi görmeyeceğini belirlemektedir (Cadwalladr, 2018; Digital Forensic Research Lab, 2020).

Big Tech şirketlerinin oldukça büyük lobi gücü bulunmaktadır. Bu şirketler, yasa yapıcıları etkilemek, regülasyonları zayıflatmak ve kendi çıkarlarını korumak için milyarlarca doları aşan lobicilik faaliyetleri yürütmektedir. Örneğin, 2023'te yalnızca ABD'de Google, Amazon, Meta ve Apple yaklaşık 70 milyon dolar lobicilik harcaması yapmıştır. Big Tech şirketleri lobicilik faaliyetleriyle birlikte teknoloji politikaları, vergi mevzuatı, rekabet yasaları ve yapay zekâ regülasyonu gibi alanlarda karar vericiler üzerinde doğrudan etkiye sahiptirler (OpenSecrets.org, 2023; EFF, 2023).

Dijital platformlar, demokratik denetime açık olmayan kendi kurallarını da işletmektedir. Algoritmalar aracılığıyla "özel yasalar" koymakta, içerikleri istedikleri gibi silebilmekte, hesapları kapatmakta ve sansür uygulayabilmektedirler. İçerik standartları, sansür uygulamaları ve reklam politikaları gibi alanlarda devlet dışı yasa koyucu rolü üstlenmektedirler. Bu durum, özel şirketlerin kamu düzeni üzerinde güç kurmasına neden

olmaktadır. Örneğin, Twitter bazı devlet başkanlarının hesaplarını kapatabilirken, bazı ülkelerde ise muhaliflerin hesaplarını kaldırarak siyasi pozisyon almıştır (Kaye, 2019).

Büyük platformlar, devletlerle veri paylaşımı, sansür talepleri veya vergi yasaları konusunda pazarlık yapabilen ulus aşırı aktörler haline gelmiştir. Örneğin, Apple ile Çin hükümeti arasında kullanıcı verilerinin Çin sunucularına taşınması yönünde bir anlaşma yapılmış; Facebook'un Türkiye'de temsilcilik açması ise tartışma konusu olmuştur (Cohen, 2019; UNCTAD, 2021). Dijital altyapıların çoğu ve kamu hizmetlerinin (iletişim, güvenlik, bulut veri) önemli bir kısmı bu şirketler tarafından sağlanmaktadır. Örneğin, Amazon Web Services (AWS) birçok devletin dijital altyapısını desteklemektedir. Bu durum, dijital platformlara devletler üzerinde önemli bir etkileme gücü kazandırmaktadır (UNCTAD, 2021).

Tablo 4: Dijital Platformların Ekonomik ve Siyasal Gücü

Boyut	Etki Alanı	Örnek/Açıklama
Ekonomik	Piyasa tekelleşmesi, veri egemenliği	Amazon, Google reklam ve arama pazarını domine eder
Siyasal	Lobi, kamuoyu yönlendirme	Facebook–Cambridge Analytica olayı
Altyapısal	Devlet hizmetlerini gölgeleme	AWS üzerinden kamu hizmetlerinin ifası
Kültürel	Algoritmik gündem belirleyicilik	YouTube öneri algoritmaları

3. DİJİTAL DÜZENDE HAKLAR, MAHREMİYET VE RİSKLER

3.1. Bireysel Mahremiyet

Veri kapitalizmi döneminde bireysel mahremiyet korunması en zor alanlardan biri olmuştur. Çünkü dijital çağda veri kapitalizmi ve bireysel mahremiyet, doğası gereği birbirine doğrudan zıt iki güç alanını temsil etmektedir. Veri kapitalizmi, bireylerin davranışlarından mümkün olduğunca çok veri elde edip bunu ekonomik değere dönüştürmeyi amaçlarken; bireysel mahremiyet, bireyin bu veriler üzerindeki kontrol hakkının korunmasıdır. Bu iki kutup arasında sürekli mücadele vardır ve biri büyüdükçe diğeri zayıflar (Nissenbaum, 2010).

Bireysel mahremiyetin en temel esası, kişisel bilgilerin izinsiz toplanmaması, ifşa edilmemesi ve bu bilgilerin kontrolünün bireyde kalmasıdır. Dijital boyutta ise internetteki tıklamaların, konum bilgilerinin, aramaların ve beğenilerin kişisel veri haline dönüştürülmesi, ardından bu verilerin platformlar tarafından genellikle bireyin bilgisi dışında toplanıp kullanılması söz konusudur (GDPR, 2016).

Özetle, veri kapitalizmi bireyler hakkında mümkün olan her veriyi toplayıp bu verilerden yola çıkarak bireylerin davranışlarını öngörmeyi amaçlar ve bu süreçte şeffaf olmayan algoritmalar kullanır. Bireysel mahremiyet ise verinin sadece izinle kullanılmasını, bireyin tercih özgürlüğünü korumayı, hesap verebilirliği ve kullanılan yöntemlerle ilgili şeffaflığı gerektirir. Örneğin, Facebook'un kullanıcılarının etkileşim verilerini Cambridge Analytica ile paylaşarak siyasi manipülasyon yapılması, bireysel mahremiyetin ihlal edildiği veri kapitalizminin somut bir örneğidir (Zuboff, 2019).

Görüldüğü üzere, veri kapitalizmi bireylerin mahremiyetini temelden sarsan bir sistemdir, çünkü ortaya çıkarılan değerlerin kaynağı kullanıcı verisidir. Bu sistemde bireysel mahremiyetin sağlanması zor olsa da tamamen olanaksız değildir. Ancak bu koruma, bireysel çabalardan çok hukuki, teknolojik ve kolektif önlemlerle mümkündür (Nissenbaum, 2010; GDPR, 2016).

Dijital çağda bireysel mahremiyeti korumak için üç aşamalı bir yöntem benimsenebilir:

1. Kanuni Yoldan Verilerin Korunması:

Avrupa Birliği'nde yürürlükte olan GDPR ve Türkiye'deki KVKK gibi yasalar, bireylere kendi verileri üzerinde kontrol hakkı tanımaktadır. Bu yasalara göre açık rıza olmaksızın kişisel veri toplanamaz; bireyler, kendilerine ait verileri görme, düzeltme ve silme hakkına sahiptir. Ayrıca "unutulma hakkı" ve "veri taşınabilirliği" de bu düzenlemelerle güvence altına alınmıştır. Ancak bu hakların etkin biçimde uygulanabilmesi için yasaların sadece varlığı değil, aynı zamanda denetlenebilir ve yaptırım gücüne sahip olması da gereklidir. Uluslararası teknoloji şirketlerinin bu düzenlemelere uyum göstermesinin sağlanması da

kritik bir konudur (General Data Protection Regulation [GDPR], 2018; Kişisel Verileri Koruma Kanunu [KVKK], 2016).

2. Teknolojik Yönden Verilerin Korunması (Privacy by Design):

Şifreleme, anonimleştirme ve uçtan uca veri koruma gibi teknolojik önlemlerle platformların bireysel verilere erişimi engellenebilir. Bu bağlamda; WhatsApp'ın mesajları uçtan uca şifrelemesi, Firefox ve Brave tarayıcılarının izleyici engelleme özellikleri ve DuckDuckGo'nun veri toplamayan yapısı önemli örnekler arasında yer almaktadır. "Privacy by Design" (Mahremiyetin Tasarımla Korunması) ilkesi ise bireysel mahremiyetin yazılım sürecine sonradan eklenen bir unsur değil, yazılımın ilk tasarım aşamasından itibaren temel bir bileşen olarak dahil edilmesi gerektiğini savunmaktadır.

3. Bireyler Yönünden Verilerin Korunması:

Dijital platformlarda bireysel mahremiyetin korunmasında ilk adım, bireylerin bu ortamları bilinçli kullanması ve dijital okuryazarlık becerilerine sahip olmasıdır. Bu doğrultuda kullanıcıların, hangi uygulamanın hangi bilgilere eriştiğini bilmeleri, çerez ve izleme izinlerini yönetebilmeleri ve gereksiz erişim taleplerine "hayır" diyebilmeleri gerekmektedir. Ancak, bireysel farkındalık ve bilinçlenme tek başına yeterli değildir. Sistemsel ve yapısal korumalar sağlanmadan sadece kullanıcı inisiyatifiyle mahremiyetin korunması mümkün olamaz.

Günümüzde bireysel mahremiyetin korunmasına ilişkin yeni yaklaşımlar gelişmektedir. Bu yaklaşımlara göre veri yalnızca bireysel değil, aynı zamanda kolektif bir varlık olarak değerlendirilmelidir. Eğer veri sağlanması ekonomik bir değer oluşturuyorsa, bu değer karşılığı bireylere ödenmelidir. Ayrıca, veri kamusal bir varlık olarak kabul edilmeli, özel şirketlerin tekeline bırakılmamalıdır. Bu çerçevede; vatandaşlara yönelik veri sendikalarının kurulması, kamusal veri yönetim platformlarının oluşturulması ve mahremiyet odaklı platform kooperatiflerinin desteklenmesi gibi modeller önerilmektedir (Viljoen, 2020; Morozov, 2016.).

Özetle, veri kapitalizmi içinde gerçek anlamda bireysel mahremiyetin sağlanabilmesi için sistemin yeniden tasarlanması gerekmektedir. Bu dönüşüm ise yalnızca bireysel tercihlere değil, aynı zamanda politik kararlar, teknolojik altyapı seçimleri ve toplumsal taleplerin etkili bir şekilde örgütlenmesine bağlıdır.

Tablo 5: Mahremiyetin Korunması için 3 Temel Aşama

Konu	Açıklama
Yasa	Bireyin haklarını tanıyan, uygulanan veri koruma yasaları.
Teknoloji	Şifreleme, izleme engelleme, açık kaynak mahremiyet araçları.
Toplumsal Bilinç	Dijital okuryazarlık + kolektif veri hakları bilinci.

3.2. Gözetim Toplumu

Devletler çok eski zamanlardan bu yana, yönettikleri halk hakkında ekonomik ve siyasi nedenlerle bilgi sahibi olma arzusu taşımaktadır. Ancak bu çaba, geçmişte daha çok toplumun genel özelliklerini ve eğilimlerini anlamaya yönelik olmuştur. Günümüzde hem devletlerin hem de özel şirketlerin elinde, yaşadıkları topluma dair son derece geniş ve detaylı veri tabanları bulunmaktadır.

David Lyon'a göre gözetim toplumu, bireylerin günlük yaşamları sistematik biçimde izlenip kayıt altına alınması ve bu verilerin çeşitli çıkarlar doğrultusunda işlenmesiyle oluşan bir toplumsal yapıdır (Lyon, 2018). Veri kapitalizmi çağında ise bu gözetim yalnızca devletler eliyle değil, özel şirketler aracılığıyla da gerçekleştirilir.

Dijital gözetim toplumunda sürekli ve kesintisiz bir izleme hali söz konusudur. Mobil cihazlar, uygulamalar, çerezler ve kameralar gibi araçlarla kullanıcılar 7/24 izlenir. Bu kullanıcılar, çoğu zaman farkında bile olmadan, sistemlere veri sağlarlar. Yapay zekâ destekli sistemler; yüz tanıma, davranışsal izleme ve tahmin algoritmaları yoluyla bireylerin davranış kalıplarını modellemeye çalışır. Veri toplama süreci hem ticari (ör. hedefli reklamcılık) hem de politik (ör. kamuoyu yönlendirmesi) amaçlarla yürütülür (Zuboff, 2019).

Bu gözetim yapısı, toplumsal ilişkileri ve birey davranışlarını yeniden şekillendirir. Mahremiyetin aşınması, bireyin özel alanının yok olmasına yol açar ve kişiler sürekli gözetleniyormuş gibi davranmaya başlarlar. İzlenen birey, kendini sansürleyerek davranışlarını kontrol altına alır. Ayrıca, toplanan dijital veriler kredi skorlarını, sağlık verilerini ve tüketim alışkanlıklarını etkileyerek dijital ayrımcılığa neden olur. Yapay zekâ algoritmaları, toplumsal manipülasyonun aracı hâline gelir; gündem, topluluk davranışları ve hatta oy verme eğilimleri bile yönlendirilebilir (Zuboff, 2019; Cohen, 2019).

Dijital platformlar, gözetim uygulamalarının sadece devletler eliyle yapılması anlayışını dönüştürmüştür. Artık özel şirketler de bireysel ve toplumsal davranışları takip edebilmektedir. Ancak burada gözetimin amacı, kapsamı ve sınırları farklılık gösterir. Devlet gözetimi daha çok güvenlik ve istihbarat amaçlı olup yasal sınırlarla düzenlenirken; şirketler gözetimi, reklam ve tüketimi artırmaya yönelik olarak gerçekleştirir. Dahası, devlet gözetimi çoğunlukla ulusal ölçekliken, dijital platformlar küresel düzeyde gözetim yapabilmektedir.

Sonuç olarak, veri kapitalizmi çağında gözetim, bir istisna değil, olağan, görünmez ve hatta gönüllü hâle gelmiştir. Bireyler artık yalnızca izlenen değil, aynı zamanda sürekli veri

üreten merkezlerdir. Bu nedenle, bireysel mahremiyetin korunabilmesi için teknolojik, hukuki ve etik düzeyde yeni bir toplumsal sözleşmeye ihtiyaç duyulmaktadır.

3.3. Dijital Haklar

Dijital haklar, bireylerin dijital ortamda sahip olduğu temel hak ve özgürlükleri ifade eder. İnternet ve dijital teknolojilerin yaygınlaşmasıyla birlikte, bu haklar insan haklarının dijital çağdaki yansımaları olarak önem kazanmıştır. Dijital haklar, özellikle veri toplama, işleme ve paylaşma süreçlerinde bireylerin çevrimiçi özgürlük ve güvenliklerinin korunmasını kapsar.

– Mahremiyet Hakkı (Right to Privacy)

Dijital hakların en temel unsurlarından biri, bireyin kişisel bilgilerinin izinsiz toplanması ve ifşa edilmemesi hakkıdır. Dijital çağda en çok tartışılan ve ihlal edilen haklardan biri olan mahremiyet hakkı, veri kapitalizminin yaygınlaşmasıyla birlikte sadece özel hayatın korunması değil, aynı zamanda bireyin kimliği, özgürlüğü ve bütünlüğünün korunmasını da kapsamaktadır. Dijital ortamda mahremiyet hakkı, bireyin verilerinin ne zaman, nasıl ve kim tarafından toplandığını kontrol etme yetkisini ifade eder. Örneğin, Google veya Facebook'un kullanıcının konum bilgisi, mesajları veya arama geçmişi gibi verileri kullanıcının açık rızası olmadan toplaması, mahremiyet hakkının ihlali olarak değerlendirilir (Zuboff, 2019; GDPR, 2018).

– Veri Koruma Hakkı (Data Protection Right)

Veri Koruma Hakkı, bireylerin dijital platformlardaki kişisel verilerinin güvenli, adil, şeffaf ve bireyin kontrolünde olacak şekilde işlenmesini güvence altına alan temel bir haktır. Bu hak, mahremiyet hakkının teknik ve hukuki uzantısıdır; bireyin verisi üzerinde gerçek söz sahibi olmasını sağlar. Bu hak, kişisel verilerin şeffaf, güvenli ve hukuka uygun biçimde işlenmesini gerektirir. Avrupa Birliği'ndeki GDPR ve Türkiye'deki KVKK gibi yasalar bu hakkın korunmasını temel alır. Bireyler, verilerinin neden toplandığını öğrenme, yanlışsa düzeltme veya tamamen sildirme hakkına sahiptir (GDPR, 2018; KVKK, 2016).

Bu kapsama giren veriler şunlardır: kimlik verisi (ad, soyad, T.C. Kimlik No, e-posta), iletişim verisi (telefon, adres, IP bilgisi), davranışsal veri (arama geçmişi, alışveriş tercihleri, tıklamalar), biyometrik veriler (yüz, parmak izi, retina, ses), konum verisi (GPS verileri, IP üzerinden belirlenen lokasyonlar) ve finansal veriler (kredi kartı bilgileri, gelir düzeyi, harcama gibi bireyin finansal geçmişiyle ilgili veriler) (GDPR, 2018; KVKK, 2016).

Veri Koruma Hakkı hem uluslararası hem de ülkemizdeki yasalarla korunmaktadır. Uluslararası alanda, Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation [GDPR], 2018), OECD Gizlilik İlkeleri (OECD, 2013) ve Birleşmiş Milletler Dijital Haklar Belgeleri (United Nations, 2019); Türkiye’de ise 2016 yılında yürürlüğe giren Kişisel Verileri Koruma Kanunu (KVKK, 2016) dijital verilerin korunmasıyla ilgilidir.

Temel olarak düzenlenen veri koruma hakları şu şekildedir: kişinin verisi toplanırken ne amaçla ve ne kadar süreyle kullanıldığını bilme hakkı (Aydınlatma Hakkı), özgür ve bilgilendirilmiş şekilde onay verme hakkı (Açık Rıza Hakkı), hangi verilerin tutulduğunu görme hakkı (Veriye Erişim Hakkı), yanlış veya güncel olmayan verilerin düzeltilmesini veya silinmesini talep etme hakkı (Düzeltilme/Silme Hakkı), verilerin belirli şekillerde işlenmesine karşı çıkma hakkı (İtiraz Hakkı) ve verilerin başka bir hizmet sağlayıcıya taşınması hakkı (Taşınabilirlik Hakkı) (GDPR, 2018; KVKK, 2016).

Veri Koruma Hakkına karşı çeşitli tehditler mevcuttur. Örneğin, siber saldırılarla kişisel verilerin çalınması mümkündür. Ayrıca, sözleşmeler ya da üyelikler sırasında “Kabul Et” butonuyla yapılan üstü kapalı veri devri risk oluşturabilir. Sağlık, konum ve tüketim verilerinin farklı amaçlarla kullanılması veya üçüncü taraflara satılması gibi tehlikeler de bulunmaktadır.

Günümüzün yeni sermayesi olan verinin korunması oldukça önemlidir. Çünkü bu sermayenin kayıtsızca teslim edilmesi, bireyin mahremiyetini, özgürlüğünü ve ekonomik haklarını teslim etmesi demektir. Bireysel verilerin yeterince korunmaması durumunda, mahremiyet ihlalleri yaşanabilir, dijital eşitsizlik artar ve bireyler şirketlerin veya devletlerin nesneleri haline dönüşür.

Bireysel verilerin korunması tek taraflı bir konu değildir ve çeşitli araçlarla gerçekleştirilir. Yasal olarak GDPR ve KVKK gibi düzenlemeler, açık rıza, denetim ve ceza sistemleriyle koruma sağlar. Teknolojik olarak ise verilerin anonimleştirilmesi, şifrelenmesi ve şeffaf, açık kaynaklı veri yönetim sistemleri kullanılmalıdır. Toplum olarak da dijital hak hareketleriyle ve veri istismarına karşı kamusal bilinçle bu koruma güçlendirilmelidir.

– İfade Özgürlüğü (Freedom of Expression)

Dijital bir hak olarak ifade özgürlüğü, bireylerin dijital ortamlarda – özellikle internet ve sosyal medya platformlarında – düşüncelerini, görüşlerini, inançlarını ve duygularını ifade etme, bilgiye ulaşma ve paylaşma hakkını içerir. Bu hak, klasik anlamda ifade özgürlüğünün internet çağındaki uzantısıdır. Sosyal medya, blog, forum gibi dijital

mecralarda fikir açıklama, içerik üretme ve yayma, sansürsüz biçimde bilgiye ve kaynaklara ulaşma, kamusal dijital tartışmalara katılma bu hak kapsamındadır.

Dijital ortamda ifade özgürlüğü, demokratik katılımı teşvik etmesi, bilgiye erişim sağlaması ve eleştirel düşünceyi desteklemesi bakımından oldukça önemlidir. Bu hak; İnsan Hakları Evrensel Bildirgesi'nin 19. maddesi, Avrupa İnsan Hakları Sözleşmesi'nin 10. maddesi, Birleşmiş Milletler İnternet Özgürlüğü Bildirisi ve UNESCO Dijital Haklar İlkeleri gibi belgeler tarafından koruma altına alınmıştır (United Nations, 1948; Council of Europe, 1950; UNESCO, 2021). Avrupa İnsan Hakları Mahkemesi (AİHM) de sosyal medya paylaşımlarını ifade özgürlüğü kapsamında değerlendirmektedir.

– Ağ Tarafsızlığı (Net Neutrality)

Ağ tarafsızlığı, internet servis sağlayıcılarının (ISS – Türk Telekom, Vodafone, Superonline gibi) tüm internet trafiğine eşit ve ayırım gözetmeksizin davranmasını öngören temel bir ilkedir. Bu ilkeye göre ISS'ler, kullanıcıların erişmek istediği içerik, uygulama veya web sitelerine göre internet trafiğini yavaşlatamaz, engelleyemez ya da öncelik tanıyamaz.

Ancak veri kapitalizminin etkisiyle bu tarafsızlık ilkesi zaman zaman reklam öncelikleri veya içerik sansürüyle zedelenebilmektedir. Ağ tarafsızlığı üç temel prensibe dayanır: (1) Hiçbir meşru internet içeriği veya uygulama erişime kapatılmamalıdır, (2) içerik türüne göre bilinçli yavaşlatma yapılmamalıdır ve (3) ödeme yapan şirketlere öncelik tanınmamalı, tüm içeriklere eşit erişim sağlanmalıdır (EU Regulation 2015/2120).

Ağ tarafsızlığı, ifade özgürlüğünün ve dijital eşitliğin sağlanması açısından önemlidir. Fikirlerin eşit koşullarda dolaşıma girmesine imkân tanır ve küçük girişimlerin büyük teknoloji şirketleri karşısında rekabet edebilmesini destekler. Avrupa Birliği'nde bu hak EU Regulation 2015/2120 ile yasal güvence altına alınmıştır; ancak Türkiye'de henüz bu konuda özel bir yasal düzenleme bulunmamaktadır.

– Unutulma Hakkı (Right to Be Forgotten)

Unutulma hakkı, bireylerin geçmişte dijital ortamlarda yer almış kişisel, yanlış, güncelliğini yitirmiş ya da haksız şekilde zarar verici bilgilerin internetten kaldırılmasını talep etme hakkıdır. Bu hak, bireyin dijital izlerinin yaşamı boyunca kendisini takip etmesini önlemeyi amaçlayan bir mahremiyet hakkıdır.

Bu hak çeşitli dijital ortamlarda ileri sürülebilir. Örneğin, cezasını tamamlamış bir kişinin, Google gibi arama motorlarında hâlâ erişilebilen mahkûmiyet bilgilerini sildirmek istemesi

mümkündür. Aynı şekilde, artık kamu yararı taşımayan gazete arşivlerinde geçen isimlerin kaldırılması talep edilebilir. Bireyler ayrıca, sosyal medyada rızaları dışında paylaşılan fotoğraflar, yorumlar ya da haber içeriklerindeki kişisel verilerin kaldırılmasını isteyebilir. Dijital geçmişin bireyin gelecekteki yaşamını olumsuz yönde etkilemesini önlemek amacıyla, önceden yapılan hataların erişime kapatılması da hakkın kapsamına girer.

Avrupa Birliği Adalet Divanı, 2014 tarihli “Google Spain” davasıyla birlikte unutulma hakkını tanıdı; bu hak, Genel Veri Koruma Tüzüğü’nün (GDPR) 17. maddesinde “Veri sahibinin kişisel verisinin silinmesini talep etme hakkı vardır” şeklinde düzenlenmiştir. Türkiye’de ise 6698 sayılı KVKK’nın 7. ve 11. maddelerinde kişisel verilerin silinmesi ve unutulma hakkı açık şekilde yer almaktadır. Ayrıca, Anayasa Mahkemesi 2020 yılında verdiği kararla, arama motorlarından içerik kaldırılmasına ilişkin içtihat geliştirmiştir.

Unutulma hakkı; Google’ın “İçerik Kaldırma Talep Formu”, Facebook’un “İçerik Bildirimi ve Kaldırma Başvurusu” gibi yollarla kullanılabilir. Diğer dijital platformlarda ise KVKK kapsamında bireyler, kişisel veri silme/düzeltilme başvurusu ve şikâyet hakkı aracılığıyla taleplerini iletebilirler.

– Veri Taşınabilirliği Hakkı (Data Portability)

Verinin taşınabilirlik hakkı, dijital dünyada bireyin kendi verileri üzerindeki kontrolünü artırmayı amaçlayan temel dijital haklardan biridir. Özellikle platform bağımlılığını azaltmak, tekeli yapıları karşı kullanıcı özgürlüğünü güçlendirmek ve dijital pazarda rekabeti desteklemek açısından önem taşır. Bu hak bireylere, kişisel verilerini talep etme, yeniden kullanma ve bir platformdan başka bir platforma taşıma imkânı tanır.

Veri taşınabilirliği kapsamındaki bilgiler; ad, soyad, e-posta adresi, konum gibi birey tarafından sağlanan verilerin yanı sıra; alışveriş geçmişi, izlenen videolar, dinlenen müzik gibi davranışsal verileri de içerir.

Bu hak, GDPR’nin 20. maddesinde "Veri sahibi, kişisel verilerini yapılandırılmış, yaygın kullanılan ve makine tarafından okunabilir bir biçimde alma ve bu verileri başka bir veri sorumlusuna iletme hakkına sahiptir" şeklinde düzenlenmiştir. Türkiye’de ise KVKK’da veri taşınabilirliği açıkça tanımlanmış değildir; ancak, “kişisel veriye erişme ve düzeltme hakkı” bu hakkın temelini oluşturmaktadır.

3.4. Dijital Haklar Nasıl Korunur?

Veri kapitalizmi altında dijital hakların korunması üç şekilde mümkündür:

– Hukuki Koruma (Yasa ve Denetim)

Kişisel verilerin korunmasına yönelik yasal çerçeve, bireylerin dijital haklarını güvence altına almayı amaçlamaktadır. Avrupa Birliği GDPR ve Türkiye'deki KVKK, kişisel verilerin işlenmesini sınırlandıran başlıca yasal düzenlemelerdir (GDPR, 2018; KVKK, 2016). Bu yasalar, veri sorumlularına yükümlülükler getirirken, bireylere verileri üzerinde denetim hakkı tanımaktadır. Denetleyici kurumlar (örneğin, Avrupa Veri Koruma Otoritesi ve Türkiye'de Kişisel Verileri Koruma Kurumu) bu düzenlemelerin uygulanmasını sağlamak amacıyla çeşitli yaptırımlar uygulayabilmektedir.

Ancak büyük teknoloji şirketlerinin ulusötesi ve merkezîyet olmayan yapısı, ulusal yasal düzenlemelerin etki alanını daraltmakta ve hukuki yaptırımların etkinliğini azaltmaktadır (Zuboff, 2019).

– Teknolojik Araçlarla Koruma

Bireyler, dijital mahremiyetlerini korumak amacıyla çeşitli teknik araçlara başvurabilmektedir. Uçtan uca şifreleme teknolojileri (örneğin, Signal veya ProtonMail), veri iletimini güvenli hale getirirken; reklam ve izleme engelleyici tarayıcılar (örneğin, Brave Browser, uBlock Origin), kullanıcıların çevrimiçi hareketlerinin takip edilmesini önlemektedir. Ayrıca DuckDuckGo gibi gizlilik odaklı arama motorları, kullanıcı verilerini kaydetmeden hizmet sunmaktadır.

Bununla birlikte, bu tür araçların etkin kullanımı belirli düzeyde teknik bilgi gerektirdiğinden dijital koruma araçlarına erişim eşitsizliği oluşabilmektedir.

3.5. Kültürel ve Toplumsal Mücadele

Dijital hakların korunmasında hukuki ve teknolojik çabaların yanında kültürel ve toplumsal farkındalık da kritik rol oynamaktadır. Dijital okuryazarlığın artırılması, birey haklarını tanınması ve koruyabilmesi açısından önemlidir. Bunun yanı sıra, veri hakkı hareketleri (örneğin, *Data Justice* ve *Data Commons*) ile platform kooperatifleri gibi alternatif dijital ekonomi modelleri, dijital alanda daha adil ve kolektif çözümler sunmaktadır (Hintz et al., 2019).

Mozilla Vakfı, Electronic Frontier Foundation (EFF) ve Access Now gibi kuruluşlar, dijital hakların korunmasına yönelik küresel ölçekte çalışmalar yürütmektedir. Bu yapılar hem farkındalık oluşturmakta hem de hukuki ve teknik destek sağlamaktadır.

Veri kapitalizmi, dijital hakları özsel olarak tanımaz; bu haklar yalnızca bireylerin gönüllü olarak haklarından vazgeçmesi hâlinde işlerlik kazanır. Bu nedenle, dijital haklar yalnızca hukuki koruma meselesi değil; aynı zamanda politik ve etik bir mücadele alanıdır.

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

4. YAPAY ZEKÂ VE ALGORİTMİK KARAR ALMA

Algoritmik karar alma, insanların yerine ya da desteğiyle kararların, önceden tanımlı kurallar, veri modelleri veya öğrenen sistemler tarafından verilmesidir. Bu kararlar genellikle yapay zekâ sistemleri, makine öğrenimi, derin öğrenme veya basit kurallara dayalı algoritmalar aracılığıyla gerçekleşir.

Algoritmik karar alma süreçlerine birçok sektörde rastlamak mümkündür. Örneğin; finans alanında kredi puanlaması ve robot yatırım danışmanları, hukuki alanlarda (örneğin ABD’de COMPAS sistemiyle) mahkeme risk skora uygulama uygulamaları, insan kaynaklarında özgeçmiş tarama ve işe alım önerileri, sosyal medyada içerik önerisi, sansür ve görünürlük düzenlemeleri; sağlık alanında ise hastalık teşhisi, risk analizi ve ilaç önerileri bu sürecin örnekleri arasındadır. Güvenlik alanında ise yüz tanıma, suç tahmin sistemleri ve gözetim uygulamaları algoritmik karar alma sistemleriyle yürütülmektedir (Pasquale, 2015; Eubanks, 2018).

Bu sistemler, dijital ortamda toplanan kullanıcı davranışları, geçmiş işlemler ve demografik bilgiler gibi verileri, önceden tanımlanmış kurallar ya da makine öğrenimi ile oluşturulmuş modellerle değerlendirilerek karar üretirler. Örneğin, algoritmik sistem kullanan bir finans kuruluşu, 35 yaşında, düşük gelirli ve geçmişte borcunu aksatmış bir kullanıcıyı yüksek riskli olarak değerlendirip kredi başvurusunu reddedebilir.

Ancak yapay zekâ temelli algoritmalar, belirli riskleri de beraberinde getirmektedir. Bu risklerin başında **şeffaflık sorunu** (black box) gelmektedir. Algoritmanın karar verme süreci çoğu zaman anlaşılmaz olduğundan, özellikle kamusal hizmetlerde ve adalet sisteminde ciddi sakıncalar ortaya çıkabilir. Ayrıca, algoritmaların kullandığı veriler hatalı, yanlış veya eksikse, bu durum karar süreçlerine de yansır. Örneğin, kadın adayların teknik pozisyonlara önerilmemesi gibi örnekler algoritmik önyargılara işaret eder (Noble, 2018).

Algoritmaların belirli toplumsal grupları sistematik biçimde dışlaması mümkündür. Bu kararların nasıl verildiği anlaşılmadığında, bireylerin kararlara itiraz etme yolları da kapanır. Örneğin, algoritmik bir kredi reddi durumunda kullanıcı, kararın nedenini anlayamayabilir ve bu nedenle hakkını arayamayabilir (Wachter, Mittelstadt, & Floridi, 2017).

Bu tür sorunlar nedeniyle çeşitli hukuki önlemler alınmaktadır. Avrupa Birliği tarafından kabul edilen Yapay Zekâ Yasası (AI Act), algoritmik karar alma süreçlerinin açıklanabilir, şeffaf ve insan denetimine açık olmasını zorunlu kılmaktadır. Ayrıca GDPR’ın 22.

maddesinde, bireylerin yalnızca otomatik işleme dayalı bir karara tabi tutulmama hakkına sahip olduğu açıkça belirtilmektedir (GDPR, 2018).

Algoritmik karar alma sistemlerinin daha adil işlemesi için bazı önlemler alınabilir. Öncelikle, sistemlerin işleyişi kullanıcılar tarafından anlaşılabilir biçimde açıklanmalı; kullanılan algoritmalar dış uzmanlarca incelenebilir olmalı ve karar süreçlerinde nihai yetki insanda bulunmalıdır. Ayrıca, algoritmaların ayrımcılık üretip üretmediği düzenli olarak test edilmeli ve kullanıcıların algoritmik kararları sorgulama ve itiraz etme hakkı güvence altına alınmalıdır.

4.1. Veri Kapitalizminde Algoritmik Kararlar

Günümüz dijital dünyasında yapay zekâ, bireylerin davranışlarını şekillendiren ve kurumların kararlarını belirleyen otomatik, veri temelli sistemler aracılığıyla işlemektedir. Büyük teknoloji şirketleri, topladıkları devasa kişisel verileri karar destek sistemlerine, otomatik önerilere ve davranışsal tahminlere dönüştürmektedir.

Bu süreçte dijital platform kullanıcılarının davranışları, tercihleri, tıklamaları, konumları ve yüz ifadeleri birer veriye dönüştürülmektedir. Yapay zekâ sistemleri bahsi geçen verileri kullanarak çeşitli davranış kalıplarını ortaya çıkarmakta ve bireyleri “riskli” ya da “riskli değil” gibi kategorilere ayırmaktadır. Örneğin, bir kullanıcı hakkında “kredisini geri ödeyemez” öngörüsü yapılabilmekte, bu sınıflandırmalar da çeşitli karar mekanizmalarında belirleyici olmaktadır. Sosyal medya algoritmaları, sınıflandırmalara göre hangi içeriği kimin göreceğine karar verirken; bankacılık algoritmaları, kimin kredi alabileceğini; e-ticaret platformları ise hangi kullanıcıya, hangi ürünün, hangi fiyattan gösterileceğini belirlemektedir. Bu tür algoritmalar, başta reklamcılık ve finans olmak üzere işe alım süreçleri, dijital platform hizmetleri ve kamu politikalarında (örneğin, suç tahmini ve sosyal yardım algoritmaları gibi) yaygın biçimde kullanılmaktadır.

Algoritmik karar alma süreçleri; Meta, Google, Amazon gibi dijital platformlara, kullanıcıların yalnızca mevcut değil, gelecekteki tercihlerini de belirleme ve yönlendirme gücü kazandırmaktadır. Veri kapitalizmi bağlamında dijital platformlar, kullanıcıları sadece tanımakla yetinmemekte; onları öngörme, ikna etme ve yönlendirme kapasitesine de sahip olmaktadır. Bu nedenle algoritmalar, yalnızca teknik araçlar değil, aynı zamanda birer iktidar mekanizması hâline gelmektedir (Zuboff, 2019).

4.2. Siber Bağımlılık ve Dijital Altyapı Eşitsizlikleri

Siber bağımlılık, dijital çağın bireyler ve toplum üzerindeki en yaygın ancak görünmez etkilerinden biri olarak öne çıkmaktadır. Teknolojik gelişmeler yaşamı pek çok açıdan kolaylaştırmakla birlikte, dijital teknolojilerin kontrolsüz ve sürekli kullanımı bireyleri fiziksel, zihinsel ve sosyal yönden olumsuz etkileyebilmektedir. Bireylerin dijital teknolojilere (örneğin internet, sosyal medya, dijital oyunlar, akıllı telefonlar ve ekranlar) aşırı ve kontrolsüz şekilde bağımlı hâle gelmesi; psikolojik, sosyal ve fiziksel işlevlerinde bozulmalara yol açabilmektedir. Bu bağlamda siber bağımlılık, kumar bağımlılığı gibi davranışsal bağımlılık türlerinden biri olarak kabul edilmektedir.

Siber bağımlılık, farklı biçimlerde kendini gösterebilir. Örneğin, sürekli ekran kontrolü ve bildirim uyarılarının tetiklediği akıllı telefon bağımlılığı; internette amaçsız ve saatler süren gezinmelerin oluşturduğu internet bağımlılığı; sanal oyunlara yoğun ilgi ve sürekliliğin neden olduğu oyun bağımlılığı; beğeni, paylaşım ve takip gibi sosyal geri bildirimlere dayalı sosyal medya bağımlılığı ile sürekli video, dizi ve içerik tüketiminin yol açtığı dijital içerik bağımlılığı bu türlere örnek olarak gösterilebilir.

Dijital bağımlılığın birçok fiziksel, psikolojik ve sosyal belirtisi bulunmaktadır. Göz kuruluğu, baş ağrısı, uyku düzensizlikleri ve sürekli ekran kontrolü gibi fiziksel belirtiler, bireyde dijital bağımlılık eğiliminin göstergesi olabilir. Psikolojik belirtiler arasında ise huzursuzluk, öfke, dikkat dağınıklığı, gerginlik, kaygı ve gerçeklikten uzaklaşma gibi durumlar öne çıkmaktadır. Dijital bağımlılık, aynı zamanda bireyin toplumsal bağlarını zayıflatabilir; sosyal izolasyona, yüz yüze iletişimde zorlanmalara ve okul ya da iş gibi sorumlulukların aksamasına neden olabilir.

Bu bağımlılık türünün temelinde ise çoğunlukla psikolojik nedenler yer almaktadır. Bireyler teknolojiyi yalnızca bir araç olmaktan çıkararak; duygusal, zihinsel ve sosyal ihtiyaçların tatmin aracı hâline getirmektedir. Özellikle stres, yalnızlık, sosyal onay ihtiyacı ve düşük özsaygı gibi faktörler, bireyleri dijital dünyaya daha fazla yönlendirmekte ve bağımlılık riskini artırmaktadır.

4.2.1. Dijital Bağımlılığın Psikolojik Nedenleri

– Dopamin Arayışı (Anlık Haz Döngüsü)

Dijital platformlar (sosyal medya, oyun, video) beyin ödül sistemi üzerinden işler. Beğeni almak, yeni bir bildirim görmek, oyunda seviye atlamak gibi eylemler dopamin salgısına neden olur. Zamanla oluşan haz duygusu, beyinde bir bağımlılık biçimine dönüşür ve birey

tekrar tekrar aynı davranışa yönelir. Böylece, “sadece beş dakika” diyerek başlanan kullanım saatlerce sürebilir.

– **Gerçeklikten Kaçış**

Zihinsel stres, yalnızlık ve düşük benlik algısı gibi psikolojik durumlar yaşayan bireyler için dijital dünya bir kaçış alanı hâline gelir. Oyunlar, sosyal medya veya dijital içerikler aracılığıyla gerçeklikten uzaklaşmak mümkündür.

– **Sosyal Onay İhtiyacı (FOMO ve Beğeni Dürtüsü)**

İnsan psikolojisi onaylanma ve kabul görme ihtiyacıyla şekillenir. Sosyal medyada alınan beğeni ve yorumlar bu ihtiyacı hızlı ve yapay bir şekilde karşılarken, aynı zamanda FOMO (Fear of Missing Out – bir şeyleri kaçırma korkusu) hissini de tetikler. Birey, dışlanma kaygısıyla sürekli çevrimiçi kalma ihtiyacı hisseder.

– **Düşük Benlik Saygısı ve Öz-Yeterlilik Eksikliği**

Gerçek yaşamda kendini yetersiz, başarısız veya görünmez hisseden bireyler, dijital dünyada daha güçlü, takdir edilen ve önemli bir kimlik kazanabilir. Özellikle oyunlar aracılığıyla kısa sürede sağlanan başarı hissi (rozet, seviye, skor) bu duyguyu pekiştirir. Böylece “gerçek hayatta başaramıyorum ama burada başarılıyım” düşüncesi, dijital bağımlılığı derinleştirir.

– **Yalnızlık ve İletişim Eksikliği**

Gerçek sosyal ilişkileri zayıf olan bireyler, dijital ortamları oluşan boşluğu doldurmak için kullanabilir. Bu durum bireyin yüzeysel ama sürekli dijital ilişkiler kurmasına neden olur. Zamanla gerçek sosyal bağların yerini dijital bağlar alır ve yalnızlık hissi derinleşir.

– **Duygusal Düzenleme Zorluğu**

Stres, öfke, can sıkıntısı gibi duygularla başa çıkmakta zorlanan bireyler, dijital ortamları bir kaçış ya da “dijital uyuşturucu” gibi kullanabilir. Oluşan geçici rahatlama hissi, uzun vadede bağımlılığın gelişmesine neden olur. Böylece ekran kullanımı, duygusal olgunlaşmanın yerine “duygu bastırma” alışkanlığına dönüşür.

– Özgürlük ve Kontrol Yanılsaması

Dijital dünyada bireyler kendilerini daha özgür hisseder; istediklerini paylaşabilir, farklı kimlikler edinebilirler. Bu durum, gerçek hayattaki sınırlardan kaçma arzusunu besler ve dijital dünyada sınırsız bir kontrol yanılsamasına neden olur. Sonuçta, bireyin gerçek dünyaya ilgisi azalır ve dijital kimliklere bağlılık artar.

Dijital dünya, bireyleri bir psikolojik döngü içerisine sokar. Gerçek hayatta yaşanan stres, boşluk ve yalnızlık gibi duygulara karşılık dijital dünyada dopamin etkisiyle geçici bir rahatlama sağlanır. Ancak geçici rahatlama uzun vadede gerçek sorunları daha da büyütür. Sorunlar büyüdükçe birey tekrar dijitale yönelir ve böylece bağımlılık döngüsü güçlenir. Bu süreçte ekranla etkileşim, beynin ödül sistemini sürekli tetikleyerek tıpkı madde bağımlılığında olduğu gibi “ödül beklentisi – tekrar etme” döngüsünü doğurur.

4.3. Dijital Altyapı Eşitsizlikleri

Bireylerin ve toplumların dijital teknolojilere erişim, kullanım ve teknolojilerden faydalanma düzeyleri farklılık göstermektedir. Bu farklar yalnızca teknik bir "erişim" meselesi değil; aynı zamanda sosyoekonomik, kültürel ve politik etkileri olan yapısal bir eşitsizliğin sonucudur.

Dijital altyapı eşitsizliği; bireylerin donanım (cihaz, bilgisayar, telefon), bağlantıya (internet erişimi, hız ve istikrar), yazılımlara (uygulama, platform, güvenlik), becerilere (dijital okuryazarlık) ve katılıma (veri üretimi-tüketimi, ifade özgürlüğü, temsil edilme) farklı düzeylerde erişebilmesi anlamına gelir. Bu eşitsizlik yalnızca dijital ortamlarda değil, aynı zamanda ekonomik, toplumsal ve siyasal alanlarda da güce erişimi belirleyici bir faktör haline getirmektedir. Dijital altyapı eşitsizliği, 21. yüzyılın görünmeyen ancak etkili sınıfsal ayrımlarından biridir.

4.3.1. Dijital Altyapı Eşitsizliğinin Boyutları

– Erişim Eşitsizliği

Fiziksel bağlantı altyapısının eksikliği, özellikle kırsal bölgelerde önemli bir sorundur. Elektrik altyapısından yoksun olan bölgelerde dijital dünyaya erişim mümkün olmamaktadır. Geniş bant internet altyapısının bulunmadığı yerlerde mobil veri bir alternatif olsa da daha pahalı ve daha yavaş bir bağlantı sağlamaktadır. Örneğin, Afrika kıtasındaki bazı ülkelerde nüfusun yalnızca %20'si sabit internet erişimine sahiptir. Uluslararası Telekomünikasyon Birliği (ITU, 2023) verilerine göre, dünya genelinde yaklaşık

2,6 milyar insan hâlâ internet erişiminden yoksundur. Özellikle Sahra Altı Afrika, Güney Asya ve bazı Latin Amerika ülkelerinde kırsal bölgelerde sabit internet erişimi %20'nin altındadır (World Bank, 2021).

– **Donanım Eşitsizliği**

Dijital dünyaya erişimde donanım farkları da büyük önem taşımaktadır. Güncel, hızlı ve işlevsel cihazlara sahip olmayan bireyler—örneğin eski model telefon veya paylaşımlı bilgisayar kullananlar—dijital dünyanın sunduğu birçok içeriğe erişememektedir. Bu durum özellikle eğitim ve çalışma alanlarında ciddi kısıtlamalara yol açmaktadır. Covid-19 pandemisi sırasında, birçok çocuk evlerinde yalnızca eski cihazların bulunması nedeniyle uzaktan eğitime erişememiştir. Bilgisayar, tablet ya da akıllı telefon gibi cihazlara erişim, eğitime katılım ve iş yaşamına dâhil olabilmek açısından belirleyici bir unsurdur. UNICEF ve ITU'nun ortak yayımladığı rapora göre, düşük gelirli ülkelerdeki öğrencilerin %67'sinin evinde bilgisayara erişim bulunmamaktadır (UNICEF & ITU, 2020).

– **Dijital Beceriler Eşitsizliği**

Dijital okuryazarlık yalnızca teknik bilgiyle sınırlı değildir; aynı zamanda eleştirel düşünme, bilgi doğrulama ve dijital güvenlik farkındalığı gibi bilişsel ve davranışsal becerileri de içerir. Kadınlar, yaşlılar, düşük gelirli gruplar ve göçmenler, dijital beceriler açısından dezavantajlı konumda bulunma eğilimindedir. Örneğin, OECD ülkelerinde yapılan ölçümlere göre düşük gelirli öğrencilerin dijital okuryazarlık testlerinde daha düşük başarı sergilediği görülmektedir. Donanım ve internet bağlantısına sahip olmak, dijital teknolojilerden verimli şekilde faydalanmak için yeterli değildir. Kullanıcıların teknolojileri etkin, güvenli ve eleştirel biçimde kullanma yetkinlikleri de gereklidir. OECD'nin PISA 2018 verileri, düşük sosyoekonomik geçmişe sahip öğrencilerin dijital ortamda bilgi arama, doğrulama ve analiz etme becerilerinin sınırlı olduğunu göstermektedir (OECD, 2019).

– **Hizmet Kalitesi Eşitsizliği**

Aynı ülke içerisinde farklı bölgelerde internet hızı ve fiyatı önemli ölçüde değişiklik gösterebilmektedir, kırsal bir bölgede 5 Mbps hızla eğitim almaya çalışan bir öğrenci ile kent merkezinde 100 Mbps bağlantıya sahip bir öğrencinin sahip olduğu sosyal ve ekonomik fırsatlar aynı değildir, yani dijital erişimde yalnızca varlık değil, hizmetin kalitesi de önemlidir. İnternetin yavaşlığı, kesintili olması ya da yüksek maliyetli oluşu dijital eşitsizliği derinleştirir. Alliance for Affordable Internet (A4AI, 2022) raporuna göre, birçok düşük gelirli ülkede mobil veri fiyatları, asgari ücretin %10'una kadar ulaşabilmektedir.

– **Veri Erişimi ve Katılım Eşitsizliği**

Dijital eşitsizlik yalnızca teknolojiye erişimle sınırlı değildir; bireylerin bu süreçlere katılımı da bu eşitsizliklerden etkilenmektedir. Veri üretim hakkı, teknik olduğu kadar politik bir meseledir. Hangi bireylerin veri ürettiği, hangi verilerin toplandığı ve bu verilerden kimin ekonomik fayda sağladığı gibi sorular, dijital katılım eşitsizliğinin özünü oluşturur. Gelişmekte olan ülkelerde faaliyet gösteren küresel şirketler, bu bölgelerden topladıkları verileri işleyerek büyük ekonomik kazançlar elde etmekte, ancak bu kazançların kaynağı olan ülkelere herhangi bir geri dönüş sağlanmamaktadır. Bu durum, literatürde “veri sömürgeciliği” (data colonialism) kavramı ile tanımlanmaktadır (Couldry & Mejias, 2019).

4.3.2. Dijital Altyapı Eşitsizliğinin Sonuçları ve Çözüm Önerileri

Dijital altyapıdaki eşitsizlikler; eğitim, istihdam, sosyal katılım ve demokratik haklara erişim gibi birçok alanda etkilere yol açmaktadır. Uzaktan eğitime erişemeyen öğrenciler, uzun vadeli öğrenme kayıpları yaşamaktadır. Dijital becerilere sahip olmayan bireyler, iş gücü piyasasında dezavantajlı duruma düşmekte ve dışlanabilmektedir. Ayrıca, dijital okuryazarlığı düşük bireylerin e-devlet hizmetlerine erişimde güçlük yaşaması, söz konusu kişilerin demokratik süreçlere katılımını sınırlandırmaktadır. Bu bireyler aynı zamanda dijital dolandırıcılık ve veri ihlallerine karşı da savunmasız hale gelmektedir.

Ortaya çıkan eşitsizliklere karşı kısa, orta ve uzun vadeli çözüm önerileri geliştirilebilir. Kısa vadede kamusal alanlarda ücretsiz Wi-Fi hizmetlerinin sunulması, internet sübvansiyonlarının uygulanması, düşük maliyetli cihazların temini ve okullarda dijital beceri eğitimlerinin yaygınlaştırılması etkili olabilir. Orta ve uzun vadede ise geniş bant altyapısının yaygınlaştırılması için devlet-özel sektör iş birlikleri kurulmalı, dijital haklar anayasal düzeyde güvence altına alınmalı ve yerel veri üretimi desteklenmelidir. Bu kapsamda, veri egemenliği politikalarının hayata geçirilmesi büyük önem taşımaktadır.

5. ULUSLARARASI VERİ POLİTİKALARI VE DİJİTAL EGEMENLİK

5.1. Uluslararası Veri Politikaları

Uluslararası veri politikaları; verinin toplanması, işlenmesi, saklanması, paylaşılması ve sınır ötesi aktarımı gibi süreçlerin nasıl düzenleneceği konusunda ülkelerin ve uluslararası kurumların benimsediği yasal, teknik ve etik çerçeveleri kapsamaktadır. Bu politikalar yalnızca bireylerin mahremiyeti açısından değil; ekonomik rekabet, ulusal güvenlik, dijital egemenlik ve jeopolitik güç dengeleri bakımından da kritik önemdedir. Veri, 21. yüzyılda petrol kadar değerli, hatta daha stratejik bir kaynak haline gelmiştir. Devletler ve uluslararası kuruluşlar, veri akışını düzenleyen politikalar aracılığıyla dijital çağın ekonomik, siyasal ve güvenlik boyutlarını yeniden şekillendirmektedir.

Ülkeler, vatandaşlarının kişisel verilerinin korunması (siber güvenlik), verinin ülke sınırları içinde yerelleştirilmesi, sınır ötesi veri akışının yönetilmesi ve veriden doğan ekonomik değerin ülke içinde kalmasını sağlamak gibi gerekçelerle ulusal ve uluslararası düzeyde veri politikaları geliştirmektedir.

5.1.1. Veri Politikalarının Kapsamı ve Kavramsal Çerçeve

Veri politikaları; kişisel ve kurumsal verilerin toplanması, işlenmesi, saklanması, paylaşılması ve sınır ötesi transferi gibi süreçleri düzenleyen kurallar bütünüdür. Veri egemenliği (data sovereignty), verinin üretildiği ülkenin o veri üzerinde sahiplik ve denetim hakkına sahip olması gerektiği anlayışını ifade ederken; veri akışkanlığı (data flow), verinin ülke sınırları içinde ya da dışında serbest dolaşımını ifade eder (Aaronson, 2018).

5.1.2. Temel Uluslararası Yaklaşımlar

▪ Avrupa Birliği: Veri Hakları ve Dijital Egemenlik

AB, veri politikalarında en gelişmiş ve hak temelli rejimi benimsemiştir. Bu kapsamda 2018 yılında yürürlüğe giren GDPR, tüm bireylere veri üzerinde kontrol hakkı tanımaktadır. GDPR'ın temel ilkeleri arasında veri minimizasyonu, açık rıza, unutulma hakkı ve veri taşınabilirliği yer almaktadır. AB dışındaki ülkelere veri alınabilmesi için “yeterli koruma düzeyi” şartı aranmaktadır. GDPR, küresel ölçekte veri işleme standartlarını belirleyerek “Brüksel Etkisi” oluşturmuş ve küresel firmaları AB kurallarına uyum sağlamaya zorlamıştır (Bradford, 2020; De Hert & Papakonstantinou, 2016).

▪ ABD: Serbest Veri Akışı ve Sektörel Düzenleme

ABD’de ulusal düzeyde kapsamlı bir genel veri koruma yasası bulunmamakta, bunun yerine sektör bazlı düzenlemeler tercih edilmektedir. Sağlık (HIPAA), çocuklar (COPPA) ve

finans (GLBA) gibi alanlarda sektörel yasalar mevcuttur. ABD, uluslararası düzeyde serbest veri akışını savunur ve verinin yerleştirilmesine karşıdır. Büyük teknoloji firmalarının çoğunlukla ABD merkezli olması nedeniyle, ülke veri politikalarında şirket çıkarlarını önceleyen bir yaklaşım benimsemektedir. Bu yaklaşım, veri mahremiyeti açısından AB'ye kıyasla daha zayıf kullanıcı koruması sağlamaktadır (Schwartz & Solove, 2011).

▪ Çin: Veri Güvenliği ve Dijital İstikrar

Çin, veriyi ulusal güvenliğin ayrılmaz bir parçası olarak değerlendirmektedir. Ülkede 2021 yılında yürürlüğe giren Veri Güvenliği Yasası (Data Security Law) ve Kişisel Bilgilerin Korunması Yasası (Personal Information Protection Law – PIPL) ile kapsamlı bir veri düzenleme çerçevesi oluşturulmuştur. Çin merkezli şirketlerin verileri yurt dışına aktarması, devletin onayına tabi tutulmuştur. Veri yerelleştirmesi zorunlu hale getirilmiş; özellikle kritik verilerin Çin sınırları içerisinde depolanması şart koşulmuştur. Ayrıca Çin devleti, bu veriler üzerinde geniş kapsamlı gözetim ve erişim hakkına sahiptir.

Çin'de dijital altyapı ve veri üzerindeki denetim, "siber egemenlik" ilkesi doğrultusunda sağlanmaktadır. Bu yaklaşımın temel amacı; dijital egemenliğin tesis edilmesi, ulusal güvenliğin sağlanması ve siyasi istikrarın korunmasıdır. Ancak bu model, beraberinde "dijital otoriterlik" (digital authoritarianism) tartışmalarını da gündeme getirmiştir (Liu, 2021).

▪ Diğer Ülkeler

Afrika ve Latin Amerika'daki birçok ülke, veri politikalarını geliştirirken Avrupa Birliği modelini örnek almakta; aynı zamanda veri kaynaklarının Batılı teknoloji şirketleri tarafından sömürülmesini eleştirmektedir. Veri kaynaklarının gelişmekte olan ülkelere toplanarak, bu verilerden elde edilen ekonomik değer daha çok kuzey ülkelerinde üretilmesine "veri sömürgeciliği" (data colonialism) adı verilmektedir (Couldry & Mejias, 2019).

Afrika Birliği, kıta genelinde veri yönetişimini sağlamak amacıyla "Data Policy Framework for Africa" başlıklı belgeyi 2022 yılında yayınlamıştır (African Union, 2022). Latin Amerika'da ise, Brezilya örneğinde olduğu gibi, Genel Kişisel Veri Koruma Yasası (LGPD) ile birçok ülke, AB'nin GDPR modeline benzer düzenlemeleri uygulamaya koymaya başlamıştır.

5.2. Veri Konusunda Uluslararası Çatışma ve İş Birliği Alanları

Uluslararası veri politikaları; yalnızca mahremiyet ve dijital hakları değil, aynı zamanda ticaret, güvenlik, egemenlik ve ekonomik rekabet gibi çok boyutlu ve kritik alanları da doğrudan etkilemektedir. Bu nedenle, veri politikaları kimi zaman ülkeler ve bölgesel

bloklar arasında ciddi gerilimlere neden olurken, diğer yandan belirli alanlarda iş birliği mekanizmalarının gelişmesine de zemin hazırlamaktadır.

5.2.1. Çatışma Alanları

– Veriyi Yerelleştirme vs. Serbest Veri Akışı

Veri yerelleştirme, ülkelerin verileri kendi sınırları içinde depolanmasını ve işlenmesini zorunlu kıldığı bir uygulamadır. Buna karşın serbest veri akışı, dijital ticaretin kesintisiz şekilde sürdürülebilmesi için sınır ötesi veri dolaşımını savunmaktadır. Bu bağlamda, farklı ülke blokları arasında uygulamalara ilişkin ciddi görüş ayrılıkları ve çıkar çatışmaları ortaya çıkmaktadır.

Örneğin, Avrupa Birliği yeterli koruma düzeyine sahip olmayan ülkelere veri aktarımını GDPR kapsamında sınırlandırmaktadır (GDPR, madde 45; Bradford, 2020). ABD ise serbest veri akışını desteklemekte ve veri yerelleştirmeyi dijital ticaret açısından bir engel olarak değerlendirmektedir (WTO, 2020). Öte yandan, Çin ve Rusya gibi ülkeler, kritik verilerin dışa aktarımını ulusal güvenlik gerekçesiyle büyük ölçüde yasaklamaktadır (Data Security Law, 2021).

– Hukuki Yetki ve Yargı Alanı Çatışmaları

Veri, nerede işlendiğinden ziyade nereden kaynaklandığına göre bir ülkenin hukukuna tabi olabilir. Bu durum, çifte yargı yetkisi (dual jurisdiction) sorununu doğurmakta ve uluslararası düzeyde hukuki çatışmalara zemin hazırlamaktadır. Örneğin, 2018 yılında ABD hükümetinin Microsoft'tan, İrlanda'daki sunucusunda bulunan bir e-postayı talep etmesi, ciddi yargı uyuşmazlıklarına neden olmuştur. Benzer şekilde, 2020 yılında Avrupa Adalet Divanı tarafından verilen Schrems II kararında, ABD'nin gözetim yasaları gerekçe gösterilerek "Privacy Shield" veri aktarım mekanizması iptal edilmiştir. Bu iptalin ardından, AB ve ABD arasında yeni bir çerçeve olan Trans-Atlantic Data Privacy Framework geliştirilmeye çalışılsa da düzenlemenin güvenlik seviyesi ve hukuki yeterliliği halen tartışmalıdır (CJEU, 2020).

– Ulusal Güvenlik Gerekçesiyle Veri Erişimi Talebi

Devletler, kimi zaman terör, casusluk veya siber tehdit gerekçeleriyle veri şirketlerinden kullanıcı verilerine erişim talep edebilmektedir. Bu durum, teknoloji şirketlerini bireysel mahremiyet ile devlet baskısı arasında zor bir tercihe zorlamaktadır. Örneğin, 2016 yılında FBI ile Apple arasında, San Bernardino saldırısına ilişkin bir iPhone'un şifresinin kırılması yönünde yaşanan kriz gerilime neden olmuştur. Benzer biçimde, TikTok'un kullanıcı verilerini Çin hükümetiyle paylaştığı iddiaları nedeniyle ABD ve Avrupa Birliği'nde çeşitli dönemlerde yasaklama girişimleri olmuştur (Greenleaf, 2018).

– **Yapay Zekâ ve Algoritmik Şeffaflıkta Uyum Sorunları**

Yapay zekâ sistemlerinin kullandığı veriler ve bu verilerle alınan kararlar, ülkeden ülkeye farklı etik ve hukuki değerlendirmelere tabi tutulmaktadır. Avrupa Birliği, yüksek riskli algoritmalar için denetim, şeffaflık ve insan denetimi gibi kriterleri zorunlu hale getiren bir yasa tasarısı hazırlamıştır (European Commission, 2021). Buna karşın, ABD ve Çin'de daha esnek ve piyasa odaklı yaklaşımlar benimsenmiş; inovasyonu sınırlamamak adına daha serbest bir düzenleme ortamı oluşturulmuştur.

5.2.2. İş Birliği Alanları

– **Veri Standartları ve Teknik Protokoller Üzerinde İş Birliği**

Ülkeler farklı hukuki yaklaşımlar benimsemiş olsalar da teknik düzeyde veri aktarımı için ortak standartlara ihtiyaç duymaktadır. Bu amaçla, ISO/IEC 27001 gibi güvenlik standartları ve OECD'nin veri yönetişimi ilkeleri geliştirilmiştir. Ayrıca W3C ve IETF gibi teknik kuruluşlarda ülkeler arasında veri mimarisi, şeffaflık ve erişim kolaylığı gibi konularda birlikte çalışmalar yürütülmektedir (OECD, 2021).

– **Veri Güvenliğine Dayalı Serbest Akış (DFFT)**

G20 ve G7 ülkeleri, 2019 Osaka Zirvesi'nde "Data Free Flow with Trust" (DFFT) ilkesini benimsemiştir. Bu ilke; kişisel mahremiyetin korunması, veri güvenliği, dijital güven ilişkilerinin tesisi gibi alanlarda güvenilirliği sağlayarak uluslararası veri akışını teşvik etmeyi amaçlamaktadır. Bu kapsamda Avrupa Birliği ve Japonya arasında karşılıklı "uygunluk" anlaşmaları yapılmış ve veri alışverişine yasal zemin oluşturulmuştur (G20, 2019).

– **Çift Taraflı ve Bölgesel Anlaşmalar**

Avrupa Birliği, GDPR kapsamında "yeterlilik kararları" ile bazı ülkeleri veri aktarımı açısından güvenli olarak tanımaktadır. Japonya, İsviçre ve Güney Kore gibi ülkeler bu kapsamda yer almaktadır. AB ile Japonya arasında Karşılıklı Uyum Mekanizması kurulmuş ve yüksek seviyede kişisel veri koruma standartları benimsenmiştir. Latin Amerika ülkeleri ise Ibero-Amerikan Veri Koruma Ağı aracılığıyla bölgesel veri politikaları geliştirmeye çalışmaktadır. Afrika kıtasında ise Smart Africa Alliance girişimi, dijital altyapı ve veri paylaşımı alanında bölgesel iş birliğini hedeflemektedir.

– **Siber Güvenlik ve Siber Suçlarla Mücadelede İş Birliği**

Siber saldırılar, küresel ölçekte organize olabildiğinden tekil ülke çabaları yetersiz kalmaktadır. Bir saldırganın başka bir ülkenin sunucusunu kullanarak üçüncü bir ülkenin kritik altyapısını hedef alması mümkündür. Bu durum, yargı alanlarının çakışması, dijital

delillerin farklı ülkelerde bulunması (örneğin log kayıtları) ve altyapıların küresel bağlılığı nedeniyle uluslararası düzeyde iş birliği gerektirmektedir. Özellikle bankacılık, enerji ve sağlık gibi alanlarda yaygın fidye yazılım saldırılarına karşı ortak savunma stratejileri geliştirilmesi elzemdir.

Siber suçlarla mücadelede uluslararası temel mekanizmalar şunlardır:

- ✓ **Budapeşte Sözleşmesi (2001) – Avrupa Konseyi Siber Suçlar Sözleşmesi:** İlk ve en kapsamlı uluslararası siber suç sözleşmesidir. 68 ülke tarafından imzalanmıştır (AB ülkeleri, ABD, Japonya, Türkiye, Kanada vb.). Siber suçları tanımlar ve cezai kovuşturma, kanıt paylaşımı, hızlı iletişim mekanizmaları gibi hükümler içerir (Council of Europe, Convention on Cybercrime, ETS No. 185).
- ✓ **Interpol – Küresel Polis Ağı:** Interpol'ün Siber Suçlar Merkezi (Cybercrime Directorate), üye ülkeler arasında tehdit istihbaratı paylaşımı, operasyonel destek ve soruşturma koordinasyonu sağlar. Örneğin, Operation Cyclone ile 30'dan fazla ülkede ATM'lere yönelik siber saldırı çetesi çökertilmiştir (Interpol Annual Cybercrime Report, 2023).
- ✓ **Europol – Avrupa Siber Suç Merkezi (EC3):** Avrupa'daki organize siber suçlarla mücadele için oluşturulmuştur. AB içi ve dışı ortak operasyonları koordine etmektedir. Dijital adli analiz, fidye yazılımı soruşturmaları ve çevrimiçi istismar gibi alanlara odaklanır. Örneğin, No More Ransom Platformu, fidye yazılımı mağdurlarına ücretsiz çözüm araçları sağlamaktadır ve 188 ülkeden erişim sağlanmıştır (Europol, EC3 Activity Report, 2022).
- ✓ **Birleşmiş Milletler (UNODC):** Siber suçları transnasyonal organize suç olarak ele almaktadır. 2023'te "Kapsayıcı Uluslararası Siber Suç Sözleşmesi" taslağı için müzakerelere başlanmıştır; ancak normatif çatışmalar (özellikle ifade özgürlüğü ve devlet kontrolü gibi) sözleşmenin kabulünü zorlaştırmaktadır (UNODC Cybercrime Repository, 2024; Council of Europe, Convention on Cybercrime).

– **Veri Paylaşımı ve Araştırma İçin Açık Veri İş Birlikleri**

Dünya Ticaret Örgütü (WTO), dijital ticaretin sürdürülebilirliği için kesintisiz veri akışlarının önemini vurgularken; OECD ve UNESCO, kamu verilerinin şeffaf, erişilebilir ve adil biçimde paylaşılmasının, araştırma ve kamusal yarar açısından kritik olduğunu belirtmektedir (UNESCO, 2021; OECD, 2019). Nitekim pandemi döneminde sağlık verilerinin küresel düzeyde paylaşımı, bu ilkelerin pratiğe yansımaya örnek teşkil etmiştir.

– **Gelecekle İlgili Eğilimler**

Uluslararası veri politikaları, hızla dijitalleşen dünyada ekonomik rekabet, teknolojik gelişmeler ve birey hakları etrafında şekillenmektedir. Bu alan yalnızca geçmişe dönük düzenlemelerle değil; aynı zamanda hızla evrilen riskler, fırsatlar ve stratejik denklemlerle birlikte geleceğe yönelik politika yaklaşımlarıyla da ele alınmaktadır.

Bu kapsamda ülkeler, giderek veriyi hem ekonomik bir kaynak hem de ulusal güvenlik unsuru olarak değerlendirmekte ve veri üzerinde politik kontrol, yani *veri egemenliği* talebini artırmaktadır. Örneğin, Çin, Rusya ve Hindistan gibi ülkeler veri yerelleştirme uygulamalarını yaygınlaştırırken; Avrupa Birliği, dijital stratejilerinde “veri özgürlüğü” (*data autonomy*) kavramına vurgu yapmaktadır. Küresel veri akışını savunan ABD gibi ülkeler ile veri yerelleştirme eğilimindeki ülkeler arasında bu nedenle çeşitli çatışmalar yaşanmaktadır. Bu durum, dijital dünyanın çok merkezli ve parçalanmış bir internet yapısına—yani “Splinternet”e—doğru evrilmesine yol açmaktadır (Aaronson, 2021).

Ayrıca günümüzde dijital altyapıların yalnızca teknik değil, aynı zamanda politik ve stratejik bir öneme sahip olması, kendi verisini kendi yöneten federatif modellerin gelişimini tetiklemektedir. Örneğin, Gaia-X, Avrupa merkezli ve bulut veri işleme süreçleri için açık, şeffaf ve egemen bir altyapı hedeflemektedir. Hindistan ise Data Empowerment and Protection Architecture (DEPA) modeli ile veriyi kullanıcı merkezli yöneten bir sistem kurmuştur. Önümüzdeki dönemde, kamusal çıkarı ve şeffaflığı merkeze alan veri platformlarının ön plana çıkması beklenmektedir (European Commission, 2020).

Veriden doğan değerın daha adil dağılması ve bireylerin dijital ortamlardaki haklarının güçlendirilmesi, özellikle Avrupa Birliği ve Küresel Güney ülkelerinde giderek yükselen bir taleptir. Bu bağlamda, veri adaleti kavramı veriye erişim, temsiliyet, denetim ve fayda paylaşımı temelli bir yaklaşım olarak öne çıkmakta; ayrıca yapay zekâ etiği, şeffaf algoritmalar ve rızaya dayalı veri kullanımı gibi ilkeler de uluslararası normlara dönüşmektedir (Taylor, 2017; UN OHCHR, 2022).

Yapay zekâ sistemlerinin başarısı, doğru ve nitelikli veriye dayanmaktadır. Bu nedenle veri politikaları artık yalnızca mahremiyetle sınırlı kalmamakta; aynı zamanda yapay zekânın etik, şeffaf ve güvenli kullanımı açısından da değerlendirilmektedir. Örneğin, Avrupa Komisyonu tarafından hazırlanan 2024 tarihli AB Yapay Zekâ Yasası taslağı, “yüksek riskli” yapay zekâ sistemleri için veri kalitesi, ayrımcılık denetimi ve algoritmik şeffaflık gibi kriterleri zorunlu kılmaktadır (European Commission, 2021). Bu çerçevede, gelecekte yapay zekâ uygulamalarının “veri denetimi” mekanizmalarıyla birlikte işletilmesi zorunlu hale gelecektir.

Dijital ticaretin sürekliliği açısından verinin sınır ötesi akışı kaçınılmazdır. Ancak bu akışın ortak güven ve normlara dayalı olarak gerçekleşmesi hedeflenmektedir. 2019 G20 Osaka Zirvesi'nde geliştirilen "Data Free Flow with Trust (DFFT)" ilkesi, bu yaklaşımın temelini oluşturmuş; Japonya ve AB, bu ilkenin öncülüğünü üstlenmiştir. Gelecekte ortak güvenlik ve etik standartlarla desteklenen, şeffaf ve güvenilir bir veri paylaşım düzeninin inşası öngörülmektedir (G20, 2019; WTO, 2021).

Parçalı ve çelişkili ulusal veri politikaları yerine, daha bütüncül ve kapsayıcı bir sistem talebi de küresel ölçekte artmaktadır. Bu doğrultuda, Birleşmiş Milletler "Küresel Dijital Pakt (Global Digital Compact)" oluşturma yönünde çalışmalar başlatmıştır. Paktın amacı; mahremiyet, güvenlik, erişim, şeffaflık ve dijital haklar ekseninde evrensel normlar geliştirmektir. Gelecekte küresel bir veri yönetim mimarisi oluşturma çabalarının ivme kazanması beklenmektedir. Zira devletlerin yalnız başına veri güvenliğini sağlaması güç görünmektedir. Bu nedenle teknoloji şirketleri, dijital platformlar ve devletler arasında daha sistematik iş birlikleri geliştirilmektedir. Örneğin, Microsoft, AWS ve Google gibi şirketler devletlerle siber tehdit istihbaratı paylaşmakta; Apple ile AB ise kullanıcı mahremiyetine yönelik standartların belirlenmesi konusunda ortak çalışmalar yürütmektedir.

Önümüzdeki dönemde, platform ekonomisinin kamu yararına uygun şekilde yeniden düzenlenmesi beklenmektedir. Veri üzerinden oluşan ekonomik değerin kullanıcılar arasında nasıl paylaşılacağı, önemli ve güncel bir tartışma alanıdır. Kullanıcı verileri üzerinden elde edilen reklam, analiz ve modelleme gelirlerine ilişkin mülkiyet ve gelir paylaşımı talepleri artmaktadır. Bu bağlamda, blockchain tabanlı sistemler ve "veri cüzdanı" gibi teknolojilerle bireylerin kendi verileri üzerindeki kontrolünü artıracı modeller gündeme gelmektedir. Bu gelişmelere paralel olarak "veri hakkı" ve "veri geliri" gibi kavramların hukuk sistemlerine entegre edilmesi de olasıdır (Posner & Weyl, 2018).

Verinin Geleceği Nereye Gidiyor?

Veri politikaları günümüzde yalnızca teknolojik düzenleme alanı olmanın ötesine geçmiş; jeopolitik, ekonomik ve demokratik çıkarların kesiştiği stratejik bir zemine dönüşmüştür. Uluslararası düzeyde hâlen norm birliği sağlanamamışken, Avrupa Birliği hak temelli bir yaklaşımla küresel standartları belirlemeye çalışmakta; ABD serbest veri akışını savunmakta, Çin ise ulusal güvenliği önceliklendirmektedir. Gelişmekte olan ülkeler ise veri egemenliği ile dijital sömürüye karşı daha adil ve kapsayıcı bir sistem talep etmektedir. Bu bağlamda, uluslararası veri politikaları yalnızca mahremiyet, güvenlik ve egemenlik ekseninde değil; aynı zamanda adalet, eşitlik ve sürdürülebilir kalkınma açısından da belirleyici rol oynamaktadır. Önümüzdeki yıllarda, veriye erişim hakkı,

veriden fayda üretimi ve bu faydanın adil bölüşümü, yapay zekâ ile bütünleşik veri etiği, dijital altyapıların güvenliği ve küresel yönetim mimarileri gibi konular, veri politikalarının temel yapıtaşlarını oluşturacaktır (European Commission, 2021; Taylor, 2017).

5.3. Dijital Egemenlik

21. yüzyılda devlet egemenliği yalnızca fiziksel topraklar üzerinde değil; veri, dijital altyapı, algoritmalar ve çevrimiçi platformlar üzerinden de şekillenmektedir. Bu yeni güç alanı, "dijital egemenlik" (digital sovereignty) kavramı altında tanımlanmaktadır. Geleneksel egemenlik, devletlerin kendi sınırları içinde mutlak karar verme yetkisini ifade ederken, dijital çağda bu yetki; siber uzay, veri akışları, teknolojik altyapılar ve küresel dijital platformlar aracılığıyla sınır ötesine taşmıştır. Devletler yaşanan değişim karşısında egemenlik anlayışlarını dijital alana doğru genişletmek zorunda kalmıştır (Nye, 2010; Fidler, 2016).

Dijital egemenlik, bir devletin veya siyasi otoritenin, veri yönetimi, dijital altyapılar ve bilgi akışı üzerinde kendi hukuk sistemi ve ilkeleri doğrultusunda denetim kurabilmesini ifade eder (Floridi, 2020). Bu kavram, devletlerin dijital dünyadaki varlığını, kontrolünü ve politik reflekslerini belirleyen yeni nesil egemenlik biçimidir. Ancak bu güç inşası, bireysel hakları, küresel iş birliğini ve teknolojik gelişimi engellemeden, adalet temelli bir dijital yönetim yaklaşımıyla gerçekleştirilmelidir. Gelecekte dijital egemenlik yalnızca bir güç aracı değil; aynı zamanda kapsayıcı, güvenli ve hak temelli dijital dönüşümün dayanak noktası hâline gelmelidir.

Bölgesel Yaklaşımlar ve Politikalar

Dijital egemenlik, dünya genelinde farklı bölgesel yaklaşımlar doğrultusunda şekillenmektedir. Avrupa Birliği, bu kavramı "Brüksel Etkisi" çerçevesinde değerlendirerek temel haklar ve veri güvenliği odaklı bir yapı geliştirmektedir. GDPR ve Yapay Zekâ Yasası gibi düzenlemelerle küresel ölçekte standartlar belirlenmektedir (Bradford, 2020). Ayrıca, "European Data Strategy" kapsamında geliştirilen Gaia-X gibi projelerle Avrupa merkezli dijital altyapılar teşvik edilmektedir (European Commission, 2020).

Çin'de ise dijital egemenlik, devlet kontrolü ve siber egemenlik ekseninde anayasal düzeyde tanımlanmış ve "Great Firewall" ile Veri Güvenliği Yasası (Data Security Law, 2021) aracılığıyla uygulamaya konulmuştur. Bu yapı hem içerik denetimini hem de sınır ötesi veri akışını sıkı biçimde düzenlemektedir. Ayrıca TikTok, Alibaba ve Huawei gibi şirketlerin uluslararası faaliyetleri de devletin denetimi altında yürütülmektedir (Creemers, 2017).

ABD ise dijital dünyaya daha serbest bir yaklaşım sergilemekte ve dijital egemenlik kavramını çoğu zaman serbest veri akışını kısıtlayan bir unsur olarak görmektedir. Ancak son yıllarda siber güvenlik kaygıları ve Çin merkezli dijital tehditler nedeniyle, ABD’de de dijital otonomi tartışmaları önem kazanmıştır. 2018 tarihli Cloud Act, ABD hükümetinin yurt dışındaki veriler üzerinde de yetki kurmasına olanak tanımaktadır (Kerry, 2019).

Afrika, Latin Amerika ve Güney Asya’da ise dijital egemenlik kavramı, veri sömürgeciliğine karşı direnç göstermek amacıyla kullanılmakta ve bu bölgelerde “veri adaleti” ile “dijital haklar” söylemleri ön plana çıkmaktadır (Couldry & Mejias, 2019).

Uygulama Alanları ve Stratejik Yönelimler

Günümüzde Google, Microsoft ve Amazon gibi şirketler, küresel ölçekte bulut hizmetleri üzerinde tekel oluşturmuş durumdadır. Buna karşılık, devletler yerli bulut sistemleri geliştirerek dijital egemenliklerini pekiştirmeye çalışmaktadır. Gaia-X (AB), Yandex Cloud (Rusya) ve Baidu Cloud (Çin) bu yöndeki stratejik adımlardır.

Öte yandan, Huawei, Ericsson ve Nokia gibi firmaların 5G altyapılarındaki rolü, ulusal güvenlik sorunu hâline gelmiştir. ABD ve Avrupa Birliği, güvenlik gerekçeleriyle Huawei’nin 5G altyapılarından dışlanmasını savunmaktadır (Lee, 2019).

Tartışmalar ve Eleştiriler

Veri, dijital çağda artık yalnızca “yeni petrol” değil; aynı zamanda “yeni toprak” olarak tanımlanmakta ve egemenlik tartışmalarının merkezine yerleşmektedir. Çin ve Rusya gibi ülkelerin dijital egemenlik adı altında ifade özgürlüğünü sınırlandırması, bu kavramın otoriter uygulamalarla özdeşleşmesine neden olmaktadır (Feldstein, 2021).

Küresel internetin parçalanarak çok merkezli bir yapıya, yani “Splinternet”e dönüşmesi, dijital dünyanın evrensel yapısını tehdit etmektedir. Gelecekte kamu-özel iş birlikleriyle dijital egemenliğin daha kapsayıcı, şeffaf ve adaletli şekilde yeniden tanımlanması kaçınılmaz görünmektedir. Bu kapsamda, Birleşmiş Milletler tarafından önerilen “Küresel Dijital Pakt” gibi girişimlerin yanı sıra, yapay zekâ ve veri etiğine yönelik küresel regülasyonların da dijital egemenlik tartışmalarının merkezine yerleşmesi beklenmektedir.

6. MODERN EMPERYALİZM ÇAĞINDA DİJİTAL SÖMÜRÜ DÜZENİ

21. yüzyılın dijital kapitalizmi; veri mülkiyeti, küresel teknoloji tekelleri ve dijital eşitsizlikler üzerinden şekillenen yeni bir güç yapılanmasını ifade etmektedir. Sanayi çağında emperyalizm, fiziksel kaynak ve emek sömürsüne dayanırken dijital çağda veri, dikkat, algoritmik işleme ve dijital emek, yeni sömürü alanları haline gelmiştir. Dijital sömürgecilik yalnızca ekonomik değil; aynı zamanda kültürel ve siyasal düzeyde yeni bağımlılık ilişkileri üretmektedir.

Bu bölümde, dijital teknolojilerin uluslararası düzeyde nasıl asimetrik, bağımlılık içeren ve sömürüye dayalı ilişkiler ürettiği; platform kapitalizmi, veri kolonizasyonu ve dijital egemenlik ekseninde tartışılacaktır. Küresel teknoloji tekellerinin gelişmekte olan ülkeler üzerindeki etkileri ile dijital yurttaşlık kavramı bağlamında modern emperyalizmin nasıl yeniden kurulduğu, uluslararası ilişkiler ve küresel ekonomi çerçevesinde analiz edilecektir.

Klasik emperyalizm, Batılı devletlerin ekonomik, askerî ve kültürel olarak çevre ülkeleri kontrol altına almasıyla tanımlanırken (Lenin, 1916); günümüzde bu kontrol dijital teknolojiler ve veri üzerinden sağlanmaktadır. “Artık zenginlik yeraltından değil, buluttan çıkarılıyor.” (Morozov, akt. Couldry & Mejias, 2019). Dijital emperyalizm, gelişmiş ülkelerde merkezlenmiş büyük teknoloji şirketlerinin; gelişmekte olan ülkelerin veri kaynaklarını, dijital altyapılarını ve bilişsel emeklerini yönlendirmesi ve kontrol altına alması sürecidir (Couldry & Mejias, 2019). Klasik dönemde gücün temel araçları askerî üstünlük ve doğal kaynak kontrolü iken; modern dönemde bu rolü dijital şirketler, veri merkezleri ve algoritmalar üstlenmektedir. Veri, günümüzde hem yeni bir sermaye biçimi hem de güç politikalarının temel malzemesi hâline gelmiştir. “Veri, dijital çağın petrolüdür ama aynı zamanda toprak gibidir: Üzerinde yaşanır, kontrol edilir ve işgal edilir” (Couldry & Mejias, 2019).

İlgili Kavramlar

Veri Sömürgeciliği: Verinin üretildiği ülkeden çıkarılarak merkez ülkelere taşınması ve burada ekonomik değere dönüştürülmesidir.

Algoritmik Tahakküm: Küresel dijital platformların, bireylerin davranışlarını yönlendiren kararlar alarak toplumsal yapılar üzerinde kontrol kurmasıdır.

Platform Kapitalizmi: Ekonomik ilişkilerin dijital platformlar aracılığıyla kâr odaklı şekilde yeniden yapılandırılmasıdır.

Dijital Emek: Kullanıcıların dijital platformlarda geçirdiği zaman, dikkat ve ürettikleri içeriklerin ekonomik kaynak olarak değerlendirilmesidir (Zuboff, 2019; Srnicek, 2017).

6.1. Dijital Sömürünün Mekanizmaları

▪ Veri Kolonizasyonu

Veri kolonizasyonu bireylerin, toplumların ve kurumların ürettiği verilerin; bu verileri işleyebilecek kapasiteye ve teknolojiye sahip olmayan ülkelere veya bölgelerden toplanarak, küresel teknoloji tekelleri aracılığıyla merkez ülkelere aktarılması ve veriler üzerinden ekonomik, kültürel ya da siyasal üstünlük sağlanması sürecidir. Bu kavram, 19. yüzyılın klasik sömürgecilik pratiklerinin dijital çağdaki karşılığı olarak değerlendirilmektedir.

Toplanan veriler çoğunlukla ABD ve Avrupa merkezli sunucularda depolanmakta; verinin üretildiği ülkeler ise veri mülkiyeti, algoritmik denetim ya da fayda paylaşımı konusunda söz sahibi olamamaktadır. Örneğin, Facebook'un "Free Basics" projesi, kullanıcıya ücretsiz internet erişimi sağlamaktadır; ancak bu erişim yalnızca Facebook ürünleriyle sınırlıdır. Bu sayede milyonlarca kullanıcının verisi ABD merkezli sunuculara aktarılmakta ve küresel ölçekte yeniden işlenmektedir (Birhane, 2021).

▪ Bulut Bilişim ve Teknolojik Bağımlılık

Dijital çağda veri altyapıları, fiziksel donanım ve yerel sunuculardan bulut tabanlı sistemlere kaymıştır. Microsoft Azure, Amazon AWS ve Google Cloud gibi platformlar, dünya genelinde dijital altyapının %70'inden fazlasını kontrol etmektedir. Bu geçiş, teknik kolaylık ve ölçeklenebilirlik gibi avantajlar sunsa da özellikle gelişmekte olan ülkeler açısından siyasi, ekonomik ve stratejik düzeyde yeni bağımlılık ilişkileri oluşturmaktadır.

Bu durum, "teknoloji bağımlılığı" kavramı çerçevesinde, dijital egemenlik tartışmalarını gündeme getirmektedir. Gelişmekte olan ülkeler, kendi devlet verilerini ve ulusal dijital altyapılarını küresel bulut hizmetlerinde barındırmak zorunda kalmakta, böylece veri üzerinde denetim ve güvenlikten yoksun hâle gelmektedir (Internet Society, 2020).

▪ Dijital Emek ve Dikkat Ekonomisi

Dijital çağda bireyler, sosyal medya kullanırken, içerik üretirken ya da yalnızca dijital ortamda vakit geçirirken görünmeyen ancak ekonomik olarak yüksek değere sahip bir emek üretmektedir. Kullanıcılar, platformlar üzerinde geçirdikleri zaman ve dikkatleri

karşılığında doğrudan bir ekonomik getiri elde etmemektedir. Ancak bu katkı, şirketler tarafından reklam ve veri ekonomisine (dikkat ekonomisi) dönüştürülmektedir.

Dikkat ekonomisinde temel kaynak, kullanıcıların dikkat süresi ve etkileşim düzeyidir. Veri bir ham madde olarak değerlendirilirken; dikkat, dijital çağın enerji kaynağıdır. Üretilen içerikler, algoritmalar aracılığıyla analiz edilerek YouTube, TikTok ve Facebook gibi platformlarda şirketlerin reklam gelirine dönüştürülmektedir (Terranova, 2000). Davenport ve Beck'e (2001) göre, dikkat çekmek artık doğrudan gelir oluşturmaktadır: "Daha fazla dikkat, daha fazla reklam geliri demektir."

▪ Kültürel Homojenleşme ve Anlatı Sömürüsü

Küresel dijital platformlar yalnızca veri değil, aynı zamanda dil, davranış biçimleri, değer sistemleri ve kültürel pratikleri de tek tipleştirilmektedir. Netflix, YouTube ve Instagram gibi platformlar, küresel kültürel anlatıları merkezileştirmekte ve içerik üretimini büyük ölçüde merkez ülkelerin değer yargıları doğrultusunda filtrelemektedir. Bu süreçte yerel anlatılar küresel standartlara uyum sağlamak zorunda bırakılmakta; böylece kültürel çeşitlilik ve özgünlük gerilemektedir (Chakravartty & Zhao, 2008).

Kültürel hegemonyaya karşı mücadele etmek için çeşitli stratejiler geliştirilebilir. Yerel dil, gelenek ve estetik öğeleri koruyan dijital içerik üretimi teşvik edilmeli; küresel platformlara karşı yerel video, blog ve sosyal medya ağları desteklenmelidir. Ayrıca, kültürel anlatının sahibine ait olduğu anlayışını temel alan yeni telif hakkı modelleri geliştirilerek, Netflix ve Spotify gibi platformların kültürel telif sorumluluğu üstlenmeleri zorunlu hâle getirilebilir.

6.2. Dijital Sömürüye Direniş ve Alternatifler

Dijital sömürüye karşı direnmek ve alternatif yollar inşa etmek ekonomik, teknolojik, hukuki ve kültürel düzlemlerde çok katmanlı bir mücadeleyi gerektirmektedir. Dijital kapitalizm çağında veri, dikkat, anlatı ve kültürel üretim; bireylerin gönüllü veya farkında olmadan sundukları katkılar üzerinden ekonomik değere dönüştürülmektedir. Bu süreç, kullanıcıların rızası dışında gerçekleşen dijital sömürü pratikleri doğurmakta ve dijital ortamda yeni bir tahakküm biçimi oluşturmaktadır (Zuboff, 2019).

Bu bağlamda, dijital sömürüye karşı bireysel ve kolektif düzeyde direnç stratejilerinin geliştirilmesi zorunludur. Alternatif platformlar, açık kaynak yazılımlar, şeffaf algoritmalar ve veri mülkiyetini kullanıcıya iade eden teknolojik çözümler direnişin temel araçları

olabilir. Aynı zamanda dijital okuryazarlık düzeyinin artırılması ve farkındalık kampanyaları ile kullanıcıların dijital haklarını savunmaları teşvik edilmelidir (Mozilla Foundation, 2023).

Tablo 6: Dijital Sömürüye Direniş Alanları: Bireysel Düzeyde

Strateji	Açıklama
Dijital farkındalık geliştirme	Kişisel verilerin ne şekilde toplandığını ve kullanıldığını sorgulama.
Dijital minimalizm	Gereksiz bildirimleri kapatma, çevrim içi geçirilen zamanı sınırlama ve dijital platform kullanımını azaltma.
Alternatif uygulamalar	Küresel teknoloji firmaları yerine, yerli ve bağımsız geliştiriciler tarafından sunulan uygulamaların tercih edilmesi.
Veri haklarını talep etme	GDPR ve benzeri düzenlemeler kapsamında kişisel veriler üzerinde erişim, silme ve kısıtlama gibi yasal hakların kullanılması.
Dijital detox	Platform bağımlılığından kurtulmak amacıyla dijital molalar verme veya bireysel/toplumsal detoks hareketlerine katılma.
Slow Tech hareketi	Tüketim ve dikkat sömürsüne karşı yavaş,sade ve bilinçli teknoloji kullanımını savunan alternatif bir yaşam tarzı benimseme

Tablo 7: Dijital Sömürüye Direniş Alanları: Toplumsal Düzeyde

Strateji	Açıklama
Dijital kooperatiflerin kurulması	Kullanıcıların sahip olduğu ve yönettiği sosyal medya ya da içerik paylaşım platformlarının geliştirilmesi (örnek: Mastodon, Resonate).
Toplum tabanlı veri yönetimi	Verilerin anonimleştirilerek kamu yararına açık veri olarak paylaşılması ve yönetilmesi (örnek: Data Trusts modelleri).
Dijital dayanışma ağları	Dijital haklar konusunda bilgilendirme yapan, platform kapitalizmine karşı kolektif mücadeleyi destekleyen sivil ağların kurulması (örnek: Tactical Tech, Access Now).

Dijital kooperatifler, kullanıcıların yalnızca “tüketici” değil, aynı zamanda üretici, ortak ve hak sahibi olarak yer aldığı platform modelleridir. Bu yapılar, dijital emeğin adil paylaşımı ve platform sahipliğinin demokratikleştirilmesi yönünde önemli bir alternatifi temsil etmektedir. Örneğin, Mastodon merkeziyetsiz bir sosyal medya ağı iken, Resonate kullanıcıya ait ve gelir paylaşımı ilkesine dayanan bir müzik platformudur. Benzer şekilde, PeerTube, YouTube’a alternatif olarak geliştirilen dağıtık bir video ağıdır. Bu tür platformlarda veri hem güvenli şekilde korunmakta hem de kamu ya da akademi gibi yetkilendirilmiş aktörler tarafından toplumsal fayda doğrultusunda kullanılabilir (Scholz, 2016; Fuchs, 2014).

Yerli sosyal ağlar, mesajlaşma uygulamaları, kamuya ait bulut sistemleri (örneğin Fransa'nın "Bleu" projesi) ve kullanıcı merkezli açık kaynaklı çözümler, dijital verinin kolektif biçimde sahiplenilmesi ve yönetilmesi için geliştirilen modeller arasında yer almaktadır. Linux, Mastodon ve Diaspora gibi platformlar, küresel dijital devlere karşı geliştirilen katılımcı ve şeffaf teknolojik altyapılardır.

Ayrıca, kullanıcının kaynak kodunu inceleyebildiği ve değiştirebildiği açık kaynak yazılımlar da büyük teknoloji firmalarının sunduğu hizmetlere alternatif oluşturmaktadır. Örneğin, Firefox internet tarayıcısı, NextCloud bulut teknolojisi, Mastodon sosyal medya ağı ve Jitsi video konferans uygulaması başlıca örnekler arasındadır. Bu tür araçlar, dijital alanda hem mahremiyetin hem de kolektif üretimin desteklenmesine olanak tanımaktadır.

Tablo 8: Dijital Sömürüye Direniş Alanları: Politik ve Hukuki Düzeyde

Strateji	Açıklama
Veri egemenliği yasaları / Veri yerelleştirme	Verilerin yerel sunucularda tutulmasını zorunlu kılan düzenlemeler. Örnek ülkeler: Hindistan, Çin.
Veri adaleti çerçeveleri	Veriye erişim, mülkiyet ve dağıtımda toplumsal adaleti esas alan yasal çerçeveler.
Kâr paylaşımı modelleri	Kullanıcı katkısıyla oluşan gelirin paylaşımına dayalı sistemler (platform kooperatifçiliği)
Teknoloji tekellerine karşı rekabet hukuku	Büyük dijital platformlara karşı devlet müdahaleleri. Örnek: Avrupa Birliği'nin Google ve Meta'ya yönelik cezaları.
Dijital hak bildirgeleri	İfade özgürlüğü, veri mülkiyeti, algoritmik şeffaflık, unutulma hakkı gibi dijital hakların tanınması. Örnek inisiyatifler: Access Now, EDRI, Electronic Frontier Foundation.

Küresel ölçekte yürütülen dijital haklar hareketleri kapsamında, Privacy International, Access Now, AlgorithmWatch gibi sivil toplum inisiyatifleri öne çıkmaktadır. Ayrıca, Afrika Birliği'nin Malabo Sözleşmesi ile Latin Amerika'da dijital hak temelli anayasal düzenlemelere yönelik girişimler (örneğin Şili, 2022) bu alandaki önemli örnekler arasında yer almaktadır.

6.3. Sonuç: Dijital Emperyalizme Karşı Yeni Bir Dayanışma

Modern emperyalizm artık tanklarla değil; sunucular, algoritmalar ve dijital bağımlılık ilişkileri aracılığıyla işlemektedir. Dijital sömürgecilik, bireyleri ve toplumları ekonomik ve kültürel düzeyde bağımlı hâle getiren çok katmanlı bir yapı olarak karşımıza çıkmaktadır. Söz konusu yeni sömürü biçimi yalnızca ekonomik değil; aynı zamanda kültürel, siyasal ve

etik boyutlarıyla da ele alınması gereken bir meseledir. Bu yapıya karşı geliştirilecek direnç, yalnızca düzenleyici politikalarla sınırlı kalmamalı; dijital adalet, dijital haklar ve dijital özgürlük ilkeleri doğrultusunda küresel düzeyde bir dayanışma ve farkındalık çerçevesinde inşa edilmelidir.

Alternatif dijital modellerin geliştirilmesi, sadece devlet politikalarının değil; aynı zamanda sivil toplumun, bağımsız teknoloji geliştiricilerin ve kullanıcı topluluklarının aktif katkısını gerektirmektedir. Dijital sömürüye karşı direnç, sadece platform değişikliğiyle sınırlı kalmamalı; bunun ötesinde, etik, adil ve kolektif dijital yaşam biçimlerinin inşasını da içermelidir. Hem bireysel hem de kolektif düzeyde, veri mülkiyetinden kültürel anlatı hakkına kadar uzanan bu mücadelede temel ilke ise şu şekilde ifade edilebilir: "Katıldığımız dijital sistemlerin yalnızca kullanıcısı değil, aynı zamanda sahibi ve şekillendiricisi de olmalıyız."

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

7. TEKNOFEODALİZM

Teknofeodalizm, dijital çağda ortaya çıktığı ileri sürülen ve teknoloji şirketlerinin ekonomik, politik ve sosyal yaşam üzerindeki gücünü Orta Çağ Avrupa'sında yaşanan feodal düzene benzeten bir kavramdır. Bu kavrama göre günümüzde, büyük teknoloji şirketleri (ör. platform devleri, bulut altyapı sağlayıcıları, yapay zekâ devleri) modern ekonomide bir tür “dijital derebeyi” gibi davranarak veri üzerinde mülkiyet kurmakta, kullanıcıları ve işletmeleri ise “dijital serf” konumuna getirmektedir. Bu yaklaşıma göre, kapitalizm yeni bir evreye girmiştir ve artık klasik rekabet, piyasa ilişkileri veya endüstriyel üretim mantığıyla değil; platforma bağımlılık, veri mülkiyeti ve algoritmik tahakküm üzerinden işlemektedir.

7.1. Orta Çağ Avrupa'sıyla Günümüz Dijital Ortamındaki Benzerlikler

- a) Mülkiyet ve erişim ilişkileri: Feodal dönemde toprak derebeyinin mülküydü; köylüler sadece kullanırdı. Teknofeodalizmde ise, veri, kullanıcı ağları ve dijital altyapı büyük platformların mülkü olarak görülmektedir; kullanıcılar bu altyapılara erişmek zorundadır ama mülkiyet hakkına sahip değildirler.
- b) Bağımlılık ilişkileri: Orta Çağ Avrupa'sında, serfler toprağı terk edemezdi; geçim kaynakları derebeyine bağılıydı. Günümüzde ise işletmeler ve bireyler bulut sistemlerine, uygulama mağazalarına, dijital reklam altyapısına, sosyal medya algoritmalarına ve yapay zekâ modellerine bağımlı hâle gelmiştir.
- c) Harçlar ve rantsal gelirler: Orta Çağ Avrupa'sında, feodal beyler doğrudan üretime katılmadan rant toplardı. Teknofeodalizmde ise platform şirketleri benzer şekilde yine üretime katılmadan komisyon, reklam payı, veri rantı, abonelik kilidi gibi yöntemlerle gelir elde etmektedir.

7.2. Teknofeodalizmi Ortaya Çıkaran Dinamikler

Günümüzde hangi faktörler dijital ortamda, Orta çağ Avrupa'sına benzer bir yapıya dönüşümüne neden olmuştur?

- a) Aşırı odaklı platformlaşma: Google, Apple, Meta, Amazon, Tencent gibi devler kritik dijital altyapıları kontrol etmekte ve dijital pazarın kapı bekçisi gibi hareket etmektedirler. Bu nedenle, dijital ortamdan faydalanmak veya iş yapmak isteyenler bu şirketlerin koyduğu kurallara uymak zorunda kalmaktadır.

b) Veri tekelleri: Dijital platformlar kullanıcıların bilgilerini kendi bünyesinde toplamakta ve bunların başkaları tarafından kullanılmasını kısıtlamaktadırlar. Kullanıcı davranışları, işletmelerin ticari faaliyetleri, lokasyon, sağlık, tüketim vb. bilgiler devasa kapalı veri merkezlerinde toplanmakta ve dışa erişimi engellenmektedir.

c) Algoritmik yönetim: Orta çağda derebeyleri hükmü altındakilerinin yaşamlarına ilişkin birçok konuda karar verirdi. Benzer şekilde günümüzde de algoritmalar kullanıcıların ne tür deneyim yaşayacaklarına karar vermektedir. Görünmez ama güçlü bir yönetim mekanizması olan algoritmalar, kullanıcıların ne göreceğini ne satın alacağını, kime ulaşabileceğini ve işletmelerin kimlere önerileceği gibi hususlarda belirleyici olmaktadır.

d) Yapay zekâ ve otomasyon: Yapay zekânın hem altyapısının hem eğitimi için gerekli veri ve hesaplama gücü büyük teknoloji devlerinde olduğundan bu durum kale sahibi derebeylerin güç toplamasına benzer şekilde güç yoğunlaşmasına neden olmaktadır.

7.3. Günlük Yaşamda Teknofeodalizmin Etkileri

Günlük hayatta teknofeodalizm bireyler, şirketler ve toplum nezdinde farklı etkilere neden olmaktadır. Bu sistemde bireyler, sürekli gözetim altındadır, bu bireylerin dijital kimlik ve davranışları birer meta hâline gelmiştir, ayrıca bu platformlardan ayrılmakta zorlaşmıştır. İşletmeler ise, reklam algoritmalarına bağımlılık, bulut hizmetlerine geçiş maliyetleri ve erişim ve görünürlük için platformlara “haraç” öder gibi ödeme yapma nedenleriyle bu platformlara bağımlı hale gelmiştir. Genel olarak toplum ise, topluma bilgi akışının birkaç şirket tarafından kontrol edilmesi, sosyal olaylarda algoritmik manipülasyona açık hâle gelmesi ve ekonomik değer üretiminin giderek merkezileşmesi ve tekel haline gelmesi şeklinde etkiye maruz kalmaktadır.

Sonuç olarak gelecekte, teknofeodalizmin platform hegemonyasını daha da artırması, ya da devletlerin ve regülasyonların güçlenerek platform gücünü sınırlaması, diğer bir alternatif olarak da dağıtık teknolojilerin (blokzincir, açık kaynak, yerelleştirilmiş yapay zekâ) yükselerek merkezi gücü kırması beklenmektedir.

7.4. Teknofeodalizmin Türkiye’deki Durumu

Bu başlıkta, teknofeodalizmin Türkiye bağlamında nasıl somutlaştığına dair örnek olaylar, gözlemlenebilir olgular üzerinden sistematik biçimde aktarılmaktadır. Bunlar kavramın Türkiye’deki pratik karşılıklarını anlamaya yöneliktir; yorumsaldır, hukuksal bir değerlendirme değildir.

Teknofeodalizmin Türkiye’de birçok alanda etkisi görülmektedir.

1. E-ticaret Platformlarına Bağımlılık: Günümüzde küçük işletmeler ticaretlerinin önemli bir kısmını birkaç büyük dijital platformlar üzerinden yapmaktadır. Bu işletmeler, görünürlük ve satış hacmi için zorunlu biçimde bu platformlara girmek ve onları belirlediği kurallara göre hareket etmek zorundadır. Bu platformlardan dönen ticarete komisyon oranları, reklam maliyetleri ve algoritmik sıralama kriterleri tek taraflı belirlenmektedir. Platformlar “pazar yeri” olmaktan çok -altyapısının sahibi ve erişim kapısını kontrol eden aktör- haline gelmiştir. Esnaf ve KOBİ’ler, ticaretlerini platformun kurallarına bağlı olarak sürdürebilmekte, bu platformlardan ayrılmaları ise ekonomik olarak mümkün görünmemektedir.

2. Yemek ve Kurye Ekonomisi: Günümüzde büyük bir sektör haline gelen dijital alışveriş ve buna bağlı olarak kuryelerin çalışma koşulları algoritmalar tarafından belirlenmektedir; sipariş dağılımı, performans ölçümü, yoğunluk primleri tamamen platformun veri modeline bağlıdır. Müşteri değerlendirmeleri ve sistem içi puanlama, kurye gelirleri üzerinde doğrudan etkilidir. Bu nedenle, çalışanlar fiziksel emeklerini dijital platformun veriye dayalı yönetimi altında gerçekleştirmekte, gelir, zaman ve rota kontrolü insan yöneticiden çok algoritma tarafından sağlanmakta, feodal sistemdeki “toprağa bağlılık”, burada “uygulama ekosistemine bağlanma” olarak yaşanmaktadır.

3. Uygulama Mağazası Bağımlılığı: Türkiye’de mobil oyun ve uygulama sektörünün büyük bölümü iki mağazaya bağımlıdır. Bu platformlara uygulama/oyun geliştiren üreticilerin gelirlerinin önemli kısmı platform komisyonları nedeniyle kesilmektedir. Fiyatlandırma, vergi yönetimi, kullanıcıya erişim kanalları mağazaların kurallarına göre şekillenmektedir. Bu nedenle dijital ürün üreticisi, pazarı kontrol eden platform sahibine ekonomik “pay” ödemediği var olamamaktadır. Bu nedenle, platformun denetim gücü, feodal beylerin ekonomik rantsal kontrolüne benzemektedir.

4. Sosyal Medya Ekonomisi: Sosyal medyaya içerik üreticilerinin gelirleri tamamen algoritmik öneri sistemlerine bağlıdır. Hesap düşüşleri, görünürlük kaybı, içerik kaldırma gibi olaylar ekonomik faaliyetleri doğrudan etkilemektedir. Bu platformlarda şeffaf karar mekanizması yoktur; algoritma hem “yol” hem “otorite” olarak işlev görmektedir. Kullanıcının üretimi (video, fotoğraf, etkileşim) platformun mülkü olan veri havuzuna akmakta, üretici kendi kitlesine erişmek için platformun kontrolünün onayına ihtiyaç duymaktadır.

5. Dijital Reklam Piyasası: Türk KOBİ ve girişimlerinin dijital müşteri kazanımında belirli arama motorları ve dijital platformlar neredeyse vazgeçilmezdir. Ancak buralardaki reklam optimizasyonu ve hedefleme tamamen kapalı algoritmalara dayanmaktadır, alternatif kanallar sınırlıdır. Reklam verenler efektif erişim için platforma “haraç benzeri” sürekli ödeme yapmaktadır. Reklam piyasasının veri tekelleri tarafından yönetilmesi, ekonominin görünmez bir şekilde merkezileşmesine yol açmaktadır.

6. Bulut Hizmeti Bağımlılığı: Büyük Türk şirketleri ve ölçeklenen startuplar genellikle küresel bulut altyapılarına bağımlıdır. Bu altyapıdan çıkış (vendor lock-in) hem teknik hem mali olarak zorlayıcıdır. Dijital altyapının mülkiyeti girişimlerde değil, küresel platformlarda toplanmaktadır. Yerli verinin saklandığı altyapının mülkiyetine “dijital toprak” benzetmesi yapılabilir.

7. Bankacılık ve Fintek Ekosisteminde Platformlaşma: Türkiye’de ödeme sistemleri ve dijital bankacılık çerçevesi düzenlenmiş olsa da büyük bankalar ve birkaç ödeme platformu sektöre yüksek giriş bariyerleri oluşturmaktadır. Kullanıcı davranışları, kredi skorlama sistemleri, dijital cüzdan ve QR altyapıları bu platformların merkezi veri havuzlarında birikmektedir. Bu havuzlarda finansal davranışa dair kapsamlı veri platformlarda kilitlenir; yeni aktörlerin rekabeti kısıtlanmaktadır. Algoritmik kredi değerlendirmesi, bireylerin ve şirketlerin ekonomik katılımı üzerinde “yönetimsel güç” edinmesini sağlamaktadır.

Sonuç olarak, Türkiye bağlamında teknofeodalizm üç ekseninde yoğunlaşmaktadır:

1. Pazarın platform merkezli örgütlenmesi,
2. KOBİ, esnaf ve çalışanların algoritmik ekosistemlere bağımlı hale gelmesi,
3. Veri ve dijital altyapı mülkiyetinin aşırı merkezileşmesi.

Bu yapı, üretim ve dağıtımın karar merkezinin ekonomik aktörlerin elinden çıkıp dijital altyapı sahiplerine kayması nedeniyle teknofeodalizmin temelini oluşturmaktadır.

8. TÜRKİYE'DE VERİ KAPİTALİZMİ VE DİJİTAL SÖMÜRÜYLE MÜCADELE

Veri kapitalizmi ve dijital sömürüyle mücadele, Türkiye özelinde hem hukuki ve kurumsal düzeyde hem de sivil toplum, birey ve teknoloji geliştiricileri düzeyinde çok boyutlu olarak ele alınmalıdır. Bu çerçevede atılacak ilk adım, veri kapitalizminin Türkiye'deki durumunun kapsamlı biçimde tespit edilmesidir.

Türkiye'de dijital ekonomi hızla büyürken, veri kapitalizminin en yaygın biçimleri aşağıdaki alanlarda gözlemlenmektedir:

Tablo 9: Türkiye'de Veri Kapitalizminin Görünümleri

Alan	Sömürü Biçimi
Sosyal medya (Instagram, TikTok)	Kullanıcı verilerinin sürekli gözetimi ve bu verilerin hedefli reklam yoluyla ticarileştirilmesi.
E-ticaret (Trendyol, Hepsiburada)	Alışveriş alışkanlıklarının algoritmalarla analiz edilerek manipülatif tekliflere dönüştürülmesi.
Mobil uygulamalar	Konum, ses ve kullanıcı davranışlarına dair verilerin sistematik olarak toplanması.
Eğitim & sağlık sistemleri	Kamusal sistemlerde toplanan verilerin ileride ticari amaçlarla kullanılması riskinin bulunması.

(Kaynak: KVKK Raporları, TÜBİTAK BİLGEM – Dijital Güvenlik Araştırmaları, Global Voices (2022). Türkiye'de Dijital Hakların Durumu)

Türkiye'de dijital platformlar aracılığıyla vatandaşların izleme ve tıklama verilerinin yanı sıra konum, ses, davranış ve alışkanlıklarına ilişkin veriler sistematik biçimde toplanmakta, analiz edilmekte ve bu veriler üzerinden tüketici davranışları şekillendirilerek kişiselleştirilmiş ürün ve hizmetler, reklamlar yoluyla kullanıcılara yönlendirilmektedir.

8.1. Türkiye'de Veri Kapitalizminin Temel Boyutları

– Gözetim Mekanizmaları

Türkiye'de en yaygın kullanılan mobil uygulamalar ve e-ticaret platformları (Trendyol, Getir, Yemeksepeti, Sahibinden gibi) kullanıcıların konum, tercih, tıklama ve kategori tarama verilerini yoğun bir şekilde toplamaktadır. Çoğu uygulama, KVKK'ya uyumlu görünse de açık rıza kavramı kullanıcılar tarafından bilinçli şekilde kullanılmamaktadır. Örneğin, Trendyol'un uygulama açılış süresi esnasında kullanıcı davranışlarını 100 milisaniye düzeyinde analiz ettiği belgelenmiştir (KVKK Denetim Raporları, 2022).

– Algoritmik Yönlendirme ve Karar Etkisi

Türkiye'de bireylerin satın alma, haber alma ve oy verme davranışları algoritmalar aracılığıyla şekillendirilebilir hale gelmiştir. Aşağıdaki tabloda, e-ticaret, haber ve sosyal

medya algoritmalarının kişisel veriler doğrultusunda nasıl yapılandırıldığına ilişkin örnekler sunulmaktadır. Kişisel tercihlere göre belirlenen ürün ve hizmetler, bireylerin satın alma süreçleri ve kararları üzerinde önemli bir etkiye sahiptir.

Tablo 10: Algoritmik Yönlendirme

Platform	Veri Kapitalizmi Pratiği
Trendyol, Hepsiburada	Satın alma geçmişine dayalı kişiselleştirilmiş fiyat önerileri.
Instagram, TikTok	Kullanıcıların dikkat süresine göre içerik ve reklam manipülasyonu.
Google News & yerel haber portalları	Politik eğilime göre haber sıralaması ve filtreleme.

(Kaynak: Oxford Internet Institute (2021). Information Disorder in the Middle East Alternatif Bilişim Derneği (2023). Algoritmik Tarafsızlık Raporu)

– **Kişisel Verilerin Korunmasındaki Zafiyetler**

Türkiye’de KVKK aktif olmakla birlikte denetim mekanizmaları sınırlı kalmaktadır. 6698 sayılı KVKK Kanunu, Avrupa Birliği’nin GDPR düzenlemesine kıyasla veri taşınabilirliği, unutulma hakkı ve algoritmik şeffaflık gibi alanlarda yetersizdir. Bu durum, veri mülkiyetinin kullanıcıya ait görünmesine rağmen, pratikte şirketlerin veri üzerinde tam kontrol sahibi olmasına yol açmaktadır (Koç Üniversitesi Hukuk Fakültesi, 2022; Privacy Turkey, 2023).

– **Ekonomik Değerin Platformlarda Yoğunlaşması**

Platform ekonomisi, veriyi merkezileştirerek önemli gelir kaynakları sağlamaktadır:

Tablo 11: Ekonomik Değerin Platformlarda Yoğunlaşması

Örnek	Veri Kapitalizmi Sonucu
Trendyol	Kullanıcı verilerinden davranışsal reklam geliri üretir.
Meta & Google	Türkiye’de reklam pastasının %70’inden fazlasını kontrol eder.
Yemeksepeti	Restoranlara algoritmik sıralamayla müşteri yönlendirir.
E-Nabız	Sağlık verileri merkezi olarak toplanır; şeffaflık geliştirilmelidir.

(Kaynak: İAB Türkiye, Dijital Reklam Gelirleri Raporu (2023))

Sonuç olarak, 2023 yılında Türkiye dijital reklam pazarının %80’i yabancı platformlar tarafından domine edilmiştir.

8.2. Türkiye'nin Veri Kaynakları Üzerinden Sömürülme Riskleri

Türkiye, hem ekonomik olarak gelişmekte olan bir ülke hem de dijital dönüşüm sürecinde büyük veri üreten bir toplum olarak, veri sömürüsüne karşı “veri kolonisi” olma riski taşımaktadır (Couldry & Mejias, 2019).

Dijital Sömürgecilik Belirtileri:

- Kullanıcı verileri yurtdışına aktarılmakta ve veriden doğan ekonomik değer Türkiye içinde kalmamaktadır.
- Veri analitiği ve yapay zekâ sistemleri çoğunlukla yabancı şirketler (örneğin Amazon, Meta) tarafından geliştirilmektedir.
- Kültürel anlatılar ise uluslararası dijital medya platformları tarafından ticarileştirilmektedir.

Bu hususlar, Türkiye'nin dijital ekonomide karşı karşıya olduğu fırsatlar kadar önemli risklerin de altını çizmektedir (Couldry & Mejias, 2019; TÜSİAD, 2022).

8.3. Türkiye’de Veri Kapitalizmine Dair Güncel Gelişmeler

Tablo 12: Veri Kapitalizmine Dair Gelişmeler

Gelişme	Açıklama
KVKK-GDPR uyum çalışmaları	2024'te daha güçlü veri hakları için yeni yasa taslağı hazırlanmıştır.
Yerli sosyal medya girişimleri	Eksi10, Gain, X gibi platformlarla veri bağımsızlığı artmaktadır.
Yerli Bulut Projeleri	Türk Telekom, Havelsan ve Türksat tarafından “Türkiye’ye özel” bulut çalışmaları yapılmaktadır.
Açık veri ve yapay zekâ politikaları	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi – “Veri Kümeleri Stratejisi” (2023)

Sonuç olarak, Türkiye veri kapitalizminin hem üreticisi (kullanıcı verisi sağlayan) hem de tüketicisi (yabancı platformları kullanan) konumundadır. Ancak yasal eksiklikler, yerli alternatiflerin sınırlılığı ve dijital hak farkındalığının düşük olması gibi nedenlerle, veriden doğan katma değer büyük ölçüde yurt dışına akmakta ve Türkiye, gözetim sistemleri içinde pasif bir veri kaynağına dönüşmektedir.

Türkiye’de Dijital Sömürüye Karşı Atılabilecek Adımlar

Türkiye’de dijital sömürüye karşı atılabilecek adımlar, hukuki, kurumsal, toplumsal, teknolojik ve kültürel olmak üzere çok boyutlu bir yaklaşımla ele alınmalıdır.

8.4. Yasal ve Kurumsal Reformlar

– KVKK Reformu ve GDPR Uyumlaştırması

Mevcut durumda, KVKK (6698 Sayılı Kanun) Avrupa Birliği’nin GDPR’sine kıyasla veri taşınabilirliği, profil oluşturma kısıtı ve otomatik karar süreçlerine itiraz hakkı gibi alanlarda eksiklikler içermektedir. Bu nedenle, KVKK güncellenmeli; “unutulma hakkı”, “veri taşınabilirliği” ve “açık algoritma” gibi hükümler eklenmelidir. Ayrıca, veri işleyen tüm firmalar için şeffaflık raporları zorunlu tutulmalı, bağımsız denetim mekanizmaları güçlendirilmelidir. Veri Koruma Etki Değerlendirme Raporlarının (DPIA) hazırlanması zorunlu hale getirilmelidir (Koç Üniversitesi, 2022; KVKK, 2023; European Data Protection Board, 2023).

– Rekabet Kurumu ve BDDK’nın Rolü

Büyük teknoloji firmalarının reklam ve veri tekeli oluşturarak rekabeti bozması hem kullanıcıları hem de küçük işletmeleri mağdur etmektedir. Google, Meta ve TikTok gibi şirketler, Türkiye’deki dijital reklam pazarının %70’inden fazlasını kontrol etmektedir. Bu nedenle, Rekabet Kurumu dijital platformlara özel rekabet yasaları geliştirmeli (AB’nin DMA yasasına benzer şekilde), dijital piyasalarda bağımsız denetimler yürütmeli ve Fintech şirketleri için veri güvenliği ile açıklık zorunlulukları getirmelidir. Ayrıca, kullanıcıya yönelik algoritmalarla şeffaflık ve denetlenebilirlik ilkeleri getirilmeli; “veriye dayalı tekel” oluşturan yerli ve yabancı şirketlere karşı müdahale mekanizmaları kurulmalıdır (Rekabet Kurumu, 2022; BDDK, 2023; European Commission, 2022).

– Sivil Toplum ve Dijital Hak Hareketleri

Türkiye’de halkın büyük çoğunluğu veri hakları, platform manipülasyonları ve mahremiyet araçları konusunda bilinçsizdir. Bu nedenle, Milli Eğitim müfredatına dijital vatandaşlık ve veri hakları dersleri eklenmeli; belediyeler ve halk eğitim merkezlerinde dijital mahremiyet atölyeleri düzenlenmeli, “Veri Haftası” ve “Şeffaflık Festivali” gibi kamusal etkinlikler desteklenmelidir (Alternatif Bilişim Derneği, 2023).

– Sivil Toplum ve Veri Kooperatifleri

“Veri kooperatifi” modeli ile bireylere verileri üzerinde kolektif kontrol hakkı sağlanabilmektedir. Scholz’un (2016) önerdiği platform kooperatifçiliği yaklaşımı,

Türkiye’de de desteklenmeli; yerel kooperatif uygulamaları için TÜBİTAK ve KOSGEB aracılığıyla teşvik mekanizmaları oluşturulmalıdır (Scholz, 2016; UNCTAD, 2021).

– **Teknolojik Alternatifler**

Türkiye’nin veri kapitalizmine dayalı dijital sömürüye karşı direnç gösterebilmesi için dijital platformlara yönelik yerli ve açık kaynak alternatiflerin geliştirilmesi ve desteklenmesi büyük önem taşımaktadır. Bu doğrultuda, çeşitli uygulama alanlarına yönelik önerilen alternatifler aşağıdaki tabloda sunulmuştur.

Tablo 13: Dijital Platformların Yerli ve Açık Kaynak Alternatifleri

Uygulama Alanı	Önerilen Alternatif
E-posta	TÜBİTAK KAMU-SM altyapısı, ProtonMail’in Türkiye’ye uyarlanmış versiyonları.
Bulut	Nextcloud tabanlı yerli TRCloud çözümleri.
Mesajlaşma	Signal ve Matrix altyapılı yerli mesajlaşma uygulamaları.
Video Konferans	Jitsi tabanlı kamu destekli video iletişim sistemleri.
İşletim Sistemi	Pardus işletim sistemi, açık kaynak yazılımlara yönelik kamu teşvikleri.

Alternatif dijital ürünlerin yaygınlaştırılabilmesi için kamu kurumlarında açık kaynak yazılımlara geçiş zorunlu hâle getirilmelidir. Açık kaynak geliştiricilerine doğrudan fon sağlanmalı ve dijital girişimcileri desteklemek amacıyla bir “Dijital Egemenlik Fonu” oluşturulmalıdır. Bununla birlikte, üniversitelerde dijital kooperatif temelli girişimler teşvik edilmeli; e-Devlet hizmetlerinin veri güvenliği denetimleri daha şeffaf ve hesap verebilir bir yapıya kavuşturulmalıdır (TÜBİTAK, 2021–2024; Bilgi Üniversitesi, 2021).

– **Dijital Hak Savunuculuğu**

Türkiye’de dijital haklar alanında faaliyet gösteren sınırlı sayıda sivil toplum kuruluşu (STK) bulunmaktadır. Bu alandaki STK sayısı artırılmalı, mevcut STK’ların dijital okuryazarlık ve farkındalık eğitimleri kamusal düzeyde desteklenmelidir. Ayrıca, üniversitelerde veri etiği ve dijital vatandaşlık dersleri açılarak bireylerin dijital haklarını tanımaları ve bu hakları nasıl savunabileceklerini öğrenmeleri sağlanmalıdır.

Tablo 14: Dijital Hak Savunuculuğu

STK/İnisiyatif	Çalışma Alanı
Alternatif Bilişim Derneği	Dijital mahremiyet, ifade özgürlüğü.
Özgür Yazılım Derneği	Açık kaynak yazılımlar, kullanıcı haklarının korunması.
Yeşil Düşünce Derneği	Dijital adalet, iklim krizi ile ilişkili dijital politikalar.
Privacy Türkiye	Gizlilik ve gözetim karşıtı mücadele.

– **Kültürel ve Anlatı Egemenliği**

Türkiye'nin kültürel değerleri, Netflix, YouTube, TikTok gibi küresel platformlarda ticarileştirilmekte ve yerel bağlamından koparak yok olmaya yüz tutmaktadır. Bu nedenle, kültürel içeriklerin platform sömürüsüne karşı korunması zorunludur. Netflix ve TikTok gibi platformlarda yerel kültürün “klişeleştirilmesi” yerine otantik anlatıların muhafazası önem taşımaktadır. Bunun için, TRT 2, Gain, BluTV gibi yerli dijital medya platformlarına telifli kültürel destek sağlanmalı; kültürel içerik üreticilerine “anlatı hakkı” çerçevesinde koruma ve temsil güvencesi verilmelidir. Ayrıca, halk anlatılarını arşivleyen dijital kütüphaneler oluşturulmalı, dijital kültür arşivleri ve anlatı mülkiyeti yasaları düzenlenmeli, telifli halk hikâyeleri ile dijital folklor içerikleri için sivil toplum kuruluşları desteklenmeli ve yerli içerik üreticileri teşvik edilmelidir (UNESCO, 2021; Kültür ve Turizm Bakanlığı, 2024; TRT Akademi).

8.5. Uluslararası İş Birlikleri

Türkiye, veri kapitalizmine karşı mücadelede uluslararası iş birliklerini de güçlendirmelidir. Uluslararası Veri Adaleti Konsorsiyumu (Global Data Justice) gibi küresel girişimlere katılım sağlanmalı; OECD, G20 ve Birleşmiş Milletler'in dijital ekonomi düzenleme ilkeleriyle uyumlu stratejiler geliştirilmelidir. Ayrıca veri egemenliği için bölgesel dijital iş birliklerinin oluşturulması önem arz etmektedir (UNCTAD, 2022).

8.6. Türkiye İçin Dijital Egemenlik ve Direniş Yol Haritası

Dijital bağımsızlık, yalnızca teknoloji üretmekle değil; veriyi, anlatıyı ve kültürü kimin kontrol ettiğine karar vermekle ilgilidir. Türkiye'nin dijital sömürünün üç temel boyutuna — veri, dikkat ve anlatı — karşı mücadelesi aşağıdaki ana başlıklar altında özetlenebilir:

- Hukuki ve kurumsal güçlendirme (KVKK reformu, dijital rekabet yasası),
- Sivil toplum mobilizasyonu,

- Teknolojik alternatiflerin, özellikle açık kaynak ve yerli teknolojilerin teşviki,
- Kültürel egemenlik ve anlatı koruması,
- Dijital okuryazarlık toplumsallaştırılması,
- Veri kooperatifçiliği ve anlatı hakları güvence altına alınması
- Uluslararası veri politikalarında etkin rol üstlenilmesi.

Hukuki ve politik reformlar kapsamında, KVKK'da GDPR düzeyinde bir reform yapılmalı; kullanıcılara veri taşınabilirliği, algoritmik şeffaflık ve unutulma hakkı sağlanmalıdır. Ayrıca Dijital Rekabet Yasası hızlıca yürürlüğe konarak, veri temelli tekellere müdahale edilip dijital ortamda adil rekabet sağlanmalıdır. Kamusal yazılımlarda açık veri ve açık kaynak kullanımı yaygınlaştırılarak, şeffaflık ve güvenlik artırılmalıdır. Dijital Egemenlik Ulusal Politikası oluşturularak siber güvenlik, yerli yazılım ve veri politikaları bütüncül şekilde yönetilmelidir.

Teknolojik altyapı açısından, yerli bulut bilişim altyapısı kurulmalı, devlet ve özel sektör iş birliğiyle TRCloud ve veri merkezleri hayata geçirilmelidir. Rusya'daki Yandex benzeri, etik, kapsayıcı ve reklam bağımlısı olmayan yerli arama motorları ve sosyal ağlar geliştirilmelidir. Üniversiteler ve kamu kurumlarında zorunlu açık kaynak dönüşüm programları uygulanmalıdır. Ayrıca yerli yapay zekâ ve veri etiketleme altyapıları desteklenmelidir.

Toplumsal alanda ise ilkokuldan başlayarak veri hakları, algoritmik farkındalık ve bireysel mahremiyet odaklı dijital okuryazarlık eğitimleri verilmelidir. Bireylerin verilerini kolektif olarak yönettiği veri kooperatifleri teşvik edilmelidir. Yerli Uber, Hepsiburada gibi alternatif platformlara fon sağlanmalı, ulusal dijital medya ekosistemi oluşturularak telif hakları ve anlatı gücü korunmalı; böylece medya ve kültürel egemenlik sağlanmalıdır.

Uluslararası düzeyde ise veri adaleti konsorsiyumları kurulmalı, UNCTAD, OECD ve G20 gibi platformlarda adil veri paylaşımı için talepler sunulmalıdır. Türk Devletleri Teşkilatı ve İslam İşbirliği Teşkilatı gibi bölgesel yapılarla ortak dijital altyapılar geliştirilmeli; Avrupa ile veri geçişinde eşitlik temelli anlaşmalar yapılmalı ve dijital göç ile haklar güvence altına alınmalıdır.

Dijital sömürüye karşı bu tedbirler zaman çizelgesine oturtulmalıdır:

- **Kısa vadede (0–2 yıl):** KVKK güncellemesi, dijital okuryazarlık eğitimleri ve açık kaynak dönüşüm programı tamamlanmalıdır.
- **Orta vadede (2–5 yıl):** Yerli bulut ve veri merkezleri, platform kooperatifleri ve yerli yapay zekâ destekleri hayata geçirilmelidir.
- **Uzun vadede (5 yıl ve sonrası):** Uluslararası veri diplomasisi kurulmalı, kültürel anlatı altyapıları tamamlanmalı ve kapsamlı dijital anayasa ile dijital vatandaşlık sistemleri oluşturulmalıdır.

Bu rapor KOSAM tarafından
özel olarak hazırlanmıştır.
www.kosam.org

KAYNAKÇA

- Aaronson, S. A. (2018). Data is different: Why the world needs a new approach to governing cross-border data flows (CIGI Papers No. 197). Centre for International Governance Innovation. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/>
- Aaronson, S. A. (2021). The geopolitics of data. Centre for International Governance Innovation. <https://www.cigionline.org>
- African Union. (2022). AU data policy framework. <https://au.int/en/documents/20221024/data-policy-framework>
- Alternatif Bilişim Derneği. (t.y.). *Dijital Haklar Manifestosu*.
- Alternatif Bilişim Derneği. (2023). *Dijital haklar eğitimi modülü*. <https://alternatifbilisim.org.tr/>
- Alliance for Affordable Internet (A4AI). (2022). *Affordability report 2022*. <https://a4ai.org/affordability-report/>
- BDDK. (2023). *Fintek mevzuat raporları*. Bankacılık Düzenleme ve Denetleme Kurumu. <https://www.bddk.org.tr/>
- Birhane, A. (2021). Algorithmic colonization of Africa. *Real Life Magazine*. <https://reallifemag.com/algorithmic-colonization-of-africa/>
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Chakravartty, P., & Zhao, Y. (2008). *Global communications: Toward a transcultural political economy*. Rowman & Littlefield.
- Council of Europe. (1950). *European convention on human rights*. <https://www.echr.coe.int/>
- Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, 26(103), 85–100.
- Davenport, T. H., & Beck, J. C. (2001). *The attention economy: Understanding the new currency of business*. Harvard Business School Press.
- De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. <https://doi.org/10.1016/j.clsr.2016.02.006>

- EFF. (2023). *Tech lobbying and regulation reports*. <https://www.eff.org/issues/tech-lobbying>
- European Commission. (2020a). *Shaping Europe's digital future*. <https://digital-strategy.ec.europa.eu/en/library/shaping-europes-digital-future>
- European Commission. (2020b). *A European strategy for data*. https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf
- European Commission. (2021a). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- European Commission. (2021b). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
- European Commission. (2022). *The Digital Markets Act (DMA)*. https://ec.europa.eu/info/business-economy-euro/competition/digital-markets-act_en
- European Data Protection Board. (2023). *Annual Report 2022*. <https://edpb.europa.eu>
- European Parliament, Directorate General for Parliamentary Research Services. (2021). *Online platforms: economic and societal effects*. LU: Publications Office.
- European Union. (2015). Regulation (EU) 2015/2120 of the European Parliament and of the Council. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
- European Union. (2018a). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Union. (2018b). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

- Evans, D. S., & Schmalensee, R. L. (2016). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press.
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
- Fidler, D. (2016). Sovereignty and the Internet. Indiana University Center for Applied Cybersecurity Research.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2718779
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369–376.
<https://doi.org/10.1007/s13347-020-00423-6>
- Fuchs, C. (2014). *Digital labour and Karl Marx*. Routledge.
- G20. (2019). G20 Osaka Leaders' Declaration.
<https://www.mofa.go.jp/files/000486486.pdf>
- Greenleaf, G. (2018). Global data privacy laws 2017: 120 national laws and still counting. *Privacy Laws & Business International Report*, (151), 10–13.
- Grey, M. L., & Suri, S. (2019). *Ghost work: How to stop Silicon Valley from building a new global underclass*. Houghton Mifflin Harcourt.
- Interpol. (2023). *Interpol Annual Cybercrime Report 2023*.
<https://www.interpol.int/en/Crimes/Cybercrime>
- Internet Society. (2020). *Global Internet report: Consolidation in the Internet economy*.
<https://www.internetsociety.org/globalinternetreport/>
- Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3), 61–69.
- Koç Üniversitesi Hukuk Fakültesi. (2022). *KVKK ve GDPR karşılaştırmalı analiz raporu*. Koç Üniversitesi Yayınları.
- Kerry, C. (2019). Why the U.S. needs digital sovereignty, too. *Brookings Institution*.
<https://www.brookings.edu/articles/why-the-u-s-needs-digital-sovereignty-too/>
- Kişisel Verileri Koruma Kurumu (KVKK). (2016). *Kişisel verilerin korunması kanunu (KVKK)*.
<https://www.kvkk.gov.tr>
- Kişisel Verileri Koruma Kurumu (KVKK). (2023). *Faaliyet raporu 2023*.
<https://www.kvkk.gov.tr>
- Lee, T. B. (2019). The global battle over 5G network security. *Ars Technica*.
<https://arstechnica.com/tech-policy/2019/05/the-global-battle-over-5g-network-security/>
- Lenin, V. I. (1916). *Imperialism: The highest stage of capitalism*. Progress Publishers.

- Liu, H. (2021). China's Personal Information Protection Law: A comparative perspective. *Computer Law & Security Review*, 41, 105535. <https://doi.org/10.1016/j.clsr.2021.105535>
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
- Meta. (2023). *Annual report 2023*. <https://investor.fb.com>
- Mozilla Foundation. (2023). *Internet Health Report*. <https://internethealthreport.org/2023/>
- Morozov, E. (2015, June 1). Where Uber and Amazon rule: Welcome to the world of platform. *The Guardian*.
- Morozov, E. (2016, December 3). Data populists must seize our information for the benefit of us all. *The Guardian*. <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/cyber-power>
- OECD. (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>
- OECD. (2019a). *Open government data report: Enhancing policy maturity for sustainable impact*. OECD Publishing. <https://doi.org/10.1787/888933969482>
- OECD. (2019b). *PISA 2018 results (Volume I): What students know and can do*. OECD Publishing. <https://doi.org/10.1787/5f07c754-en>
- OECD. (2021). *Addressing the tax challenges of the digital economy*. Organisation for Economic Co-operation and Development. <https://www.oecd.org/tax/beps/>
- OECD. (2023). *Digital sovereignty & governance*.
- Oxfam. (2022). *Inequality kills*. <https://www.oxfam.org.uk/>
- OpenSecrets.org. (2023). *Big Tech lobbying data*. Center for Responsive Politics. <https://www.opensecrets.org/lobby/indus.php?id=F04>
- Organisation for Economic Co-operation and Development (OECD). (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

- Organisation for Economic Co-operation and Development (OECD). (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Posner, E. A., & Weyl, E. G. (2018). *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton University Press.
- Rekabet Kurumu. (2022). *Dijital piyasalar raporu*. <https://www.rekabet.gov.tr>
- Rekabet Kurumu. (2022). *Dijital Rekabet ve Platform Ekonomileri Raporu*. <https://www.rekabet.gov.tr>
- Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). *General Data Protection Regulation (GDPR)*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Scholz, T. (2016). *Platform cooperativism: Challenging the corporate sharing economy*. Rosa Luxemburg Stiftung.
- Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYU Law Review*, 86(6), 1814–1894.
- Shaughnessy, H. (2015). *Shift: A leader's guide to the platform economy*.
- Srnicek, N. (2016). *Platform capitalism*. Polity Press.
- Srnicek, N. (2017). *Platform capitalism*. Polity Press.
- Star, S. L., & Strauss, A. (1999). Layers of silence, arenas of voice: The ecology of visible and invisible work. *Computer Supported Cooperative Work*, 8(1), 9–30.
- Statista. (2024). Most valuable companies worldwide in 2024. <https://www.statista.com>
- Taylor, L. (2017). What is data justice? *Big Data & Society*, 4(2), 1–14. <https://doi.org/10.1177/2053951717736335>
- Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text*, 18(2), 33–58. https://doi.org/10.1215/01642472-18-2_63-33
- TRT Akademi. (t.y.). *Dijital kültür ve anlatılar üzerine*. [Erişim bilgisi yok]
- TÜBİTAK. (2022). *Ulusal yapay zeka stratejisi*.
- UN CTAD. (2021). *Digital economy report 2021: Cross-border data flows and development – For whom the data flow*. United Nations Conference on Trade and Development. <https://unctad.org/webflyer/digital-economy-report-2021>
- UN CTAD. (2022). *Data Governance & Digital Sovereignty Report*. Birleşmiş Milletler Ticaret ve Kalkınma Konferansı. https://unctad.org/system/files/official-document/dtlstict2022d4_en.pdf
- UNESCO. (2021a). *Universal Declaration on Ethics of Information and Digital Rights*. United Nations Educational, Scientific and Cultural Organization. <https://unesdoc.unesco.org/ark:/48223/pf0000379940.locale=en>

- UNESCO. (2021b). *Dijital kültürel ifade çeşitliliği raporu*. Paris: UNESCO.
- United Nations. (1948). *Universal Declaration of Human Rights*.
<https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- United Nations. (2019). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.
<https://undocs.org/A/74/486>
- United Nations Office on Drugs and Crime (UNODC). (2024). *Cybercrime Repository*.
<https://www.unodc.org/unodc/en/cybercrime/index.html>
- UNICEF, & ITU. (2020). How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic.
<https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/>
- Van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, 36, 105377. <https://doi.org/10.1016/j.clsr.2019.105377>
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ipx005>
- World Trade Organization (WTO). (2020). *E-commerce and cross-border data flows*.
https://www.wto.org/english/res_e/publications_e/dataflows2020_e.htm
- World Trade Organization (WTO). (2021). *World Trade Organization and e-commerce*.
https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
- World Bank. (2021). *Digital development overview*.
<https://www.worldbank.org/en/topic/digitaldevelopment/overview>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.