

Dijital Kolonyalizm ve Kişisel Veri Hakları: Medya Emperyalizmi Çerçevesinde GDPR ile KVKK'nın Karşılaştırmalı Analizi

Digital Colonialism and Personal Data Rights: A Comparative Analysis of the GDPR and the KVKK within the Framework of Media Imperialism

Nurdan Akıner, Prof. Dr., Akdeniz Üniversitesi İletişim Fakültesi,

E-posta: nurdanakiner@akdeniz.edu.tr,

ORCID ID: 0000-0003-0295-9373

Ayşe Arat, Doç. Dr., Akdeniz Üniversitesi Hukuk Fakültesi,

E-posta: aysearat@akdeniz.edu.tr,

ORCID ID: 0000-0001-8261-4302

Araştırma Makalesi/Research Article

Öz

Dijital kolonyalizm, bireylerin kişisel verilerinin büyük teknoloji şirketleri tarafından sömürülmesine yol açmaktadır. Özel hukuk açısından, kişisel verilerin korunmasına dair düzenlemeler çoğu zaman yetersiz kalmaktadır. GDPR (General Data Protection Regulation) Türkçe adıyla Genel Veri Koruma Tüzüğü, Avrupa Birliği tarafından bireylerin kişisel verilerinin korunması ve bu verilerin işlenmesine ilişkin kuralları getiren bir yasal düzenlemedir. 27 Nisan 2016'da kabul edilmiş ve 25 Mayıs 2018'de yürürlüğe girmiştir. GDPR, Avrupa Birliği (AB) vatandaşlarının kişisel verilerinin toplanması, depolanması, işlenmesi ve paylaşılması süreçlerinde şeffaflık, hesap verebilirlik ve güvenlik sağlamayı amaçlar. GDPR, kişisel verilerin korunmasına yönelik küresel bir standart haline gelmiştir. Bireylerin haklarını güçlendirirken, şirketlerin veri işleme süreçlerinde şeffaf davranmalarını ve işlemlerinden sorumlu olmalarını sağlar. Bu düzenleme, dijital çağda veri güvenliği ve gizliliği açısından önemli bir dönüm noktasıdır. AB'de GDPR, bireylere kişisel verileri üzerinde bilgi edinme hakkı, erişim hakkı, düzeltme hakkı, silinme hakkı (unutulma hakkı), veri taşınabilirliği hakkı, itiraz hakkı ve otomatik karar almaya itiraz hakkı gibi geniş haklar tanımaktadır. Türkiye'de kişisel verilerin korunması, Kişisel Verilerin Korunması Kanunu (KVKK) ile düzenlenmiştir. Ancak KVKK, GDPR ile benzer ilkeler içerse de GDPR kadar kapsamlı değildir. Türkiye'de faaliyet gösteren ve AB vatandaşlarının verilerini işleyen şirketler hem KVKK hem de GDPR'a uyum sağlamak zorundadır. Ancak GDPR, medya emperyalizminin neden olduğu ve gücü gün geçtikçe artan dijital kolonyalizm tarafından uluslararası boyutta sıklıkla ihlal edilmektedir. En bilindik örneklerden biri de Facebook'un Cambridge Analytica skandalıdır. Facebook kullanıcılarının verileri, izinleri olmadan siyasi reklamlar için kullanılmıştır. Dijital ekosistemin büyük teknoloji şirketleri (big tech companies) tarafından kontrol edilmesi, onlara platform temelli deneyimler üzerinde doğrudan güç vermekte ve emperyal bir kontrol biçimi olarak değerlendirilebilecek siyasi, ekonomik ve kültürel yaşam alanları üzerinde etki sahibi olmalarını sağlamaktadır. Klasik çağın sömürgecilğinde olduğu gibi, emperyalist güçler verinin hammaddesine el koymakta, onu işlemekte ve küresel bir hizmete dönüştürerek hakimiyetlerini pekiştirmekte ve diğerlerini kendilerine tabi kılmaktadır. Hükümetler ve teknoloji şirketleri, gözetim kapitalizminin merkezi olan büyük veriyi kontrol eden ABD'li büyük teknoloji şirketlerinin mevcut küresel hakimiyet biçimini azaltacak stratejiler geliştirmek için iş birliği yapmalıdır. Dijital sömürgecilğe karşı bir çözüm önerisi olarak, teknolojiyi merkezileştiren bir dijital ekosistem modeli öne çıkmaktadır. Bu makale, dijital kolonyalizm ve medya emperyalizmi bağlamında bireysel hak ve özgürlüklerin erozyonunu özel hukuk perspektifinden analiz etmeyi ve çözüm önerileri sunmayı amaçlamaktadır.

Abstract

Digital colonialism is one of the biggest problems of data privacy. It describes the phenomenon of big tech companies systematically exploiting personal data. Within the context of private law, protective measures are often inadequate. One such attempt is the General Data Protection Regulation (GDPR) of the European Union, which seeks to protect and regulate the processing of personal data. It came into effect after adoption on April 27, 2016, with enforcement starting on May 25, 2018. The regulation aims to safeguard personal data of EU citizens by ensuring transparency, upholding jurisdictional accountability, and reinforcing the security framework relating to the gathering, storing, processing, and sharing of data. The passage of the GDPR has become achingly important in the world for personal information protection. Also, it makes sure that there is accountability and explanation in the data processing activities of the companies. Processing and safeguarding privacy of personal information is an important aspect that has greatly progressed in the modern world, especially in the digital realm. As part of the EU, the GDPR provides individuals several rights related to their personal data including the right of access, right to information, right of data rectification, erasure, data portability, objection and also to object to automated decision making. In Turkey, personal data protection is regulated by the Law on the Protection of Personal Data, or in short KVKK. Though the KVKK has some principles of GDPR, it is not as wide-ranging as the latter. Businesses in Turkey that process personal data of EU citizens are subject to the KVKK and also to GDPR compliance. Yet, an example of "digital colonialism," which turns violations of the law into a growing form of media imperialism, is Cambridge Analytica using Facebook's data without consent, yet with a premeditated strategic intent, gaining access and control of a resource without recognition of boundaries, be it ethical, legal, or geopolitical frameworks. We can witness the same kind of "digital neocolonialism". It is undeniable that the reach of social media and multi-functional platforms greatly transformed not just the scope of access to the digital real estate, but access to "tech powers" to the lives of people, but with a major unsettling impact. By conquering social media platforms and applying multi-functional tools, these powerhouses not only diversify their control and resources but also enable themselves to shape and manipulate politics, economy, and cultures globally. This shocking form of social control draws parallels to historical imperialism. This form of social control can be understood as a type of colonialism in which Big Tech corporations shape the lives of entire societies in line with their interests. Their intentions can be slowed down only if the people targeted realize their value and work with governments to combat these schemes. An answer to the problem of digital colonialism might be the construction of a digital ecosystem which embodies the decentralization of technology. This article intends to examine the erosion of rights and freedoms of the individual regarding digital colonialism and media imperialism from the angle of private law and attempts to offer suitable remedies.

Anahtar Kelimeler:

dijital kolonyalizm,
medya
emperyalizmi, büyük
teknoloji şirketleri,
GDPR, KVKK

Keywords:

digital colonialism,
media imperialism, big
tech companies, GDPR,
KVKK

Başvuru Tarihi: 15.08.2025

Yayına Kabul Tarihi: 28.04.2026

Akıner, N., & Arat, A. (2026). Dijital kolonyalizm ve kişisel veri hakları: Medya emperyalizmi çerçevesinde GDPR ile KVKK'nın karşılaştırmalı analizi. *Kastamonu İletişim Araştırmaları Dergisi (KİAD)*, (16), 40-54. DOI: 10.56676/kiad.1766008

Giriş

Dijitalleşen küresel ekonomide kişisel veriler yeni bir “sömürü nesnesi” haline gelmiş; devletler ve çok uluslu şirketler arasındaki güç mücadelesi, “data colonialism” (veri kolonyalizmi) olarak adlandırılan ve daha geniş anlamda dijital kolonyalizm tartışmaları içinde ele alınan yeni bir tahakküm biçimini ortaya çıkarmıştır (Couldry ve Mejias, 2019, s. 4-5). Bu süreç, özellikle kişisel veriler bağlamında, AB Genel Veri Koruma Tüzüğü (GDPR) ile Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) arasındaki düzenleyici farklılıklar üzerinden analiz edilmesi gereken karmaşık bir olgudur. Oliver Boyd-Barrett'in (2014) medya emperyalizmi teorisi çerçevesinde değerlendirildiğinde, GDPR aracılığıyla küresel veri koruma standartlarının dayatılması, AB'nin bir düzenleyici güç (regulatory power) haline gelmesini sağlamaktadır (Bradford, 2020, s. 6). Söz konusu düzenleyici tahakküm, Türkiye gibi çevre ülkeler açısından dijital bir bağımlılık sarmalı yaratmaktadır.

Bu çalışma, dijital kolonyalizmin kişisel veri hakları üzerindeki etkisini, GDPR ve KVKK'nın medya emperyalizmi bağlamında karşılaştırmalı analizi yoluyla incelemeyi amaçlamaktadır. Araştırmanın temel problemi, AB'nin norm ihracı (Kuner vd., 2020, s. 87) mekanizmalarının, Türkiye'nin veri egemenliği üzerinde yarattığı baskı ve bunun bireysel hakların erozyonu ile ilişkisidir. Çalışma, özellikle şu sorulara yanıt aramaktadır:

- *GDPR'ın "küresel standart" haline gelme süreci, medya emperyalizmi teorileriyle nasıl açıklanabilir?*
- *KVKK, GDPR karşısında bir "uyum" mu yoksa "direnc" mi sergilemektedir?*
- *Dijital kolonyalizm bağlamında, Türkiye'nin veri politikaları nasıl bir dönüşüm geçirmektedir?*

Çalışmanın kapsamı, AB-Türkiye odaklı olmakla birlikte, küresel veri politikalarına atıfla şekillendirilmiştir. Sınırlılıklar ise veri koruma rejimlerinin uygulanmasındaki yerel dinamikler (ör. Türkiye'deki idari kapasite) ve teknoloji şirketlerinin küresel etkileri ile sınırlıdır. Bu analiz, hukuki metinlerin karşılaştırmalı incelenmesi ve ikincil verilerin eleştirel okuması yoluyla gerçekleştirilmektedir. Bulgular, GDPR'ın medya emperyalizmi mekanizmaları aracılığıyla küresel veri hegemonyası kurduğunu; KVKK'nın ise bu hegemonya karşısında sınırlı bir direnc sergilediğini göstermektedir.

Kişisel Verilerin Korunması Kavramının Gelişimi

Kişisel veriden ne anlaşılması gerektiği konusunda doktrinde çeşitli tartışmalar bulunmakla birlikte GDPR ve KVKK bakımından şu tanımlamaların yapıldığı görülmektedir. GDPR'a göre kişisel veri, “belirli veya belirlenebilir bir gerçek kişiye (veri sahibi) ilişkin her türlü bilgi” anlamına gelmekte, belirlenebilir gerçek kişi ise “özellikle bir isim, bir kimlik numarası, konum verileri, bir çevrimiçi tanımlayıcı veya söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen kişiyi” ifade etmektedir (GDPR, 2016, m. 4/1). Kişisel Verilerin Korunması Kanunu'na göre kişisel veri, “kimliği belirli veya belirlenebilir

gerçek kişiye ilişkin her türlü bilgi”dir (KVKK, 2016, m. 3/d). Kanun gerekçesinde, bu kavramın yalnızca ad, soyad veya doğum tarihi gibi doğrudan kimliği belirleyen bilgilerle sınırlı olmadığı; bireyin fiziksel, ekonomik, sosyal, kültürel ve psikolojik özelliklerine ilişkin verileri de kapsadığı belirtilmektedir. Buna göre bir verinin kişisel veri sayılması için, mevcut bilgiler aracılığıyla bir gerçek kişiyle ilişkilendirilebilmesi ve kişiyi belirlenebilir hâle getirmesi yeterlidir. Dolayısıyla kimlik numarası, vergi numarası, sigorta bilgileri veya bireyin sosyal ve ekonomik kimliğini ortaya koyabilecek diğer veriler de kişisel veri kapsamında değerlendirilmektedir.

Kişisel verilerin önemi aslında çok eski zamanlara kadar uzanmaktadır. Antik uygarlıklardan beri insanlara ilişkin kayıtların tutulduğu görülmektedir. Başka insanlar hakkındaki bilgilere ihtiyaç, özellikle modern devlet anlayışı ile artmıştır. Zira devletler sağlık, eğitim, nüfus, güvenlik, vatandaşlık, yabancılık gibi unsurları tespit etmek, depolamak, planlama yapmak, yatırım yapmak, kaynak aktarmak ve politika oluşturmak için gözetim yöntemini kullanmakta, bilgi toplamakta ve bundan yararlanmaktadırlar (Şimşek, 2008, s. 3). İşletmeler açısından ise bu süreç verimliliği artırmak için çalışanlara yönelik olarak başlamış, ancak zaman içinde müşterileri izlemeye, onlara ilişkin bilgi toplamaya yönelik yöntemlere dönüşmüştür (Küzeci, 2023, s. 22). Bu verilerin sınırsız bir şekilde işlenmesi, kişilerin temel hak ve özgürlükleri bakımından birtakım sakıncaları da beraberinde getirmiştir. Zaman içinde günlük yaşantımızda önemsiz gördüğümüz hareketlerimiz, tercihlerimiz sayısal ortamda işlenerek, kişisel veya toplumsal olarak etkili sonuçlar doğurabilecek bir kaynağa dönüşmüştür (Küzeci, 2023, s. 27). Bu sebeple özellikle bilgisayarlar aracılığıyla kişisel bilgilerin kolay ve hızlı toplanması, birbiriyle ilişkilendirilmesi kişisel verilerin korunması ihtiyacını doğurmuştur.

Kişisel verilerin korunmasına yönelik ilk ulusal hukuki düzenlemeler, Avrupa’da 1970’li yıllarda yapılmaya başlanmıştır. Bunun ilk örnekleri, Hessen (Almanya) Veri Koruma Yasası (Hessische Datenschutzgesetz), Federal Almanya Veri Koruma Kanunu (Bundesdatenschutzgesetz), İsveç kişisel verileri kişisel düzeyde korumaya yönelik Veri Yasası (Datalag)dir. Bunları daha sonra Fransa, Danimarka, Norveç gibi ülkeler takip etmiştir. Benzer şekilde ABD’nde Gizlilik Kanunu (Privacy Act), İngiltere Veri Koruma Kanunu (Data Protection Act) ulusal düzenlemeler arasında sayılabilir. Bu durum Avrupa’nın yaşadığı iki dünya savaşının acı etkilerinin bir sonucudur. Özellikle insan hakları hukukunun uluslararası hale gelmesi, anayasa yargısının yaygınlaşması, bireyi devlet karşısında korumaya yönelik mekanizmalar oluşturmuştur. (Küzeci, 2023, s. 28-30). Bu çerçevede birinci kuşak veri koruma kanunları, bireyi devlet karşısında koruma, devlette toplanan bilgilerin birey aleyhine kullanılmasının önüne geçmeye odaklanmaktadır.

Uluslararası adımlar ise 1980’lerde atılmaya başlanmıştır. Bunlardan ilki OECD’nin yayınladığı, özel yaşamın gizliliğinin ve sınır ötesi kişisel veri dolaşımının korunmasına ilişkin rehber ilkelerdir (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) ki, tavsiye niteliğindeki bu rehber (Develioğlu, 2017, s. 7; Taştan, 2017, s. 10; Özkan, 2020, s. 37), sonraki düzenlemelerin de kaynağını oluşturmuştur (Küzeci, 2023, s. 30; Şimşek, 2008, s. 13).

Kişisel verilerin korunmasına yönelik uluslararası alandaki ilk bağlayıcı düzenleme (Küzeci, 2023, s. 35; Şimşek, 2008, s. 22; Kaya, 2020, s. 37) ise Avrupa Konseyi’nin 108

sayılı sözleşmesidir. “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin” bu sözleşme 1981 yılında imzaya açılmıştır. Ülkemiz de bu sözleşmeye ve buna ek olarak 2001 yılında çıkarılan protokole taraf olmuştur. 108 sayılı Sözleşme’de 2018 yılında değişiklikler yapılmış ve yeni hali ile 108+ Sözleşmesi olarak imzaya açılmıştır.

90’lı yılların başında BM’nin doğrudan kişisel verilerin korunmasına yönelik hukuki düzenlemesi, genel kurulda 14 Aralık 1990’da kabul edilen “BM Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri”dir (United Nations Guidelines Concerning Computerized Personal Data Files). Aynı yıllarda Avrupa Topluluğu’nda, topluluk düzeyinde kişisel verilerin korunmasına ilişkin bir direktif hazırlanması, iç hukuklar arasındaki farklılıkların giderilmesi düşüncesi ortaya çıkmıştır. Zira 108 sayılı Sözleşme bu uyumu sağlayamamıştır. Nihayet 24.10.1995 tarihinde 95/46/AT sayılı kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı konusunda bireylerin korunmasına ilişkin yönerge, (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) hem Avrupa hem de Avrupa dışında kişisel verilerin korunması alanında önemli ve etkili bir kaynak olmuştur. Bununla birlikte, yönergenin düzenlemeleri AB dışı ülkelere veri aktarımına yönelik yaklaşım, kendi sistemini dünyaya dayatma, ABD ile sanal ticarete yarışabilmek için zaman kazanma, serbest rekabet ortamını engelleme konularında eleştirilere maruz kalmıştır. Bu eleştirilere rağmen AB’nin kişisel verilerin korunmasına ilişkin getirdiği düzenlemeler, uluslararası alanda etkili bir model olmuştur (Küzeci, 2023, s. 47; Turan, 2019, s. 215). Ülkemizde 6698 sayılı KVKK, Yönerge ile uyumlu hükümler taşımaktadır.

25 Mayıs 2018’de, 95/46/AT sayılı Yönerge’nin yerini AB Genel Veri Koruma Tüzüğü (GDPR) almıştır. Üye ülkelerin tümü için birlik sağlamak amacıyla, bu yeni düzenleme Tüzük şeklinde hazırlanmış ve böylece üye ülkelerde doğrudan uygulama etkisi sağlanmıştır (Küzeci, 2023, s. 48; Özdemir, 2009, s. 29; Özer Deniz, 2022, s. 9; Özkan, 2020, s. 48). GDPR ile öncelikle yeknesak bir sistem kurulmuştur ve AB’de veri korumanın temel paradigması değiştirilmiştir. Veri sorumlusu ile veri işleyenin sorumlulukları, hesap verebilirlik, şeffaflık ve güvenlik ilkeleri çerçevesinde gözden geçirilmiştir. Privacy by design ve privacy by default kavramları ile yüksek koruma ilkeleri geliştirilmiş, veri koruma etki analizi düzenlenmiş, veri sahibinin hakları daha ayrıntılı ele alınmış, içtihat hukuku ile gelişen unutulma hakkı norm haline getirilmiş, veri taşınabilirliği hakkı tanınmış, profilleme açıkça düzenlenmiştir, yaptırım olarak ağırlaştırılmış para cezaları öngörülmüştür (Kaya, 2020, s. 39).

Ülkemizde konuya ilişkin ilk gelişme 2010 yılında yapılan Anayasa değişikliğidir. Bu değişiklik ile kişisel verilerin korunması temel bir hak olarak Anayasa’da güvence altına alınmıştır (T.C. Anayasası, 1982, m. 20/3). Sonraki süreçte dağınık şekilde farklı kanunlarla sağlanmaya çalışılan koruma, 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (KVKK) 24.03.2016 tarihinde kabul edilmesiyle bir kanuni düzenlemeye kavuşmuştur. Zira KVKK’dan önce kişisel verilerin işlenme şartları, hukuka uygunluğun sınırları gibi konularda tartışma ve çelişkili uygulamalar bulunmaktaydı. Aslında konuya ilişkin düzenlemelerin amacı kişisel verilerin işlenmesini yasaklamak değil, hukuka uygun biçimde düzenlemektir (Kaya, 2020, s. 40). KVKK bu anlamda ülkemiz için önemli bir adımdır. Bu kanun, 95/46/AT sayılı Yönerge esas alınarak hazırlanmıştır. Bu

sebeple düzenlemeler arasında genel ilkeler bakımından benzerlikler bulunmaktadır. Ancak 95/46 sayılı Yönerge mülga olmuştur. Onun yerine yürürlüğe giren 2016/679 sayılı Tüzük ise KVKK'nın uygulanması bakımından yol gösterici nitelikte kabul edilmektedir (Yücedağ, 2023, s. 138; Özkan, 2020, s. 50; Develioğlu, 2017, s. 16). Kişisel Verileri Koruma Kurulu kararlarında da bu hususa vurgu yapılmaktadır (2019/10 sayılı Karar).

Teorik Çerçeve: Yeni Bir Sömürü Biçimi Olarak Dijital Kolonyalizm

Dijital kolonyalizm, 21. yüzyılın küresel veri ekonomisinde ortaya çıkan yeni bir sömürü biçimi olarak tanımlanabilir. Bu kavram, geleneksel sömürgeciliğin dijital alana uyarlanmış halidir ve temelde teknoloji merkezli devletler ile çok uluslu şirketlerin, gelişmekte olan ülkelerin veri kaynakları, dijital altyapıları ve siber sınırları üzerinde kurduğu sistematik kontrol mekanizmalarını ifade eder. Geleneksel sömürgecilikten farklı olarak, bu modelde sömürülen kaynak petrol veya madenler değil, bireylerin kişisel verileri ve dijital emekleridir. Dijital kolonyalizm, Küresel Kuzey'in (Global North) teknoloji şirketlerinin, Küresel Güney'in (Global South) veri kaynaklarını kontrol altına alarak yeni bir emperyalizm biçimi oluşturduğu süreci tanımlar (Akıner, 2024, s. 133).

Bu teorik çerçeve, üç temel eksen üzerinden şekillenir: veri sömürüsü, teknolojik bağımlılık ve hukuki hegemonya. Veri sömürüsü, kullanıcıların sosyal medya platformlarında veya dijital servislerde ücretsiz olarak ürettikleri verilerin, büyük teknoloji şirketleri tarafından ticari bir meta olarak kullanılmasını ifade eder (Fuchs, 2021, s. 166). Örneğin, Facebook ve Google gibi platformlar, kullanıcı verilerini reklam gelirleri için işleyerek trilyon dolarlık değerler üretmektedir. Bu süreç, Scholz (2017, s. 112) tarafından "dijital kölelik" olarak eleştirilmiştir. Teknolojik bağımlılık ise, gelişmekte olan ülkelerin bulut bilişim, yapay zekâ ve veri depolama gibi kritik altyapılar için küresel teknoloji devlerine bağımlı hale gelmesini tanımlar (Sadowski, 2020, s. 43). Örneğin, Türkiye'deki birçok kamu kurumu ve özel şirket, veri depolama ve işleme hizmetleri için yabancı bulut sistemlerini kullanmak zorunda kalmaktadır (TÜİK, 2023).

Hukuki hegemonya boyutu ise dijital kolonyalizmin yasal ve düzenleyici araçlar üzerinden nasıl işlediğini ortaya koyar. Bu bağlamda, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), küresel veri koruma standartlarını belirleyerek bir tür "norm ihracı" gerçekleştirmektedir. GDPR'ın ekstraterritorial uygulanabilirliği, AB dışındaki şirketleri de bu düzenlemelere uymaya zorlamakta ve bu durum, küresel bir hukuki hegemonya yaratmaktadır (Bradford, 2020, s. 74-142). Kuner vd. (2020, s. 98), bu süreci "düzenleyici emperyalizm" olarak adlandırmıştır. Özellikle gelişmekte olan ülkeler, AB'nin belirlediği standartlara uyum sağlamadığı takdirde uluslararası ticaretten dışlanma riskiyle karşı karşıya kalmaktadırlar.

Dijital kolonyalizm, medya emperyalizmi teorileriyle de yakından ilişkilidir. Boyd-Barrett (2014, s. 8), medya emperyalizmini "merkez ülkelerin kültürel ve normatif değerlerini çevre ülkelere dayatması" olarak tanımlar. Dijital kolonyalizm de benzer bir mekanizmayı dijital alanda işletir; ancak bu sefer dayatılan şey, kültürel içeriklerden ziyade veri işleme pratikleri ve dijital altyapı standartlarıdır. Bu bağlamda, dijital kolonyalizm, medya emperyalizminin 21. yüzyıldaki bir uzantısı olarak görülebilir.

Eleştirel perspektifler, dijital kolonyalizme karşı çeşitli direniş stratejileri önermektedir. Örneğin, Hindistan'ın veri yerelleştirme politikaları veya Çin'in "siber

egemenlik" modeli, bu tür bir hegemonyaya karşı geliştirilen ulusal tepkiler olarak değerlendirilebilir (Jia, 2022; Borgogno ve Savini Zangrandi, 2024, s. 580). Ancak, bu stratejilerin küresel dijital ekonominin baskıları karşısında ne kadar sürdürülebilir olduğu tartışma konusudur. Sonuç olarak, dijital kolonyalizm, modern kapitalizmin yeni bir aşamasını temsil etmekte ve bireylerin, toplumların ve ulus devletlerin dijital gelecekleri üzerinde derin etkiler yaratmaktadır. Bu nedenle, konunun disiplinler arası bir yaklaşımla ele alınması ve küresel adalet perspektifiyle değerlendirilmesi gerekmektedir.

Veri sömürüsü (data exploitation), dijital kapitalizm bağlamında, teknoloji devlerinin kullanıcı verilerini kontrolsüzce çıkararak ekonomik ve siyasi güç elde etmesini ifade eder (Zuboff, 2019, s. 96). Bu süreç geleneksel sömürgecilikten farklı biçimde, meta olarak veri (data as commodity) üzerinden işler (Couldry ve Mejias, 2019, s. 9-10). Dijital bağımlılık (digital dependency) ise çevre ülkelerin teknoloji altyapısı, platformları ve hukuki rejimler açısından merkez ülkelere bağımlı hale gelmesini tanımlar (Fuchs, 2021, s. 171). Kullanıcılar, sosyal medya platformlarında ürettikleri veriler karşılığında parasal bir gelir elde etmez; bu durum dijital emek (digital labour) olarak teorize edilir (Scholz, 2017, s. 147). Zuboff (2019), bu süreci gözetim kapitalizmi (surveillance capitalism) kavramıyla açıklar. Kişisel veriler, davranışsal tahmin ve manipülasyon için ham madde olarak kullanılır. Dijital sömürü, tarihsel sömürgecilik pratiklerinin teknolojik uzantısıdır (Hesmondhalgh, 2015, s. 35). Küresel Güney ülkeleri, verilerini ABD ve AB merkezli şirketlerin sunucularında depolamak zorunda kalır, bu da veri kolonyalizmi (data colonialism) ile sonuçlanır. Örneğin, TÜİK'in 2023 verilerine göre bireylerin en fazla kullandıkları sosyal medya ve mesajlaşma uygulamaları arasında %84,9 ile WhatsApp, %69,0 ile YouTube ve %61,4 ile Instagram yer almaktadır (TÜİK, 2023). Bu yaygın kullanım, kullanıcı verilerinin Meta ve Google gibi küresel dijital platformlarda yoğun biçimde işlenmesine zemin hazırlamaktadır. Dijital bağımlılığın en önemli sonucu da yerel şirketlerin AWS veya Google Cloud gibi altyapıları kullanmak zorunda kalarak teknik özerkliklerini kaybetmesidir (Sadowski, 2020, s. 198).

Yöntem

Bu çalışma, dijital kolonyalizm ve medya emperyalizmi bağlamında kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin etkinliğini, nitel araştırma yöntemleri kullanarak incelemektedir. Karşılaştırmalı hukuk analizi ile GDPR ve KVKK'nın temel ilkeleri (şeffaflık, hesap verebilirlik, güvenlik) sistematik olarak değerlendirilmiş; vaka çalışması yöntemiyle Facebook-Cambridge Analytica skandalı gibi somut örnekler üzerinden pratik ihlaller analiz edilmiştir. Veriler, birincil kaynaklar (yasa metinleri, mahkeme kararları) ve ikincil kaynaklar (akademik yayınlar, uluslararası raporlar) aracılığıyla toplanmış, içerik ve normatif analiz teknikleriyle yorumlanmıştır. Araştırma kapsamı, 2018-2024 döneminde AB ve Türkiye'deki yasal uygulamalarla sınırlandırılmıştır. Bulgular dijital hakimiyetin sınırlandırılması için merkeziyetsiz teknoloji modellerinin gerekliliğini ortaya koyacağı öngörülmüştür. Çalışmanın temel sınırlılığı, GDPR'nın küresel yaptırım gücüne ve KVKK'nın idari kapasite eksikliklerine ilişkin tartışmaların kapsam dışı bırakılmasıdır.

Medya emperyalizmi üzerine yapılan çalışmalar ağırlıklı olarak medya devlerinin tarihi, mülkiyeti, ekonomileri ve operasyonlarına odaklanmaktadır. Medya emperyalizminde en az üç ilişki biçimi vardır (Boyd-Barrett, 2014, s. 38-41): Birincisi,

emperyalizm süreçleri çeşitli anlamlarda medya tarafından ve medya aracılığıyla yürütülür, teşvik edilir, dönüştürülür, baltalanır ve direnilir. İkincisi, medya; ürettiği ve dolaşıma soktuğu anlamlar ile bunları sürdüren politik-ekonomik mekanizmalar aracılığıyla, süregelen imparatorluk kurma ve sürdürme süreçleriyle şekillenir ve geçmiş imparatorlukların kalıntılarını taşır. Üçüncü olarak, bazı medya davranışları daha geniş çerçevelere atıfta bulunmaksızın emperyalist olarak değerlendirilebilir. Bunlar uluslararası (eşitsiz haber alışverişinde olduğu gibi), Batılı uluslararası haber ajansları tarafından ulusal basına dayatılan ilişkiler (19. ve 20. yüzyıllarda) veya ulusal nitelikte (güçlü eğlence ve haber medyasının belirli bir ulusal bölge üzerinde aşırı ticari ve siyasi etki kurması durumunda olduğu gibi) gerçekleşebilir.

Bulgular ve Tartışma

Dijital platformların kullanıcı verilerini kötüye kullanımı Facebook-Cambridge Analytica skandalı gibi örneklerde de görülmektedir. Bazı platformlar kullanıcı verilerini rıza alınmadan veya manipülatif yollarla işleyerek ihlal etmektedir. GDPR'nın (2016), açık rıza (m. 7) ve veri minimizasyonu (m. 5/1-c) ilkeleri, teorik düzeyde güçlü bir koruma çerçevesi sunsa da uygulamada platformların kullanıcıları, karmaşık aydınlatma metinleri ve tasarımsal yönlendirmeler aracılığıyla rıza üretimine yönlendirebildiği görülmektedir (Costello ve Leiser, 2024, s. 47-66).

Facebook-Cambridge Analytica Skandalı, 2018'de ortaya çıkan ve 87 milyon Facebook kullanıcısının kişisel verilerinin, Cambridge Analytica şirketi tarafından siyasi manipülasyon amacıyla izinsiz kullanıldığını gösteren bir veri ihlalidir. Skandal, veri toplamak için bir anket uygulamasının kötüye kullanılmasıyla başlamıştır ve ABD seçimleri ile Brexit referandumunda hedefli reklamlar için kullanıldığı iddia edilmiştir (Cadwalladr ve Graham-Harrison, 2018).

Başka bir olayda, Google'ın 2022'de 391 milyon ABD doları ceza alması, kullanıcı konum verilerini şeffaf olmayan yöntemlerle topladığının tespitiyle ilişkilidir (State of New Jersey, Department of Law ve Public Safety, 2022). Benzer şekilde, Türkiye'de KVKK'nın (2016, m. 4) düzenlediği "hukuka ve dürüstlük kurallarına uygunluk" ilkesi, pratikte platformların veri işleme amaçlarını belirsiz bırakması nedeniyle işlevsiz kalabilmektedir.

GDPR'nın küresel etkisini, norm ihracı (norm export) kavramı çerçevesinde ele almak mümkündür. Bu süreç, AB'nin dijital politikalarını üçüncü ülkelere dolaylı veya doğrudan dayatarak ekonomik ve hukuki hegemonya kurmasını ifade eder (Bradford, 2020, s. 64). GDPR'nın (2016, m. 3) ekstraterritorial uygulanabilirliği, AB dışındaki şirketleri de kapsayacak şekilde tasarlanmıştır. Bu durum, AB'nin düzenleyici güç olarak konumlanmasını sağlamıştır. GDPR'nın norm ihracı, geleneksel medya emperyalizmi teorileriyle paralellik göstermektedir. Boyd-Barrett (2014), medya emperyalizmini "merkez ülkelerin kültürel ve yasal normları çevre ülkelere dayatması" olarak tanımlar. GDPR de benzer şekilde, veri koruma standartlarını küresel dijital ekonomiye dayatarak "dijital merkez-çevre" ilişkisini pekiştirir. Örneğin, AB'nin yeterlilik kararları (adequacy decisions), üçüncü ülkelerin KVKK gibi düzenlemelerde AB standartlarına uyumunu zorunlu kılar (Kuner vd., 2020, s. 83). Böylece çevre ülkeler, AB'nin teknik ve hukuki altyapısını benimsemek zorunda kalarak dijital bağımlılık sarmalına girer (Fuchs, 2021, s. 180) ve GDPR'nın yaptırımları (ör. küresel cirosunun %4'üne varan cezalar), AB

dışındaki şirketler için orantısız bir yük oluşturur (Svantesson, 2018). GDPR, medya emperyalizmi teorisinin dijital alandaki yansıması olarak okunabilir. AB, veri koruma standartlarıyla küresel dijital ticareti şekillendirirken, Türkiye gibi ülkeleri "uyum" veya "dışlanma" ikileminde bırakmaktadır. GDPR ve KVKK'daki ilkeler, etkin denetim olmadan işlevsizdir. Bu analiz, hukukun evrenselliği bağlamında dijital etiğin önemini vurgulamaktadır.

Tablo-1: Medya Emperyalizmi Bağlamında GDPR ve KVKK'nın Karşılaştırmalı Analizi

Kriter	GDPR (AB)	KVKK (Türkiye)	Medya Emperyalizmi Yansıması
Kapsam	Tüm AB üye devletleri + AB dışındaki veri işleyenler (Madde 3)	Yalnızca Türkiye'de veri işleyenler (Madde 2)	GDPR'nın ekstraterritorial uygulanması, küresel hegemonya örneği
Rıza Şartları	Açık, özgür iradeyle verilmiş rıza (Madde 7)	Benzer, ancak "açık rıza" tanımı daha esnek (Madde 5)	KVKK'nın AB normlarına uyumlu yapısı / Norm ihracı
Veri Transferi	Yeterlilik kararı olmayan ülkelere transfer kuralı olarak yasak (Madde 45)	Yabancı ülkelere transferde KVK Kurulu'ndan izin (Madde 9)	AB'nin "yeterlilik" kriterleriyle Türkiye'yi dolaylı kontrolü
Yaptırımlar	Küresel cirosunun %4'üne kadar ceza (Madde 83/4-6)	Maktu idari para cezaları (Madde 18)	GDPR'nın küresel şirketler üzerinde baskı gücü ancak KVKK'nın ulusal sınırlılığı
Veri Yerelleştirme	Zorunlu değil (ancak ülkeler ek tedbir alabilir)	KVKK'da yerelleştirme zorunluluğu yoktur. Yerelleştirme, sektörel mevzuattan kaynaklanır (örn. bankacılık).	Türkiye'nin dijital bağımlılığa karşı kısmi direnç ve güvenlik kaygıları (KVKK dışında özellikle Bankacılık Düzenleme ve Denetleme Kurulu, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Madde 25 ile "Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmalarını zorunlu" kılmaktadır.)
Veri Sahibi Hakları	Silinme, itiraz, taşınabilirlik hakları (Madde 16-20)	Benzer haklar (Madde 11)	AB vatandaşlarına "üstün koruma" ancak çevre ülkelerde kademeli uyum
Dijital Platformlar	Google/Facebook gibi şirketler merkezi AB politikalarına uymak zorunda	Türkiye'de yerleşik olmayan veri sorumluları için temsilci atama zorunluluğu (Madde 16/2)	Teknoloji devlerinin Türkiye'deki fiili egemenliğini engelleme çabasıdır; çevre ülkelerin merkez ülkelerin teknoloji devlerine karşı geliştirdiği direnç stratejilerini yansıtır.

Türkiye'nin Kişisel Verilerin Korunması Kanunu (KVKK) ile AB'nin Genel Veri Koruma Tüzüğü (GDPR) arasında, bireysel hakların korunması bağlamında bazı farklar ortaya çıkmaktadır. Türkiye'deki veri koruma rejimi, AB standartlarına kısmen uyumlu olsa da uygulamada haklar konusunda birtakım sınırlılıklar bulunmakta, denetim mekanizmaları ve yaptırımlar konusunda da bazı eksiklikler içermektedir:

Rıza ve İşleme Şartlarındaki Farklılıklar: AB vatandaşları, verilerinin nasıl kullanılacağı konusunda daha fazla kontrol hakkına sahipken, Türkiye'deki bireyler için belirsizlikler mevcuttur.

GDPR (AB)

Açık ve özgür iradeyle verilmiş rıza gereklidir (GDPR, 2016, m. 4/11), kullanıcıların veri işleme faaliyetlerini anlayarak onay vermesi şarttır (GDPR, 2016, m. 7). Hassas verilerde ise ek koruma söz konusudur; ırk, din, sağlık verileri gibi özel kategorideki veriler için açık rıza zorunluluğu vardır (GDPR, 2016, m. 9/1-2). Ancak kamu sağlığı gibi bazı durumlarda özel nitelikli kişisel verilerin işlenmesi için istisnalar getirilmiştir (GDPR, 2016, m. 9/2-i).

KVKK (TÜRKİYE)

Genel nitelikli kişisel verilerin ve özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmış (Kişisel Verilerin Korunması Kanunu, 2016, m. 5 ve m. 6), bunlara yönelik istisnalar (m. 5/2 ve m. 6/3) da ayrıca düzenlenmiştir. Ancak bu düzenlemelerde; önceden, olumlu bir davranışla rıza gösterilmesinin belirtilmemesi ve rızanın geri alınmasının her zaman mümkün olduğunun açıkça ifade edilmemesi, GDPR karşısında birer eksiklik olarak görülmektedir (Akkurt, 2023, s. 183). Bununla birlikte, özel nitelikli kişisel verilerin işleme şartlarına ilişkin KVKK'nın (2016) 6. maddesi, 12 Mart 2024 tarihli Resmî Gazete'de yayımlanan 7499 sayılı kanun ile değiştirilmiş ve ilgili düzenleme 1 Haziran 2024 tarihinde yürürlüğe girmiştir. Aynı şekilde KVK Kurulu'nun kararları ile uygulamanın bu yönde gelişmesi sağlanabilecektir.

Veri Sahibi Haklarındaki Uygulama Farkları: AB vatandaşları, dijital özerklik konusunda daha avantajlıdır. Türkiye'de ise kurum pratikleri ve bilinçlenmeyle birlikte bu hakların kullanımının daha etkin hale gelmesi beklenmektedir.

GDPR (AB)

GDPR'da AB vatandaşları için güçlü bireysel haklar söz konusudur. Bunlar sırasıyla, silinme hakkı (Madde 17: AB vatandaşları, verilerinin derhal silinmesini talep edebilir, ancak bu mutlak bir hak değildir (Turan, 2019, s. 165), veri taşınabilirliği (Madde 20: Kullanıcılar, verilerini bir platformdan diğerine aktarabilir, örneğin Facebook'tan Twitter'a) ve otomatik kararlara itirazdır (Madde 22: Algoritmik ayrımcılığa karşı itiraz hakkı).

KVKK (TÜRKİYE)

KVKK'da bireysel haklar daha sınırlıdır. Örneğin silinme hakkı (genelde unutulma hakkı olarak isimlendirilmektedir) Madde 11'de vardır, ancak uygulamada (şirketlerin hukuki yükümlülükleri gerekçe göstererek silmeyi reddedebilmesinde olduğu gibi) bazı aksaklıklar yaşanabilmektedir. Veri taşınabilirliğine ilişkin bir düzenleme bulunmamakta, KVKK'da bu hak yer almamaktadır.

Veri transferi yeterlilik kararı verilen ülkeler bakımından herhangi bir özel izin gerekmeden yapılabilmektedir. Ancak Türkiye, AB'nin yeterlilik kararı (adequacy decision) verdiği ülkeler arasında yer almamaktadır (European Commission, 2026). Ülkemizde veri transferi ile ilgili işlemler, GDPR'da da izin verilen standart sözleşmeler yoluyla yapılmaktadır. Bu da işlemleri yavaşlatan ve zorlaştıran bir durumdur. Öte

yandan ülkemizden yurt dışına veri transferinde, KVKK (2016, m. 9) uyarınca yeterli korumanın bulunduğu ülkelere veri aktarımına izin verilmektedir. KVK Kurulu yeterli korumanın bulunduğu ülkelere ilişkin esas alınacak kriterleri belirlemiştir (2019/125 sayılı Karar).

Otomatik kararlara itiraz ise kısmen düzenlenmiştir. KVKK (2016, m. 11/1-h) bunu düzenlemiş olmakla birlikte kapsamı GDPR'a göre dardır. GDPR (2016, m. 77/1) şikâyetin yapılabileceği yerler bakımından daha çok alternatif sunmaktadır. Örneğin ihlalin gerçekleştiği ülke, kişinin yerleşim yeri veya çalışma yerinin bulunduğu ülke kurumuna başvuruda bulunulabilir. Bu düzenlemede GDPR'ın, AB ülkelerinin tamamında uygulanmasının da etkisi vardır. Ülkemizde bu şikâyetler sadece KVK Kurulu'na yapılabilmektedir (KVKK, 2016, m. 14/1).

Yaptırımlar ve Denetim: AB'de şirketler GDPR'a uymak zorundadır, bu konuda AB'nin caydırıcılığı söz konusudur; Türkiye'de ise yaptırımlar daha zayıftır (Kişisel Verileri Koruma Kurumu'nun faaliyet raporunda başvurular ve yaptırımlarla ilgili istatistikler yer almaktadır).

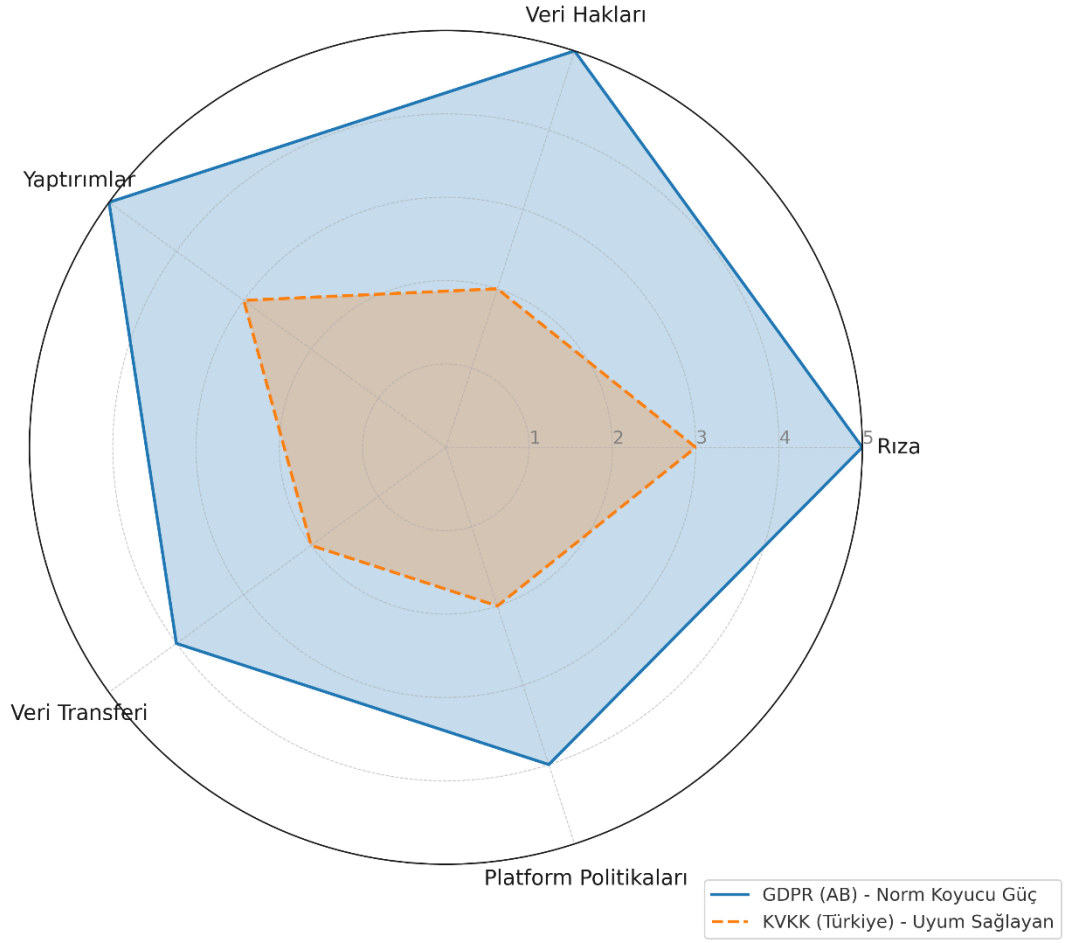
GDPR (AB)

GDPR'ın güçlü yaptırımları bulunmaktadır, örneğin Madde 83 ile bir şirketin küresel cirosunun %4'üne kadar ceza uygulanmaktadır; Meta'ya 2023 yılında 1,2 milyar € para cezası verilmiştir. Ayrıca AB ülkelerinde ulusal veri koruma otoriteleri (ör. Almanya'da BfDI) oldukça etkin çalışmaktadır.

KVKK (TÜRKİYE)

KVKK'da (2016, m. 18) idari para cezaları maktu tutarlar üzerinden düzenlenmiştir. Buna karşılık GDPR (2016, m. 83/4-6), yıllık küresel cironun %4'üne kadar ulaşabilen idari para cezaları öngörmektedir. Bu durum, GDPR'ın yaptırım gücünü KVKK'ya kıyasla daha caydırıcı hale getirmektedir.

Dijital Platformların Türkiye'deki Fıili Egemenliği: AB vatandaşları, platformlar üzerinde daha fazla kontrol hakkına sahipken, Türkiye'deki kullanıcılar için aynı durum söz konusu değildir. Tam da medya emperyalizmine örnek teşkil edecek şekilde Google/Facebook gibi şirketler, AB vatandaşlarına daha şeffaf politikalar uygularken (ör. Avrupa'da reklam profillemeye kısıtlamaları), aynı platformlar Türkiye'de farklı politikalar benimseyebilmektedir. Yerel temsilci zorunluluğu (KVKK, 2016, m. 11/2) bulunmasına rağmen, uygulamada işleyiş, zayıf görünmektedir. Aslında dijital platformlar için getirilen yerel temsilci atanması zorunluluğu, veri sorumlusuyla iletişimi kolaylaştırmak ve tebligat süreci için önemlidir. Konuya ilişkin ayrıca, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da (5651 sayılı Kanun, 2007, m. 4, 7, 8 ve 9) sorumluluk ve yaptırımlarla ilgili bir düzenleme yer almaktadır ve bu düzenleme ile temsilci atanmamasına yönelik yaptırım getirilmektedir. Bundan başka yabancı sermaye şirketlerinin gerçek faydalanıcı bildirimini yapmaları da gerekmektedir. Böylece bir ihlal gerçekleştiğinde veri sorumlusunun tespitinin kolaylaştırılması sağlanmaktadır. Ancak dijital platformların bu düzenlemelere yönelik direnci ile karşılaşabilmektedir.



Şekil-1: Dijital Kolonyalizm Perspektifinden GDPR (AB)-KVKK (Türkiye) Karşılaştırması

Şekil 1’de GDPR “norm koyucu güç” olarak daha geniş alan kaplamakta, KVKK ise “uyum sağlayan” pozisyonda kalmaktadır. Radar diyagramı, dijital kolonyalizmdeki güç asimetrisini doğrudan yansıtmaktadır.

Sonuç

Bu çalışmanın bulguları, dijital kolonyalizm olgusunun hukuki alandaki tezahürlerini net biçimde ortaya koymaktadır. GDPR’ın küresel bir standart haline gelmesi, AB’nin norm ihracı kapasitesinin bir göstergesi olarak yorumlanabilir. Bradford’un (2020) "Brüksel Etkisi" tezinde vurguladığı üzere, AB ekonomik gücünü düzenleyici hegemonya aracına dönüştürerek dijital alanda belirleyici aktör konumunu pekiştirmektedir. Bu açıdan bakıldığında KVKK’nın hazırlanmasında AB normlarının esas alınması, olumsuz bir durum olarak görülebilir. Ancak KVKK ülkemiz için önemli bir düzenlemedir, AB vatandaşlarının sahip olduğu kişisel verilerin korunmasına yönelik haklardan ülkemiz vatandaşlarının da yararlanmasına imkân vermektedir. KVKK şüphesiz GDPR düzeyinde bir koruma henüz sağlayamamaktadır. Ancak insanların bilinçlenmesi, KVKK’da yapılan değişiklikler ve KVK Kurulu uygulamaları ile bu

korumanın genişleyeceği öngörülebilmektedir. Nitekim gerek Adalet Bakanlığı Yargı Reformu Stratejisi'nde gerekse 2024-2028 yıllarını kapsayan On İkinci Kalkınma Planı'nda KVKK'nın GDPR çerçevesinde güncellenmesi de öngörülmektedir (Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023). Ayrıca belirtilmelidir ki KVKK bilgi güvenliğine yönelik bir düzenleme değildir. Amaç veriyi ve verinin adresi olan bireyi korumaktır. Bu bağlamda KVKK, temel hak ve özgürlüklerin korunmasını güvence altına almaktadır. Bununla birlikte, kişisel verilerin korunması ile veri temelli ekonominin sürdürülebilirliği arasında hassas bir denge sağlanması gerekmektedir.

Hukuki asimetrinin kaynakları üç temel eksen de incelenebilir: Birincisi, AB'nin birey hakları odaklı anayasal geleneği ile Türkiye'nin devlet merkezli yaklaşımı arasındaki felsefi ayrımdır. İkincisi, denetim mekanizmalarının kurumsal kapasite farklılıklarıdır. Üçüncüsü ise yaptırımların caydırıcılık düzeyindeki belirgin eşitsizliklerdir. Özellikle Meta'ya kesilen 1,2 milyar avroluk rekor ceza (European Data Protection Board, 2023), GDPR'ın uygulama kararlılığını somutlaştırırken, KVKK'nın benzer vakalardaki tutumu, Türkiye'nin ekonomik, politik ve jeopolitik niteliklerinden dolayı hibrit bir profile sahiptir.

Dijital özerklik için yapısal öneriler bağlamında üç temel reform alanı öne çıkmaktadır. Normatif düzeyde KVKK'nın, GDPR ile tam uyumlu hale getirilmesi, özellikle veri taşınabilirliği hakkı ve otomatik karar alma mekanizmalarına itiraz gibi eksik hakların düzenlenmesi önem arz etmektedir. Kurumsal düzeyde ise Kişisel Verileri Koruma Kurumunun idari ve mali özerkliğinin güçlendirilmesi gerekmektedir. Ayrıca, medya emperyalizmine karşı en büyük direnç noktası olarak teknolojik düzeyde ulusal bulut sistemleri ve açık kaynaklı platformların geliştirilmesi gerekli görülmektedir. Sonuç olarak, dijital kolonyalizmle mücadelede hukukun koruyucu rolünün etkinleştirilmesi için çok katmanlı bir stratejinin gerekliliği ortaya çıkmaktadır.

Etik Beyanı: Yazarlar çalışmanın, etik kurul izni gerektirmeyen çalışmalar arasında yer aldığını beyan etmektedir. Aksi bir durumun tespiti halinde Kastamonu İletişim Araştırmaları Dergisi'nin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.

Yazar Katkıları: Çalışma iki yazarlı olup, birinci yazarın katkı oranı %50, ikinci yazarın katkı oranı %50'dir

Çıkar Çatışması Beyanı: Yazarlar herhangi bir çıkar çatışması olmadığını beyan etmektedir.

Kaynakça

- T.C. Adalet Bakanlığı. (2025). *Türkiye Yüzyılı Yargı Reformu Stratejisi*. <https://cdn.uyap.gov.tr/yrsportal/strategydocument/Vo2bMRfG/7OXINODO5.pdf>
- Akiner, N. (2024). A theoretical approach to digital colonialism in the context of media imperialism. In *International Conference on Social Science Research (ICONSR 2024) Abstracts & Proceedings Book* (pp. 131–141). Association of Kutbilge Academics.

- Akkurt, S. S. (2023). Açık rıza. P. Ç. Aksoy ve H. C. Aksoy (Ed.), *Kişisel verilerin korunmasına akademik bakış: KVKK akademi derleme çalışması* (ss. 155–194). KVKK Yayınları.
- Borgogno, O., & Savini Zangrandi, M. (2024). Chinese data governance and trade policy: from cyber sovereignty to the quest for digital hegemony? *Journal of Contemporary China*, 33(148), 578–602. <https://doi.org/10.1080/10670564.2023.2299961>
- Boyd-Barrett, O. (2014). *Media imperialism*. Sage.
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Cadwalladr, C., & Graham-Harrison, E. (2018, 17 Mart). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Costello, R. Á., & Leiser, M. (Eds.). (2024). *Critical reflections on the EU's data protection regime: GDPR in the machine*. Bloomsbury Publishing.
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2023). *On ikinci kalkınma planı (2024–2028)*. https://www.sbb.gov.tr/wp-content/uploads/2023/12/On-Ikinci-Kalkinma-Plani_2024-2028_11122023.pdf
- Develioğlu, H. M. (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca kişisel verilerin korunması hukuku*. On İki Levha Yayıncılık.
- European Commission. (2026). *Adequacy decisions*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- European Data Protection Board. (2023, May 22). *1.2 billion euro fine for Facebook as a result of EDPB binding decision*. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
- Fuchs, C. (2021). *Digital capitalism: Media, communication and society volume three*. Routledge.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. (2016, 27 April). *Official Journal of the European Union*, L119/1. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Hesmondhalgh, D. (2015). Exploitation and media labor. In R. Maxwell (Ed.), *The Routledge companion to labor and media* (pp. 30–39). Routledge.
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, No. 5651. (2007, 23 Mayıs). *Resmî Gazete* (Sayı: 26530). resmigazete.gov.tr

- Jia, L. (2022). Digital sovereignty with Chinese characteristics: Data governance and cyber governance in China's 14th Five-Year Plan. *Chinese Journal of Communication*, 15(3), 350–367. <https://doi.org/10.1080/17544750.2022.2055135>
- Kaya, M. B. (2020). Kişisel verilerin işlenmesi ve korunması arasındaki denge. A. Bilgili ve L. Keser Berber (Ed.), *Güncel gelişmeler ışığında kişisel verilerin korunması hukuku* (ss. 36–42). On İki Levha Yayıncılık.
- Kişisel Verilerin Korunması Kanunu, No. 6698. (2016, 7 Nisan). *Resmî Gazete* (Sayı: 29677). resmigazete.gov.tr
- Kişisel Verileri Koruma Kurulu. (2019, 24 Ocak). *Kişisel veri ihlali bildirim usul ve esaslarına ilişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı kararına ilişkin duyuru*. <https://www.kvkk.gov.tr>
- Kişisel Verileri Koruma Kurulu. (2019, 2 Mayıs). *Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form hakkındaki 02/05/2019 tarihli ve 2019/125 sayılı Kurul Kararı*. <https://www.kvkk.gov.tr/>
- Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
- Küzeci, E. (2023). *Kişisel verilerin korunması*. On İki Levha Yayıncılık.
- Özdemir, H. (2009). *Elektronik haberleşme alanında kişisel verilerin özel hukuk hükümlerine göre korunması*. Seçkin Yayıncılık.
- Özer Deniz, M. (2022). *Özel nitelikli kişisel verilerin işlenmesi ve bundan doğan sorumluluk*. On İki Levha Yayıncılık.
- Özkan, O. (2020). *Kişisel verilerin korunması*. Yetkin Yayıncılık.
- Sadowski, J. (2020). *Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world*. MIT Press.
- Scholz, T. (2017). *Überworked and underpaid: How workers are disrupting the digital economy*. Polity Press.
- State of New Jersey, Department of Law & Public Safety. (2022, November 14). *Forty attorneys general announce historic settlement with Google over location tracking practices* [Press release]. <https://www.njoag.gov/forty-attorneys-general-announce-historic-settlement-with-google-over-location-tracking-practices/>
- Svantesson, D. J. B. (2018, May 1). *GDPR and the extraterritorial reach of EU privacy law: Are you at risk of fines of 4% of global turnover?* Quinn Emanuel Urquhart & Sullivan LLP. <https://www.quinnemanuel.com/the-firm/publications/article-may-2018-gdpr-and-the-extra-territorial-reach-of-eu-privacy-law-are-you-at-risk-of-fines-of-4-of-global-turnover/>
- Şimşek, O. (2008). *Anayasa hukukunda kişisel verilerin korunması*. Beta Yayıncılık.
- Taştan, F. G. (2017). *Türk sözleşme hukukunda kişisel verilerin korunması*. On İki Levha Yayıncılık.
- Turan, M. (2019). *Karşılaştırmalı hukukta kişisel verilerin korunması*. Seçkin Yayıncılık.

- Türkiye Cumhuriyeti Anayasası, *Kanun No. 2709*. (1982, 9 Kasım). *Resmî Gazete* (Sayı: 17863 Mükerrer). resmigazete.gov.tr
- Türkiye İstatistik Kurumu [TÜİK]. (2023). *Hanehalkı bilişim teknolojileri (BT) kullanım araştırması, 2023*. [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanım-Arastirmasi-2023-49407](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanım-Arastirmasi-2023-49407)
- Yücedağ, N. (2023). Kişisel verilerin korunması kanunu kapsamında genel ilkeler. P. Ç. Aksoy ve H. C. Aksoy (Ed.), *Kişisel verilerin korunmasına akademik bakış* (ss. 135–154). KVKK Yayınları.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- 7499 Sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun. (2024, 12 Mart). *Resmî Gazete* (Sayı: 32487). resmigazete.gov.tr