

Sosyal Ağlarda Mahremiyetin Ticarileşmesi Sorunu ve Çözüm Önerileri

Sema ÇINAR ALEVLI*

ÖZ

Bu çalışma, dijital çağda sosyal medya platformlarının kullanıcı mahremiyetini sistematik biçimde ticarileştirme pratiklerini inceleyerek, bu sürecin bireylerin veri üzerindeki denetimi, veri güvenliği ve dijital kamusal alanın yapısı üzerindeki etkilerini analiz etmektedir. Araştırmada, platformların kullanıcı verilerini hangi yöntemlerle topladığı, bu verileri nasıl ekonomik metaya dönüştürdüğü, kullanıcıların veri kontrol düzeyinin ne ölçüde işlevsel olduğu, mevcut yasal ve etik düzenlemelerin bu süreci sınırlandırmadaki yeterliliği ve daha adil bir dijital düzenin inşasının imkânı sorgulanmıştır. Bulgular, mahremiyetin giderek algoritmik sistemler içinde metalaştığını, rıza mekanizmalarının çoğu zaman sembolik kaldığını ve bireylerin dijital öznelliğinin ekonomik çıkarlar doğrultusunda yeniden biçimlendirildiğini göstermektedir. Çalışma, yalnızca hukuki düzenlemelerin değil; tasarımsal reformların, etik bilinçlenmenin ve kültürel dönüşümün de bu sürece dâhil edilmesi gerektiğini ortaya koymaktadır. Özellikle ebeveynlerin ve yetişkin bireylerin dijital farkındalık ve rehberlik rolleri, çocukların mahremiyet bilincinin gelişimi açısından kritik bir konumda değerlendirilmektedir. Bu yönüyle çalışma, mahremiyetin korunmasını yalnızca bireysel güvenlik değil; aynı zamanda dijital demokrasinin sürdürülebilirliği ve toplumsal iyi oluş hâlinin devamlılığını sağlama sorumluluğu olarak ele almaktadır.

Anahtar Kelimeler: Dijital Mahremiyet, Sosyal Medya, Veri Güvenliği, Platform Ekonomisi, Dijital Etik.

Başvuru / Kabul: 04 Mayıs 2025 / 10 Haziran 2025

Atıf: Çınar Alevli, S. (2025). Sosyal Ağlarda Mahremiyetin Ticarileşmesi Sorunu ve Çözüm Önerileri, *İmgelem*, Yeni Medya Çalışmaları Özel Sayısı, 811-842.

The Problem of the Commercialization of Privacy on Social Networks and Proposed Solutions

ABSTRACT

This study examines the systematic commodification of user privacy by social media platforms in the digital age, analyzing its implications for individual data sovereignty, information security, and the structure of the digital public sphere. It explores how platforms collect personal data, transform it into economic assets, the extent to which users retain actual control over their data, the adequacy of current legal and ethical regulations, and the possibilities for building a more just digital environment. Findings reveal that privacy is increasingly reduced to an economic object within algorithmic systems, that consent mechanisms often lack substantive meaning, and that users' digital subjectivities are reshaped in alignment with corporate interests. The study argues for the necessity of integrating not only legal reforms but also design-based interventions, ethical awareness, and cultural transformation into digital governance practices. Special emphasis is placed on the role of parents and adult users in fostering digital literacy and guiding children toward responsible engagement with digital platforms. In this respect, the study frames privacy not merely as a matter of personal security, but as a normative imperative linked to the sustainability of digital democracy and the responsibility to sustain the continuity of collective well-being.

Keywords: Digital Privacy, Social Media, Data Security, Platform Economy, Digital Ethics.

Received / Accepted: 04 May 2025 / 10 June 2025

*Dr., Bağımsız Araştırmacı. E-posta: semacinaralevli@gmail.com, ORCID Numarası: [0000-0003-3968-7594](https://orcid.org/0000-0003-3968-7594)



Citation: Çınar Alevli, S. (2025). The Problem of the Commercialization of Privacy on Social Networks and Proposed Solutions, *İmgelem*, New Media Studies Special Issue, 811-842.

GİRİŞ

Dijital çağ, bireylerin kamusal ve özel alanlarındaki sınırları yeniden tanımlayan, sosyoteknolojik dönüşümlerin hız kazandığı bir dönemi ifade etmektedir. Bu dönemin en çarpıcı yönlerinden biri, bireylerin sosyal medya platformları aracılığıyla sürekli bir bağlantı ve etkileşim içinde olmasıdır. Facebook, Instagram, TikTok ve X (eski adıyla Twitter) gibi sosyal medya ağları yalnızca bireyler arası iletişim araçları olmanın ötesine geçmiş; siyasal katılımdan kültürel üretime, ekonomik tercihlerden kimlik inşasına kadar birçok alanda belirleyici hale gelmiştir (Van Dijck 2013). Dijital platformlar, kullanıcıların davranışlarını, tercihlerini ve sosyal ilişkilerini kayıt altına alarak, bu bilgileri yapılandırılmış veriler hâline dönüştürmekte ve bu verileri çok katmanlı algoritmik sistemler aracılığıyla işlemektedir. Bu veri temelli altyapı yalnızca iletişim pratiklerini değil, mahremiyet, özerklik ve toplumsal denetim gibi temel kavramları da dönüştürmektedir. Bu dönüşüm sürecinde en belirgin epistemolojik kırılma, mahremiyet kavramı etrafında şekillenmektedir.

Geleneksel mahremiyet anlayışı, bireyin kişisel alanının korunması, kişisel verilerinin izinsiz ifşa edilmemesi ve bireysel özerkliğin güvence altına alınması gibi etik ve hukuki ilkeler üzerine inşa edilmiştir. Bu yaklaşım, liberal bireycilik çerçevesinde şekillenmiş olup, bireyin rasyonel ve özerk bir özne olarak kendi yaşamı ve bilgileri üzerinde denetim hakkına sahip olduğu varsayımına dayanır. Bu kavramsal çerçeve, uzun süre mahremiyetin hem hukuki düzenlemelerde hem de toplumsal normlarda nasıl anlaşıldığını belirlemiştir. Ne var ki, dijital teknolojilerin yaygınlaşması ve özellikle sosyal medya platformlarının günlük yaşamın vazgeçilmez bir parçası haline gelmesiyle birlikte, mahremiyetin bu geleneksel ilkeleri önemli ölçüde dönüşüme uğramıştır.

Geleneksel mahremiyet ilkeleri dijital ortamda esnekleşmiş, mahremiyet giderek bir mübadele nesnesine, daha da ötesi ekonomik değeri olan bir "meta"ya dönüşmüştür. Kullanıcılar sosyal medya platformlarına gönüllü olarak katılmakta, ancak bu katılım karşılığında kendilerine ait çok boyutlu verileri – çoğu zaman farkında olmadan – bu platformlara devretmektedir. Sosyal medya şirketleri, kullanıcı verilerini yalnızca depolamakla kalmamakta; aynı zamanda bu verileri davranışsal tahmin, kişiselleştirilmiş reklamcılık ve içerik yönlendirme gibi uygulamalarda kullanmaktadırlar (Zuboff 2019: 94; Seignani 2016: 733-35). Bu süreç, mahremiyetin ticarileştirilmesi olarak adlandırılabilir. Mahremiyetin

ticarileşmesi olgusu, bireylerin kişisel bilgilerinin rıza, kontrol ve şeffaflık ilkeleri göz ardı edilerek ekonomik kazanca dönüştürülmesini içermektedir.

Sosyal medya platformlarının işleyişinde, kullanıcı rızası genellikle varsayımsal bir kabul üzerinden kurgulanmaktadır. Karmaşık gizlilik politikaları ve algoritmik yapılar, kullanıcıların veri toplama süreçlerine dair bilgi sahibi olmalarını zorlaştırmakta; bu da fiilen bilgilendirilmiş rızanın ortadan kalkmasına neden olmaktadır (Nissenbaum 2010). Platformların tasarımı ise kullanıcıları sürekli etkileşim hâlinde tutmak, daha fazla veri üretmelerini sağlamak ve bu verileri işlevsel ekonomik girdilere dönüştürmek üzere kurgulanmıştır. Dolayısıyla bu yapı, bireyin veri üzerindeki kontrolünü zayıflatarak, mahremiyetin korunmasını ciddi biçimde tehdit etmektedir. Ayrıca, elde edilen verilerin üçüncü taraflara satılması, veri ihlallerinin artması ve algoritmik yönlendirmeyle bireysel seçimlerin manipülasyona açık hale gelmesi gibi sonuçlar, veri güvenliği ve demokratik denetim açısından ciddi riskler barındırmaktadır.

Bu bağlamda bu çalışmanın temel araştırma problemi, sosyal medya platformlarında kullanıcı mahremiyetinin sistematik biçimde ticarileştirilmesi ve bu sürecin veri güvenliği üzerindeki etkileridir. Bu doğrultuda araştırma şu sorulara yanıt aramaktadır:

- Sosyal medya platformları kullanıcı verilerini hangi yöntemlerle toplamaktadır ve bu verileri nasıl ticarileştirmektedir?
- Mahremiyetin ticarileştirilmesi veri güvenliğini ne tür şekillerde etkilemektedir?
- Kullanıcıların verileri üzerindeki kontrol düzeyi gerçekte ne kadar etkilidir?
- Mevcut yasal ve etik düzenlemeler bu süreci denetlemek için yeterli midir?
- Daha etik ve adil bir dijital altyapı ve temiz bir dijital gelecek mümkün müdür ve bu nasıl inşa edilebilir?

Bu çalışmanın amacı, sosyal medya platformlarında mahremiyetin nasıl ticarileştirildiğini derinlemesine analiz etmek, bu sürece eşlik eden veri güvenliği sorunlarını eleştirel bir bakışla irdelemek ve çözüm odaklı öneriler geliştirmektir. Araştırma kapsamında, özellikle kullanıcı rızasının sınırları, platformların ekonomik ve tasarımsal işleyişi, mevcut yasal düzenlemelerin etkinliği ile algoritmik şeffaflık gibi unsurlar, bu dönüşümün belirleyici dinamikleri olarak değerlendirilecektir. Çalışma, mahremiyeti yalnızca bireysel bir hak değil, aynı zamanda dijital çağda yeniden tanımlanması gereken kolektif bir sorumluluk alanı olarak ele almaktadır. Sorunun çözümünün yalnızca hukuki ya da politik müdahalelerle sınırlı kalamayacağı; bireysel farkındalık ve toplumsal sorumluluk temelinde geliştirilecek bütüncül

yaklaşımlarla desteklenmesi gerektiği vurgulanmaktadır. Bu doğrultuda, çalışmanın önemi; daha etik, şeffaf ve adil ve temiz bir dijital ekosistemin inşasında birey, toplum ve devlet düzeyinde sorumluluğun yeniden tanımlanmasına katkı sunmasında yatmaktadır.

Bu araştırma, nitel yöntemlere dayalı olarak yapılandırılmış ve eleştirel kuram ile politik ekonomi perspektiflerinden yararlanılarak geliştirilmiştir. Çalışma, ikincil kaynaklara dayalı belgesel tarama yöntemiyle yürütülmüş; özellikle mahremiyet, gözetim kapitalizmi, veri güvenliği ve dijital platformlar konularında yapılmış akademik çalışmalar, raporlar ve yasal metinler analiz edilmiştir.

Dijital Mahremiyetin Anlamı ve Yapısı

Mahremiyet, bireyin yaşamına ilişkin bilgi, beden ve duygusal alan üzerindeki denetimini ifade eden temel bir kavram olarak hem bireysel hakların teminatı hem de toplumsal ilişkilerin biçimlenişi açısından kurucu bir işleve sahiptir. Bu kavram yalnızca bireyin korunma talebine işaret etmekle kalmaz, aynı zamanda bireyin kimlik inşasında, toplumsal aidiyetlerinde ve öznelliğinin sınırlarının belirlenmesinde merkezi bir rol oynar. Bununla birlikte, mahremiyetin anlamı ve toplumsal işlevi, tarih boyunca siyasal, kültürel ve teknolojik dönüşümlere bağlı olarak dönüşmüştür.

Modern mahremiyet anlayışı, özellikle Aydınlanma düşüncesiyle birlikte belirginleşen birey merkezli öznellik anlayışının bir sonucu olarak ortaya çıkmıştır. Aydınlanma döneminde birey, kamusal alandan ayrılan ve devlet müdahalesine kapalı bir “özel alan” talebiyle öne çıkarken, mahremiyet bu özel alanın etik ve hukuki temelini oluşturmuştur. Bu çerçevede Immanuel Kant, *amaç olarak insan (formula of humanity)* kavramı çerçevesinde, bireyin kendi rasyonelliğiyle hareket edebilme yetisini vurgulamıştır (1996: 429). Bu ilkeye göre, insanın yalnızca araç olarak değil, aynı zamanda amaç olarak ele alınması gerekir. Bu da bireyin kendi özerkliğini inşa edebileceği müdahalesiz bir özel yaşam alanının, etik özne olmanın temel koşullarından biri olduğunu gösterir.

Hannah Arendt (1958: 38-42), mahremiyeti kamusal ve özel alan ayrımı çerçevesinde değerlendirerek, özel alanı bireyin dünyadan geri çekilerek düşünsel, duygusal ve ilişkisel derinleşme imkânı bulduğu bir mekân olarak tanımlar. Arendt’e göre özel alan, sadece dış müdahalelerden arındırılmış bir sığınak değil, aynı zamanda bireyin özgünlüğünü ve içsel bütünlüğünü inşa ettiği bir varoluş zemini olarak işlev görür. Bu yaklaşımda mahremiyet, yalnızca korunması gereken bir hak değil, bireyin varoluşsal bütünlüğünü sürdürebilmesi için gerekli bir koşuldur. Louis Wirth (1938: 12-13) ise mahremiyetin modern kent yaşamıyla

birlikte anonimlik ve bireysel sınır inşası üzerinden geliştiğini savunur. Wirth'e göre kentleşme, bireyleri sosyal bağlardan kısmen kopararak onları daha görünür ve aynı zamanda daha korunmasız hale getirir; bu durum, bireylerin kendilerine ait bir sınır ve iç alan oluşturma ihtiyacını artırır. Dolayısıyla mahremiyet, kent yaşamının anonim yapısı içinde bireyin kendilik alanını inşa etmesine imkân tanıyan bir koruma mekanizması işlevi görür.

Kentleşme bağlamında mahremiyetin sosyal mesafe ve bireysel korunma işlevine odaklanan bu yaklaşımın ötesinde, Sissela Bok'un (1982) perspektifinde mahremiyet, yalnızca bireysel bir hak değil, aynı zamanda etik ve toplumsal bir zorunluluk olarak şekillenir. Bu çerçevede mahremiyet, bireyin yaşamını başkalarının sürekli gözetiminden azade bir şekilde sürdürebilmesinin koşulu olarak görülür; söz konusu gözetimsizlik durumu ise güven, saygınlık ve özgürlük gibi temel etik değerlerin korunabilmesi açısından merkezi bir önem taşır. Bok'un yaklaşımında, mahremiyet sadece bireysel zararı önlemeye dönük bir kalkan değil, aynı zamanda toplumsal ilişkilerin sürdürülebilirliğini sağlayan normatif bir düzenleyici işleve sahiptir.

Judith Inness (1992: 57-8) mahremiyeti duygusal ve ilişkisel bağlamlarda ele alarak birey-toplum ilişkisini yeniden çerçeveledir. Inness, mahremiyetin yalnızca bireyin içe kapanma hakkı değil; aynı zamanda duygusal yakınlık içeren ilişkilerde sınır belirleme, bu sınırların tanınması ve korunmasını talep etme hakkı olduğunu ileri sürer. Bu bakış açısı, mahremiyetin yalnızca birey merkezli değil, aynı zamanda ilişkisel ve bağlamsal bir hak alanı olduğunu göstermesi açısından önemlidir. Inness'ın yaklaşımına paralel olarak, mahremiyetin duygusal ve ilişkisel bağlamlardaki dönüşümünü ele alan Anthony Giddens da bu süreci, bireysel kimlik inşasının merkezinde yer alan yapısal ve kültürel dönüşümlerle birlikte değerlendirir. Giddens'a göre modernlik, bireyleri geleneksel normatif bağlardan çözerek, onları *yaşam öykülerini (self-narratives)* sürekli biçimde yeniden inşa etmeye yönlendiren *refleksif modernlik (reflexive modernity)* olgusunu beraberinde getirmiştir. Bu bağlamda birey, artık sabit ve dışsal normlara göre değil, kendi yaşam deneyimlerini sürekli gözden geçirerek ve yeniden değerlendirerek öznelliğini biçimlendirir. Mahremiyet ise bu süreçte yalnızca korunması gereken bir alan değil, aynı zamanda bireyin kimliğini sürekli olarak yeniden tanımladığı bir öznelğin refleksif projesi olarak konumlanır (Giddens 1992: 75-78).

Giddens'ın analizinde mahremiyetin bu yeni formu, geleneksel normlarla şekillenmiş cinsiyet rollerinin, aile yapılarının ve evlilik anlayışlarının çözülmesiyle birlikte ortaya çıkan, daha esnek, seçilmiş ve bireyler arası müzakereye dayalı ilişkilerle örülüdür. Bu dönüşüm, Giddens'ın *saf ilişki (pure relationship)* adını verdiği yeni bir ilişki biçimini gündeme

getirmektedir. Saf ilişki, yalnızca geleneksel yükümlülöklere deęil, iki bireyin karřılıklı doyumuna, duygusal iletiřime ve eřitlięe dayalı olarak sürdürölür. Bu tür ilişkiler, bireylerin kişisel gelişimlerini sürdürebilecekleri bir mahrem alan yaratırken, aynı zamanda bireyin duygusal ve kimliksel ifadesine de alan açar (Giddens 1992: 58-63). Giddens bu çerçevede, mahremiyetin duygusal demokrasi olarak adlandırılabilcek bir süreçten geçtiğini savunur. Duygusal demokrasi, bireylerin duygusal ilişkilerde eřitlik, açıklık ve dürüstlük temelinde bir ilişki biçimi kurmalarını ifade eder. Bu anlayış, toplumsal cinsiyet rollerinin yeniden müzakere edildiğı, bireylerin duygusal ihtiyaçlarının karřılıklı tanındığı bir mahremiyet düzenini tanımlar. Bu bağlamda da mahremiyet, artık sadece bir geri çekilme alanı deęil, bireyin öznelliğini müzakere ettiğı, karřılıklı tanınmaya dayalı ilişkiler aracılığıyla kimliğini ifade ettiğı bir alandır (Giddens 1992:121-22).

Mahremiyetin hukuksal temellendirilmesi, modern hukuk düşüncesinde bireyin özel yaşam alanının tanınması ve korunması ihtiyacıyla birlikte gelişmiş, özellikle Samuel Warren ve Louis Brandeis'in *Mahremiyet Hakkı (The Right to Privacy)* başlıklı makalesiyle sistematik bir nitelik kazanmıştır. Warren ve Brandeis'in bu makalesi, bireyin rahatsız edilmeden yaşama hakkı şeklinde tanımlanan mahremiyetin, dönemin teknolojik gelişmeleri -özellikle fotoğraf makinesi ve gazetecilik faaliyetlerinin yaygınlaşması- karřısında hukuki güvence altına alınması gerektiğini savunur (Warren ve Brandeis 1890). Mahremiyet burada yalnızca fiziksel müdahaleye karřı bir korunma biçimi olarak deęil, bireyin manevi varlığının ve toplumsal itibarının da korunması gerektiğini vurgulayan genişletilmiş bir hak kategorisi olarak ele alınır. Bu yaklaşım, mahremiyetin hem maddi hem de duygusal bütünlüğü güvence altına alan, özerkliğe dayalı bir kişilik hakkı olarak kurulmasına zemin hazırlamıştır.

Hukuksal temellendirmeyi takip eden dönemde, özellikle İkinci Dünya Savaşı sonrasında Amerika'da mahremiyet kavramı, teknolojik gelişmelerin etkisiyle daha kapsamlı ve çok boyutlu bir şekilde ele alınmaya başlanmıştır. Yeni teknolojiler, özellikle bilgisayarların yaygınlaşması, bireylerin mahremiyetine dair kaygıları artırmış ve mahremiyetin sadece kişisel bir hak olmaktan çıkarak toplumsal bir mesele olarak yeniden tanımlanmasına zemin hazırlamıştır. 1960'ların başında New York Barosu tarafından başlatılan *Bilim ve Teknolojinin Mahremiyet Üzerindeki Etkisi (The Impact of Science and Technology on Privacy)* projesi, alanda öncü çalışmaların yürütölmesini sağlamış; bu süreçte Alan Westin'in liderliğinde gerçekleştirilen arařtırmalar, mahremiyetin teorik çerçevesinin şekillenmesinde belirleyici rol oynamıştır. Westin, mahremiyetin bireysel özerklikle sıkı bir ilişki içinde olduğunu ve bilgi teknolojilerinin yarattığı yeni koşullar altında mahremiyetin korunmasının zorunluluğunu

gündeme getirmiştir (Westin 1967). Westin'in tanımına göre mahremiyet, bireyin kişisel bilgileri üzerinde kontrol sahibi olma hakkıdır (1967: 7). Bu bağlamda, mahremiyet ancak bireyin hangi bilgiyi, ne zaman ve kiminle paylaşacağına kendisinin karar verebildiği durumlarda gerçekleşebilir; bu durum da mahremiyetin bireysel özerklikle doğrudan bağlantılı bir kontrol mekanizması olduğunu ortaya koymaktadır. Westin'in yaklaşımı, özellikle bilgi teknolojilerinin yükselişiyle birlikte, mahremiyetin giderek veri odaklı ve kontrol temelli bir biçimde tanımlanmasına öncülük etmiştir.

Bu teorik çerçeveyi izleyen Jan Holvast, Westin'in bireysel özerklik ve kontrol vurgusunu esas alarak mahremiyeti yalnızca hukuki bir hak değil, aynı zamanda toplumsal ve siyasal bağlamda şekillenen, bireyin evi, bedeni ve kişisel verileri üzerindeki kendi kaderini tayin hakkını içeren dinamik bir kavram olarak ele alır (Holvast 2009: 16). Holvast, mahremiyetin iki temel boyutuna dikkat çeker: *ilişkisel mahremiyet (relational privacy)* ve *bilgisel mahremiyet (informational privacy)*. İlişkisel mahremiyet, bireyin fiziksel ve sosyal çevresinde kimlerin hangi koşullarda bulunabileceğine dair kontrolünü ifade ederken; bilgisel mahremiyet, kişisel verilerin toplanması, saklanması ve işlenmesi süreçlerinde bireyin denetimini kapsar (2009: 28). Mahremiyetin bu iki boyutun merkezinde ise kontrol ve öz-belirlenim kavramları yer almaktadır. Holvast'ın çalışmasında, mahremiyetin işlevleri de Westin'in dört işlev modelinden (kişisel özerklik, duygusal rahatlama, kendini değerlendirme ve karar verme, sınırlı ve korunan iletişim (Westin 1967: 330-38) yola çıkarak ele alınır ve bilgi toplumunda bu işlevlerin nasıl tehdit altına girdiği tartışılır (Holvast 2009: 17). Özellikle bilgi teknolojilerinin ve gözetim araçlarının yaygınlaşmasıyla mahremiyetin yalnızca bireysel bir hak olmaktan çıkıp toplumsal güç ilişkileri ve demokratik denetim mekanizmaları açısından da kritik bir meseleye dönüştüğü ortaya konulur (2009: 37-39).

Westin'in teorik çerçevesi, Ruth Gavison'un mahremiyet analizleriyle de desteklenmiştir. Ruth Gavison (1980: 428-29), mahremiyetin yalnızca bilgi akışına ilişkin değil, aynı zamanda fiziksel ve sosyal düzeyde de ele alınması gerektiğini ileri sürer. Ona göre mahremiyet, üç temel unsurdan oluşur: *gizlilik (information secrecy)*, *yalnızlık (solitude)* ve *anonimlik (anonymity)*. Bu unsurlar, bireyin hem özel alanda görünmez olma hakkını hem de kamusal alanda tanınmaz kalma hakkını içerir. Gavison'un analizi, mahremiyetin çok katmanlı bir kavram olduğunu ve yalnızca bireysel özerkliği değil, aynı zamanda bireyin toplumsal ilişkiler içerisindeki konumunu da düzenlediğini gösterir.

Tüm bu kuramsal yaklaşımlar, mahremiyetin doğasının yalnızca bireyin bilgi üzerindeki mülkiyet hakkına ya da fiziksel alanına indirgenemeyeceğini; aksine etik, toplumsal, ilişkisel

ve Giddens’da görüldüğü gibi duygusal boyutları içeren çok katmanlı bir yapıya sahip olduğunu ortaya koymaktadır. Bu bağlamda mahremiyet hem bireysel özerkliğin sürdürülebilmesi hem de toplumsal normların işlerliğini sağlayan bir ara düzlem olarak konumlanır. Bu kavramsal zemin, dijital teknolojilerle birlikte dönüşen mahremiyet anlayışının sınırlarını tartışmak için gerekli kurucu çerçeveyi sunmaktadır. Ne var ki, bu geleneksel yaklaşımlar mahremiyeti hâlâ çoğunlukla bireysel özerklik, özel yaşamın korunması ve toplumsal normlara uygunluk gibi temalar üzerinden yapılandırmaktadır. Günümüzde dijitalleşmenin etkisiyle mahremiyetin sınırları giderek daha da belirsizleşmekte; dijital teknolojideki hızlı dönüşümler, mahremiyeti sabit bir kavram olmaktan çıkarak, sürekli yeniden tanımlanan ve toplumsal olarak müzakere edilmesi gereken dinamik bir olguya dönüştürmektedir.

Günümüzde mahremiyet, yalnızca birey ile toplum arasındaki ilişkisel bir mesele olmaktan çıkmış; aynı zamanda teknolojik altyapılar, platform mimarileri ve küresel veri ekonomileri tarafından şekillenen çok katmanlı bir sosyo-politik mesele haline gelmiştir. Bu dönüşüm en açık biçimde sosyal medya platformlarında görülmektedir. Söz konusu platformlar, kullanıcıların dijital izlerini sistematik bir biçimde toplayarak yalnızca çevrimiçi davranışları kaydetmekle kalmaz; aynı zamanda bu verileri makine öğrenimi ve yapay zekâ algoritmaları aracılığıyla analiz eder. Bu analizler sonucunda, kullanıcılar çoğu zaman farkında dahi olmadıkları öngörülen profilleme süreçlerine dâhil edilir. Böylelikle bireyin kimliği, tercihleri ve sosyal ilişkileri dijital ortamda yeniden kurgulanır (Boyd 2014: 33).

Bu dönüşümün anlaşılabilmesi için sosyal medya platformlarının veri toplama biçimleri ve türleri üzerinde durmak gerekir. Temelde iki tür veri toplama yöntemi bulunmaktadır: aktif ve pasif veri toplama. Aktif veri toplama, kullanıcının doğrudan ve kendi rızasıyla sunduğu bilgileri kapsar; örneğin paylaşımlar, beğeniler, konum bildirimleri, mesaj içerikleri ve profil düzenlemeleri. Bu veriler genellikle kullanıcı deneyimini kişiselleştirme amacıyla toplandığı iddiasıyla meşrulaştırılır. Öte yandan pasif veri toplama, kullanıcıların bilgisi ve çoğunlukla rızası dışında gerçekleşir. Cihaz bilgileri, IP adresleri, ekran süresi, çerezler, tıklama geçmişi gibi birçok detay otomatik olarak sistemler tarafından kaydedilir (Tufekci 2015). Bu pasif veriler, gelişmiş algoritmalar sayesinde bireylerin zihinsel eğilimlerini ve duygusal durumlarını tahmin eden detaylı profillere dönüştürülür. David Kosinski, Michal Stillwell ve Thore Graepel’in (2013) araştırması, sadece Facebook beğenileriyle bir bireyin cinsiyeti, dini inancı, politik eğilimleri ve hatta zekâ düzeyi gibi özelliklerinin yüksek doğrulukla tahmin edilebildiğini göstermiştir. Bu çalışma, 58.000’den fazla Facebook kullanıcısının beğenileri ve psikometrik test sonuçları üzerinden gerçekleştirilmiştir. Model, örneğin bireylerin cinsel

yönelimini %88, etnik kökenini %95 ve politik görüşünü %85 doğrulukla tahmin edebilmiştir. Bu da dijital izlerin yalnızca yüzeysel veri parçaları olmadığını, aksine bireyin iç dünyasına dair güçlü bir şeffaflık yarattığını ortaya koymaktadır.

Bu gelişmelerin en sorunlu yönlerinden biri, görünüşte “rıza” temelinde işleyen veri toplama süreçlerinin, gerçekte içerik ve bağlam açısından ciddi şekilde sorgulanabilir olmasıdır. Dijital ortamda kişisel verilerin toplanması için *bilgilendirilmiş rıza (informed consent)* ilkesine uygun hareket edilmesi gerektiği kabul edilir; yani birey, yeterli bilgiye sahip olarak ve özgür iradesiyle onay vermelidir. Ancak bu ideal çoğu zaman gerçekleşmez. Kullanıcılar genellikle uzun ve teknik terimlerle yazılmış gizlilik politikalarını okumadan kabul ederler. Aleecia McDonald ve Lorrie Faith Cranor’un (2008) yaptığı araştırma, ortalama bir kullanıcının tüm ziyaret ettiği web sitelerinin gizlilik politikalarını okuyup anlaması için yılda yaklaşık 244 saat harcaması gerektiğini ortaya koymuştur. Bu durum, kullanıcının bilinçli bir tercih yaptığı izlenimini yaratsa da aslında bir “rıza yanılsaması” üretir. Bunun yanı sıra dijital platformlar, kullanıcıları daha fazla veri paylaşmaya yönlendirmek amacıyla *karanlık desenler (dark patterns)* adı verilen tasarım stratejilerini kullanmaktadır. Bu stratejiler, kullanıcı davranışlarını yönlendirecek şekilde gizlilik ayarlarını zor erişilir hale getirir, veri paylaşımını varsayılan olarak açık bırakır veya manipülatif onay kutuları sunar. Arunesh Mathur ve arkadaşlarının (2019) çalışması, 11.000 alışveriş sitesinde 1.818 farklı karanlık desen örneği tespit etmiş ve bu desenlerin kullanıcıları yanıltıcı biçimde yönlendirdiğini göstermiştir. Bu da bireyin verileri üzerindeki kontrolünün büyük ölçüde şeklen kaldığını gösterir.

Mahremiyetin ihlalini sadece izinsiz veri sızıntılarına indirgemek de dijital ortamın dinamiklerini tam olarak kavramayı engeller. Helen Nissenbaum’un (2011: 37-8) ortaya koyduğu *bağlamsal bütünlük (contextual integrity)* teorisi, mahremiyetin sosyal normlara ve bağlamsal beklentilere dayandığını savunur. Bu kuramsal çerçeve doğrultusunda, bireyler belirli sosyal bağlamlar içinde veri paylaşımında bulunabilir; ancak bu verilerin, bireyin bilgisi ve onayı dışında başka bir bağlama taşınması mahremiyetin ihlali anlamına gelir. Örneğin, bir kullanıcı yalnızca arkadaş çevresiyle paylaşma niyetiyle bir tatil fotoğrafını sosyal medyaya yüklemiş olabilir. Ancak bu içerik, platform tarafından konum verisi çıkarımı, davranış analizi veya hedefli reklamcılık için kullanılabilir. Böylece veri, kullanıcının öngördüğü bağlamdan çıkarılarak farklı bir anlam ve amaçla kullanılmış olur. Platform tasarımları genellikle bu bağlamsal geçişleri fark edilmeden mümkün kılacak şekilde inşa edilir. Bu durum, bireyin içerik üzerindeki kontrolünü kaybetmesine neden olur. Dolayısıyla dijital mahremiyetin korunması yalnızca teknik güvenlik önlemlerine indirgenemez; bağlamsal ilişkilerin şeffaf ve

etik biçimde tasarlanması da gereklidir. Aksi halde kullanıcı, verilerinin kimler tarafından, nasıl ve ne amaçla kullanıldığını denetleyemez hale gelir. Bu bütünsel yapısıyla dijital mahremiyet, bireysel hakların ötesinde, teknolojik altyapılar, tasarım stratejileri ve veri politikaları ekseninde şekillenen çok boyutlu bir meseledir. Her bir unsur, bireyin dijital dünyadaki görünürlüğünü ve özerkliğini doğrudan etkileyen karmaşık bir dengeyi ortaya koyar. Bu nedenle dijital mahremiyet hem bireysel farkındalıkla hem de sistemsel reformlarla yeniden tanımlanmayı bekleyen bir kavramdır.

Mahremiyetin Ticarileştirilme Mekanizmaları

Sosyal medya platformlarının "ücretsiz" hizmet sunduğu iddiası, gerçekte kullanıcıların dikkatini ve verisini merkeze alan, karmaşık ve güçlü bir ekonomik modelin parçasıdır. Bu yapı, Shoshana Zuboff'un *gözetim kapitalizmi (surveillance capitalism)* olarak tanımladığı sistemle açıklanabilir. Bu modele göre kullanıcılar tüketici değil, doğrudan ekonomik faaliyetin nesnesi hâline gelir; bireylerin dijital davranışları, tercihleri ve etkileşim örüntüleri sistematik biçimde toplanır, işlenir ve üçüncü taraflara satılarak ekonomik değere dönüştürülür (2019: 92-7). Mahremiyet bu bağlamda yalnızca bireysel bir hak olmaktan çıkar, dijital ekonominin asli girdilerinden biri hâline gelir; meta olarak dolaşıma girer, platform ekonomilerinin temel sermayesine dönüşür.

Bu ticarileştirme süreci temelde üç ana mekanizma üzerinden işler: veri toplama, psikometrik profillem ve hedefli yönlendirme. Kullanıcıların açık (paylaşımlar, beğeniler) ve örtük (tıklamalar, gezinme davranışları, okuma süreleri) verileri, makine öğrenimi algoritmaları aracılığıyla analiz edilerek, bireylere ait ayrıntılı psikometrik profiller oluşturulmaktadır. Nitekim Kosinski ve arkadaşlarının (2013) çalışmasında da gösterildiği üzere, yalnızca Facebook beğenilerine dayanarak bireylerin cinsel yönelimi, politik eğilimleri, zekâ düzeyi ve dini inançları gibi son derece hassas kişisel özellikleri yüksek doğruluk oranlarıyla tahmin edilebilmektedir. Bu çerçevede, Netflix'in öneri algoritması da dikkat çekici bir örnek teşkil eder. Platform, kullanıcıların izleme geçmişini yalnızca içerik tercihlerini belirlemek için değil; aynı zamanda ruh hâli, sosyal eğilimler ve karar alma kalıpları gibi daha derin psikolojik boyutları tahmin etmek amacıyla da kullanılmaktadır (Gomez-Urbe ve Hunt 2015: 27). Bu tür çıkarımlar, yalnızca kişiselleştirilmiş reklamcılık alanında değil; siyasal yönlendirme ve kamuoyu manipülasyonu gibi daha geniş ölçekli stratejik hedeflerde de kullanılmaktadır. *Cambridge Analytica* skandalı, bireylerin rızası dışında elde edilen verilerin demokratik süreçler üzerindeki etkisini çarpıcı bir biçimde ortaya koymuş; dijital mahremiyetin yalnızca

bireysel değil, aynı zamanda kolektif bir tehdit alanı oluşturduğunu gözler önüne sermiştir (Cadwalladr ve Graham-Harrison 2018).

Verinin ticarileştirilmesi yalnızca içerik hedefleme ile sınırlı kalmayıp, kullanıcı davranışlarını yönlendirme kapasitesine sahip algoritmik müdahale stratejilerini de içermektedir. Sosyal medya platformları, kullanıcıların dijital ortamda daha uzun süre kalmasını sağlamak amacıyla algoritmik içerik düzenlemeleri kullanmaktadır. Bu algoritmalar, kullanıcıların ilgi alanlarına uyum sağlamakla kalmayıp, zamanla bu ilgileri biçimlendiren, yönlendiren ve daraltan bir işlev üstlenmektedir. İçerikler, rastlantısal değil; yüksek dikkat çeken, duygusal tepkiler yaratan ve maksimum etkileşim üretecek biçimde seçilmektedir (Eubanks 2018). Bu sayede platform, kullanıcıya özerklik hissi verirken, aslında onun davranışlarını manipülatif biçimde yönlendirmektedir. Bu durum, algoritmik yönlendirme yoluyla özerklik yanılsamasının yeniden üretimidir ve bu mekanizma, toplumsal kutuplaşmayı pekiştiren *yankı odaları (the echo chamber)* yaratmaktadır (Del Vicario vd. 2016; Gillespie 2018; Cinelli vd. 2020).

Kişisel verilerin bu denli ekonomik değere sahip olması, dijital eşitsizliği ve platformlar arasındaki güç asimetrisini derinleştirir. Meta, Google gibi şirketler yalnızca reklam gelirlerinden yüz milyarlarca dolar kazanmakla kalmamakta; aynı zamanda bu gelirin oluşmasında temel kaynak olan kullanıcıları ekonomik yapının pasif nesneleri olarak konumlandırmaktadır. Posner ve Weyl (2018), kapitalizmin bu asimetrik yapısına çözüm olarak bir *gelir paylaşımı modeli* önermektedir. Bu model çerçevesinde, kullanıcıların ürettikleri verinin ekonomik çıktısından pay almaları gerekmektedir; böylece veri odaklı ekonomi daha adil, simetrik ve katılımcı bir zemine oturtulabilir. Lanier'in de (2013) önerdiği bu yaklaşım esasen mahremiyetin ihlalini engellemekten ziyade, mahremiyetin ekonomik değerini tanıyarak bireyi veri üzerinde hak sahibi bir özne olarak konumlandırmayı hedeflemektedir. Dijital ekonomi kullanıcılar için yalnızca bir tüketim alanı olmanın ötesine geçerek, aynı zamanda değer yaratan aktif bir platforma dönüşme potansiyeline sahiptir.

Bu bölümün analizi, mahremiyetin ticarileşmesi sorununun yalnızca bireysel hak ihlali ya da teknik bir mesele olarak değil; aynı zamanda dijital çağın etik, ekonomik ve politik gerilimlerinin düğümlendiği çok katmanlı bir yapısal olgu olarak görülmesi gerektiğini göstermiştir. Bu çerçevede, mahremiyetin korunması yalnızca yasal düzenlemelerle değil, veri üretiminin bir tür emek olarak tanınması ve bu emeğin karşılığının verilmesi bağlamında ekonomik adaletin sağlanması; kullanıcıların hangi verilerinin toplandığını, bu verilerin nasıl işlendiğini, kimlerle paylaşıldığını ve ne süreyle saklandığını açık ve anlaşılır bir biçimde

öğrenebilmesi temelinde şeffaf veri politikalarının uygulanması; ve kararların toplumsal etkilerine dair bağımsız denetim mekanizmalarının devreye girmesini bağlamında algoritmik süreçlerin kamu denetimine açık hâle getirilmesiyle mümkün olabildiği görülmüştür. Aksi takdirde, dijital öznellik giderek görünürlük, yönlendirme ve veri üretimiyle tanımlanan bir gözetim nesnesine indirgenecek; birey, yalnızca dijital ekonominin değil, dijital ideolojinin de yeniden ürettiği bir araç hâline gelecektir.

Veri Güvenliği Sorunları

Sosyal medya platformlarında mahremiyetin ticarileştirilmesi, sadece etik ve hukuki bir problem alanı olarak kalmamakta, aynı zamanda kullanıcıların kişisel verilerinin güvenliğine yönelik ciddi ve çok boyutlu tehditler doğurmaktadır. Bu platformların büyük ölçekli veri toplama altyapıları, kullanıcı bilgilerini hem içsel sistem açıkları hem de dış kaynaklı tehdit aktörleri karşısında savunmasız hâle getirmektedir. Böylece veri güvenliği, yalnızca bireysel tedbirlerle yönetilebilecek bir mesele olmaktan çıkarak; teknik mimariler, kurumsal sorumluluklar ve ulusötesi hukuki rejimlerle doğrudan ilişkili karmaşık bir yapıya dönüşmektedir. Özellikle platform altyapılarındaki zaaflar, kullanıcı farkındalığının düşüklüğü ve küresel ölçekte veri dolaşımı, mahremiyet haklarını yapısal düzeyde zayıflatan başlıca etkenler arasında yer almaktadır.

Geçmişte yaşanan çok sayıda yüksek profilli veri ihlali, platformların güvenlik politikalarındaki eksiklikleri açık biçimde ortaya koymuştur. 2019 yılında Facebook'un milyonlarca kullanıcıya ait telefon numarasını şifresiz olarak halka açık bir sunucuda depoladığı ifşa edilmiş; bu durum platformun veri koruma önlemlerini ihmal ettiğini göstermiştir (BBC News 2019). Benzer biçimde, LinkedIn, Twitter ve TikTok gibi platformlar da çeşitli zamanlarda büyük çaplı veri sızıntıları yaşamıştır. Bu ihlaller genellikle zayıf kimlik doğrulama sistemleri, denetlenmeyen üçüncü taraf API'ler, merkezî sunucu yapılarında tek hata noktası oluşturulması ve kullanıcı verilerinin ticari önceliklerle yönetilmesi gibi sistemik eksikliklerden kaynaklanmaktadır. Dijital altyapıların çoğu, veri güvenliğini değil, operasyonel verimlilik ve kurumsal çıkarları önceleyen bir mantıkla tasarlanmıştır (Ohm 2009). Bu nedenle güvenlik önlemleri çoğunlukla reaktif kalmakta; ihlaller gerçekleşmeden önce değil, ancak kamuoyu baskısıyla sonrasında hayata geçirilmektedir.

Kullanıcı tarafında ise dijital okuryazarlık düzeyindeki düşüklük, bu güvenlik açıklarının etkisini derinleştirmektedir. Çoğu kullanıcı, platformların verileri nasıl topladığını, nerede ve nasıl sakladığını ya da kimlerle paylaştığını bilmemektedir. McDonald ve Cranor'un

(2008) bulguları, kullanıcıların çok azının gizlilik politikalarını okuduğunu, okuyanların ise çoğunlukla bu belgeleri anlayamadığını ortaya koymaktadır. Ayrıca birçok kullanıcı, bir içeriği sildiğinde bunun tamamen sistemden kaldırıldığını varsaymakta; oysa pek çok platform verileri yalnızca görünürlükten kaldırmakta, arka planda saklamaya ya da anonimleştirerek analiz etmeye devam etmektedir. Kullanıcı tarafında dijital okuryazarlık düzeyinin düşük olması, güvenlik açıklarının etkisini daha da derinleştirmektedir. Birçok kullanıcı, dijital platformların verileri nasıl topladığı, sakladığı ya da kimlerle paylaştığı konusunda yeterli bilgiye sahip değildir. Yapılan araştırmalar, kullanıcıların büyük kısmının gizlilik politikalarını okumadığını; okuyanların ise bu belgeleri anlamakta zorlandığını ortaya koymaktadır. Ayrıca kullanıcıların önemli bir bölümü, bir içeriği sildiklerinde bunun sistemden tamamen kaldırıldığını düşünmektedir. Oysa çoğu platform bu verileri yalnızca görünürlükten kaldırmakta; arka planda saklamaya ya da anonimleştirerek işlemeye devam etmektedir. Anonimleştirmenin her zaman tam bir gizlilik sağlamadığı ise çeşitli çalışmalarla ortaya konmuştur. Ohm'un (2009) çalışması da bunu desteklemekte ve gelişmiş analiz teknikleriyle anonimleştirilmiş veriler üzerinden dahi bireylerin kimliklerinin yeniden belirlenebileceğini ortaya koymaktadır. Bu durum, kullanıcıların verileri üzerindeki denetim hissinin büyük ölçüde yanıltıcı olduğunu göstermektedir.

Veri güvenliği sorunları, dijital alanın ulusötesi doğası nedeniyle yalnızca bireysel değil, aynı zamanda hukuki düzeyde de belirsizlik üretmektedir. Sosyal medya platformları küresel olarak faaliyet gösterdiğinden, veriler bir ülkede toplanıp başka bir ülkede işlenebilmektedir. Bu güvenlik tehditlerinden en fazla etkilenenler, toplumsal olarak kırılgan gruplardır. Politik muhalifler, etnik ve dini azınlıklar gibi gruplar için veri sızıntıları yalnızca mahremiyet ihlali değil, aynı zamanda fiziksel ve psikolojik güvenliği tehdit eden bir durumdur. Bu grupların hassas bilgilerinin açığa çıkması; dışlanma, ayrımcılık, taciz ve hatta şiddetle sonuçlanabilecek süreçleri tetikleyebilmektedir.

Bu bölüm analizi çerçevesinde görülmektedir ki; gözetim teknolojileri nötr değildir; anonimleşmiş veriler üzerinden yeni kimlikler üretebildiği gibi mevcut toplumsal eşitsizlikleri de yeniden üretebilmekte ve bazı grupları orantısız biçimde hedef hâline getirebilmektedir (Lyon 2018; Eubanks 2018; Noble 2018). Ne var ki sosyal medya platformlarının bu konuda özel koruma mekanizmaları geliştirmede yetersiz kaldığı; karmaşık gizlilik ayarları, ayrımcı eğilimler taşıyan otomatik filtreleme sistemleri ve yetersiz kullanıcı destek süreçleriyle bu dezavantajları derinleştirdiği görülmektedir.

Etik ve Toplumsal Sorunlar

Sosyal medya platformlarında mahremiyetin metalaştırılması, yalnızca bireysel gizlilik haklarını zedeleyen bir uygulama değil, aynı zamanda dijital çağın toplumsal dönüşümünü biçimlendiren köklü bir yapısal değişimin parçasıdır. Kişisel verilerin ekonomik birer kaynak olarak görülmesiyle birlikte, kullanıcılar artık sadece içerik üreticileri değil; algoritmik sistemler tarafından izlenen, analiz edilen ve yönlendirilen dijital özneler hâline gelmektedir. Bu dönüşüm, bireysel özerkliğin aşınmasından kamusal güvenin erozyonuna, güç ilişkilerinin yeniden yapılandırılmasından demokratik süreçlerin zayıflamasına kadar çok katmanlı ve kalıcı etkiler üretmektedir. Mahremiyetin bu biçimde ticarileştirilmesi, yalnızca teknik ya da hukuki bir mesele değil; doğrudan ahlaki sorumluluğa, toplumsal eşitliğe ve kamusal etik yapının sürdürülebilirliğine temas eden çok boyutlu bir sorundur.

Bu süreç birey üzerinde en doğrudan etkisini, karar alma özerkliğinin zayıflaması biçiminde göstermektedir. Platformlar görünürde “açık rıza”ya dayansa da, bu rıza çoğunlukla teknik dil içeren sözleşmeler, manipülatif arayüz tasarımları ve sınırlı bilgi sunumu üzerinden yapılandırılmakta; böylece kullanıcılar gerçek anlamda bilgilendirilmiş bir onam süreci yaşamadan veri paylaşımına zorlanmaktadır. Barocas ve Nissenbaum’un (2014: 32) vurguladığı gibi, bilgi eşitsizliği ve sistem karmaşıklığı, kullanıcıyı bilinçli bir seçim yapma kapasitesinden mahrum bırakır. Solove (2013: 1883-85), bu durumu mahremiyetin yönetilebilirliğinin çöküşü olarak görür; birey, verisi üzerindeki kontrolü yalnızca sembolik düzeyde sürdürebilir. Böylece rıza, kullanıcıyı özne olarak güçlendiren bir hak olmaktan çıkıp, veri toplamanın prosedürel gerekçesi hâline gelir.

Mahremiyetin metalaştırılması süreci, yalnızca bireysel özerkliği değil, aynı zamanda gözetimin toplumsal ölçekte içselleştirilmesini de beraberinde getirir. Lyon’un (2018: 12) *gözetim kültürü (surveillance culture)* olarak tanımladığı bu yapı, bireyin sürekli izlendiği algısıyla kendi davranışlarını otomatik olarak denetlemesine, düzenlemesine ve uyarlamasına neden olur. Foucault’nun (1977: 201) panoptikon metaforunda olduğu gibi, dışsal denetime gerek kalmadan, birey kendi üzerindeki gözetimi içselleştirir ve davranışlarını normatif çerçevede biçimlendirir. Bu durum, dijital öznenin kimliğini sürekli optimize etme çabası içinde olmasıyla sonuçlanır; görünürlük baskısı, otosansürü tetikler ve psikolojik iyi oluş üzerinde olumsuz etkilere yol açar.

Bu dönüşüm aynı zamanda derin sosyoekonomik eşitsizlikleri yeniden üretir. Dijital okuryazarlığı yüksek, teknik bilgiye ve kaynaklara erişimi olan bireyler veri sömürüsüne karşı

daha dirençli iken; düşük gelirli, eğitime sınırlı erişimi olan veya teknolojik araçlardan yoksun gruplar, mahremiyet ihlallerine karşı daha savunmasızdır. Cohen (2012: 193), mahremiyetin giderek evrensel bir hak olmaktan çıkıp, sınıfsal ve kültürel sermaye ile orantılı bir ayrıcalığa dönüştüğünü savunur. Bu bağlamda, veri üzerinden kurulan gözetim ve yönlendirme mekanizmaları, sadece bireysel mahremiyeti değil, toplumsal adaleti ve eşitliği de tehdit eder hâle gelmektedir.

Ticarileşen mahremiyetin bir diğer yapısal etkisi, toplumsal güvenin erozyona uğramasıdır. Verilerin rıza dışı kullanımı ve siyasi manipülasyon aracı hâline gelmesi, kullanıcıların yalnızca platformlara değil; daha geniş anlamda demokratik kurumlara ve bilgi sistemlerine olan güvenini de zayıflatmaktadır. Cambridge Analytica skandalı, mahremiyet ihlallerinin seçim süreçlerine müdahale potansiyelini göstermiş; etik ihlallerin demokratik meşruiyet üzerindeki yıkıcı etkisini somutlaştırmıştır (Cadwalladr ve Graham-Harrison 2018). Öte yandan, dijital platformların algoritmik içerik sunum sistemleri, kullanıcıları benzer görüşlerin sürekli tekrarlandığı yankı odalarına ve filtre balonlarına hapseder (Pariser 2011). Bu durum yalnızca bilgi çeşitliliğini sınırlamakla kalmaz, aynı zamanda daha önce de vurgulandığı üzere toplumsal kutuplaşmayı derinleştirir. Ortak bir kamusal alanın inşası zorlaşırken, demokratik iletişimin temel koşulları da aşınmaya başlar.

Son tahlilde, mahremiyetin metalaşması, teknik bir uygulamanın çok ötesinde, dijital çağın öznesini, toplumunu ve değer sistemlerini dönüştüren karmaşık ve çok katmanlı bir yapısal dönüşümdür. Bireysel özerkliğin çözülmesi, gözetimin içselleştirilmesi, güç eşitsizliklerinin derinleşmesi ve kamusal güvenin zedelenmesi, bu sürecin bütüncül sonuçlarıdır. Bu nedenle, mahremiyetin korunması yalnızca bireysel farkındalık ya da teknik çözümlerle değil; dijital etik ilkelerin platform politikalarına entegre edilmesi, dijital eşitliği gözetim yasas düzenlemeler ve kültürel bilinçle desteklenen sistemsel dönüşümler aracılığıyla mümkündür.

Uluslararası ve Ulusal Düzenlemeler

Sosyal medya platformlarının kullanıcı mahremiyetini sistematik biçimde ticarileştirmesi, yalnızca bireyler açısından değil; hukukçular, akademisyenler ve politika yapıcılar açısından da giderek büyüyen bir endişe kaynağı haline gelmiştir. Kullanıcı verilerinin izinsiz ya da bilgilendirilmemiş şekilde toplanması, işlenmesi ve ekonomik kazanca dönüştürülmesi, dijital çağda mahremiyetin ve veri güvenliğinin korunmasını küresel bir sorun haline getirmiştir. Bu kapsamda, son on yıl içinde kişisel verilerin korunmasına yönelik uluslararası ve ulusal düzeyde

çeşitli hukuki ve politik düzenlemeler yürürlüğe konulmuştur. Ancak bu düzenlemeler, çoğu zaman mevcut dijital ekonomik sistemin işleyiş mantığını dönüştürmekten uzak kalmakta; uygulama ve denetim süreçlerindeki yapısal zaaflar nedeniyle eleştirilere konu olmaktadır.

Avrupa Birliği tarafından 2018 yılında yürürlüğe giren *Genel Veri Koruma Tüzüğü* (*General Data Protection Regulation - GDPR*), dijital mahremiyetin korunmasına yönelik en kapsamlı ve bağlayıcı uluslararası düzenlemelerden biri olarak kabul edilmektedir. Tüzük, veri işleme süreçlerinde açık rıza, veri minimizasyonu, unutulma hakkı ve veri taşınabilirliği gibi ilkeleri esas alarak bireylerin verileri üzerindeki kontrolünü artırmayı hedeflemektedir (GDPR 2018, Madde 5–20). Buna göre kullanıcılar, hangi verilerinin toplandığına dair bilgi alma, bu verilerin nasıl işlendiğini öğrenme ve dilediklerinde bu verilerin silinmesini ya da taşınmasını talep etme hakkına sahiptir. Ancak GDPR'nin uygulanmasında karşılaşılan en temel sorun, özellikle küresel teknoloji şirketlerinin (örneğin Meta, Google, TikTok) bu düzenlemelere biçimsel olarak uyarken, özde veri sömürüsü pratiklerini sürdürmesidir. Bu durum, kullanıcıları rızaya dayalı veri paylaşımına zorlayan karanlık desenler gibi manipülatif arayüz tasarımlarının hâlâ yaygın biçimde kullanılmasıyla açıkça görülmektedir (Gray vd. 2018).

Benzer biçimde, ABD’de yürürlüğe giren *California Tüketici Gizliliği Yasası* (*California Consumer Privacy Act - CCPA*), bireylere verilerine erişim, bu verilerin silinmesini talep etme ve verilerinin üçüncü taraflara satılmasını engelleme gibi haklar tanımaktadır. Ancak CCPA da tıpkı GDPR gibi uygulama aşamasında zayıf denetim mekanizmalarıyla karşı karşıyadır ve ulusal düzeyde bir veri koruma yasasının eksikliği nedeniyle parçalı bir etki yaratmaktadır. Ayrıca hem GDPR hem CCPA gibi düzenlemeler, ağırlıklı olarak bireysel haklara odaklandıkları için dijital mahremiyetin kolektif boyutunu yeterince kapsayamamaktadır. Nitekim kuramsal ve kavramsal incelemelerin de gösterdiği üzere, mahremiyetin ihlali yalnızca bireysel bir hak kaybı değil; aynı zamanda algoritmik manipülasyonlar, hedefli siyasi kampanyalar ve toplum mühendisliği gibi geniş ölçekli toplumsal sonuçlar doğuran bir süreçtir.

Artan kamuoyu baskısı karşısında sosyal medya platformları da çeşitli öz düzenleme girişimlerinde bulunmuştur. Meta’nın sunduğu “gizlilik kontrol araçları”, Google’ın yayımladığı “şeffaflık raporları” ya da X’in (Twitter) kurduğu “güvenlik merkezleri”, bu çabaların örnekleridir. Ancak bu girişimler çoğu zaman kamuoyunu yatıştırmaya ve kurumsal itibar yönetimini sürdürmeye yönelik sembolik adımlar olarak değerlendirilmektedir. Gillespie’nin (2018: 104) dikkat çektiği üzere, platformların kendi etik ilkelerini belirlemesi, özdenetim mekanizmalarının işlevselliğini sınırlamakta ve kamu otoritelerinin bağımsız

denetimini zayıflatmaktadır. Böylece şirketler, şeffaflık ve hesap verebilirlik gibi ilkeleri kendi çıkarlarına uyacak biçimde esnetebilmekte; kullanıcı mahremiyetinin gerçek anlamda korunması ise retorik düzeyde kalmaktadır. Bu çerçevede, Avrupa Birliği'nin dijital alanı daha sıkı bir şekilde denetlemeyi amaçlayan *Yapay Zekâ Yasası (AI Act)*, platformların öz düzenleme çabalarının ötesine geçerek kamu otoriteleri eliyle hesap verebilirliği kurumsallaştırmayı hedeflemektedir (European Commission 2024a). 1 Ağustos 2024'te yürürlüğe giren bu yasa, kademeli olarak uygulanmaya başlanmıştır. 2 Şubat 2025 itibarıyla, “kabul edilemez risk” taşıyan yapay zekâ uygulamaları yasaklanmış; bireyleri manipüle eden, duygusal durumları analiz eden sistemler ile sosyal puanlama gibi uygulamalar yasadışı ilan edilmiştir (European Commission 2024b). Aynı tarihte, yapay zekâ okuryazarlığına ilişkin yükümlülükler de devreye girmiştir. 2 Ağustos 2025'te ise genel amaçlı yapay zekâ sistemlerine—örneğin ChatGPT benzeri modeller—yönelik düzenlemeler yürürlüğe girecek; bu düzenlemeler kapsamında şeffaflık, telif hakkı uyumu ve insan denetimi gibi yükümlülükler öngörülmektedir. Yasaya tam uyum sürecinin ise 2026 ve 2027 yıllarında tamamlanması öngörülmektedir (European Commission 2024a). Bu gelişmeler, platformların kendi belirlediği etik ilkelerle sınırlı kalan özdenetim çabalarının yetersizliğini ortaya koymakta; kamusal denetimin gerekliliğini daha da görünür kılmaktadır.

Türkiye'de de dijital mahremiyetin ticarileştirilmesi ve veri güvenliği konuları, son yıllarda artan kamuoyu farkındalığı ve küresel regülasyonlara uyum çabaları çerçevesinde gündeme taşınmıştır. Türkiye'de bu alandaki temel yasal düzenleme, 2016 yılında yürürlüğe giren 6698 sayılı *Kişisel Verilerin Korunması Kanunudur (KVKK)*. Avrupa Birliği'nin GDPR'si temel alınarak hazırlanan bu yasa, veri sorumlularına aydınlatma yükümlülüğü, veri minimizasyonu ve veri sahibinin açık rızasını alma gibi ilkeler doğrultusunda sorumluluklar yüklemektedir. Kanun, bireylere verilerinin işlenip işlenmediğini öğrenme, yanlış verilerin düzeltilmesini isteme ve verilerin silinmesini ya da anonimleştirilmesini talep etme gibi haklar tanımaktadır. Ancak uygulamada, özellikle uluslararası dijital platformlar söz konusu olduğunda etkin denetim sağlanamadığı; yaptırımların caydırıcılıktan uzak kaldığı yönünde eleştiriler mevcuttur.

Türkiye'deki düzenleyici çabalar yalnızca kişisel verilerin korunması ile sınırlı kalmamış; sosyal medya platformlarının denetimi ve yönlendirilmesi amacıyla daha kapsamlı yasal müdahaleleri de içermiştir. 2020 yılında 5651 sayılı Kanun'da yapılan değişiklikle sosyal ağ sağlayıcılarına Türkiye'de temsilci bulundurma zorunluluğu getirilmiş, içerik kaldırma ve veri paylaşım taleplerine hızlı yanıt verilmesi zorunlu hale getirilmiştir. Bu adım, platformların

yerel otoritelerle daha uyumlu çalışmasını sağlama amacı taşısa da, sansür ve gözetim kaygılarını da beraberinde getirmiştir. 2022 yılında kabul edilen ve kamuoyunda “Dezenformasyon Yasası” olarak bilinen 7418 sayılı yasa ise dijital alanda yanlış bilgiyle mücadele gerekçesiyle kamu düzenini sağlama hedefi taşımaktadır. Ancak bu düzenleme, kullanıcı verilerine erişim yetkilerinin artırılması ve çevrimiçi içerik üzerindeki denetimin yoğunlaşması risklerini de barındırmakta; ifade özgürlüğü ve dijital haklar açısından yeni tartışmalar doğurmaktadır.

Sonuç olarak gerek uluslararası gerek ulusal düzeyde gerçekleştirilen düzenlemeler, dijital mahremiyetin ticarileştirilmesine karşı çeşitli önlemler öngörmekte; ancak platformların ekonomik çıkarları ve teknolojik üstünlüğü karşısında sınırlı etki yaratabilmektedir. Öz düzenleme mekanizmalarının yetersizliği ve denetim kurumlarının bağımsızlığına ilişkin sorunlar, kullanıcıların veri üzerindeki haklarını koruma konusunda ciddi boşluklara işaret etmektedir. Dijital mahremiyetin yalnızca bireysel bir mesele olarak değil, aynı zamanda politik ve kolektif bir mesele olarak ele alınması, daha kapsayıcı bir regülasyon anlayışı geliştirilmesini gerekli kılmaktadır.

Daha Temiz Bir Sosyal Medya Ekosistemi İçin Öneriler

Dijitalleşmenin toplumsal yaşamı kuşattığı çağımızda, sosyal medya platformlarının bireysel mahremiyeti sistematik biçimde ticarileştirmesi hem teknik bir mesele hem de etik, hukuki ve kültürel bir sorunsal olarak karşımıza çıkmaktadır. Her ne kadar bazı hukuki düzenlemeler bu alandaki riskleri dengelemeye yönelik çabalar sunsa da dijital ekosistemin ilerleme hızı karşısında bu çabalar genellikle reaktif, parçalı ve geçici nitelik taşımaktadır. Mahremiyetin bir metaya dönüştürülmesi, yalnızca bireyin özel yaşam alanının sınırlarını değil, aynı zamanda dijital kamu alanının güvenilirliğini, toplumsal ilişkilerin şeffaflığını ve demokratik normların sürdürülebilirliğini de tehdit etmektedir. Bu nedenle, daha etik bir sosyal medya düzeni inşa etmek, sadece teknik düzenlemelerle değil, aynı zamanda kültürel dönüşüm, bireysel bilinçlenme ve kolektif sorumluluk temelinde şekillenen çok katmanlı bir etik mimariyle mümkündür.

Bu dönüşümün ilk adımı, mahremiyetin platformların yapısal tasarımına entegre edilmesini zorunlu kılar. Mahremiyet odaklı tasarım yaklaşım, bireylerin dijital izlerinin sadece gerekli işlevler kapsamında toplanmasını, sistemlerin varsayılan olarak gizlilik koruyucu biçimde yapılandırılmasını ve kullanıcıların kendi verileri üzerinde etkin kontrol sağlamasını hedefler (Cavoukian 2010). Bu yaklaşımın yaşama geçirilmesi, kullanıcı deneyiminin

şeffaflaştırılmasını, karanlık desenlerin ortadan kaldırılmasını, gizlilik ayarlarının daha erişilebilir hale getirilmesini ve kullanıcı onaylarının bağlam duyarlı bir biçimde alınmasını gerektirir. Bu sayede dijital platformlar yalnızca kullanıcı çekmeye değil, kullanıcıyı korumaya dayalı etik bir sorumluluk anlayışı geliştirir.

Ancak etik dönüşüm yalnızca platformların yapısal reformlarıyla sınırlı değildir. Sosyal medya şirketlerinin mevcut işleyişi, gözetim kapitalizminin belirlediği bir paradigma içerisinde kullanıcıların dikkatini ve davranışlarını ekonomik çıktıya dönüştüren bir modele dayalıdır (Zuboff 2019). Bu modelin sürdürülebilir, adil ve demokratik bir dijital yaşamla bağdaşmadığı açıktır. Bu noktada, alternatif ekonomik modellerin geliştirilmesi büyük önem arz eder. Reklamsız ve abonelik tabanlı platformlar, kullanıcıların mahremiyetini önceliklendiren bir yapıda çalışabilirken; platform kooperatifleri (Scholz 2016), dijital alanda kolektif mülkiyet ve demokratik yönetişimi mümkün kılar. Aynı şekilde, kâr amacı gütmeyen dijital kamu hizmetleri, yurttaşların iletişim ve bilgiye erişim hakkını temel alan bir dijital kamu yararını tesis etme potansiyeli taşır. Bu yapılar, kullanıcıların pasif veri nesneleri değil, dijital yurttaşlar olarak konumlandırıldığı yeni bir etik çerçevenin zeminini hazırlar.

Kuşkusuz ki bu dönüşüm, teknik ve ekonomik boyutların ötesinde, bireylerin ve toplumun etik farkındalık düzeyi ile de doğrudan ilişkilidir. Dijital okuryazarlığın güçlendirilmesi ve mahremiyetin bir kültürel değer olarak içselleştirilmesi, etik bir dijital geleceğin en sağlam dayanaklarından biridir. Özellikle genç bireylerin dijital ortamda maruz kaldıkları içeriklere karşı direnç geliştirmeleri, yalnızca teknik bilgi değil, eleştirel düşünme ve etik duyarlılık gibi becerilerle mümkündür (Boyd 2014). Bu bağlamda, eğitim sistemlerinde dijital etik ve mahremiyet konularının yer alması, medya okuryazarlığı programlarının ulusal düzeyde yaygınlaştırılması ve sivil toplum kuruluşlarının bu alanda toplumsal bilinç geliştirme rolünü üstlenmesi elzemdir. Dijital haklara dair açık erişimli kaynakların sağlanması, her yaştan bireyin dijital ortamda etik davranış geliştirmesini destekleyecektir.

Mahremiyetin Ontolojisi ve Dijital Etik: Sosyal Medyada Öznelliğin, Sorumluluğun ve Kamusallığın Yeniden Düşünülmesi

Dijital çağda birey, klasik modernitenin özerk öznesi olmaktan giderek uzaklaşmakta, mahremiyetin ontolojik bir hakikat olmaktan çıkıp algoritmik bir değişken hâline gelmesiyle, öznelliğini yalnızca teknolojik değil, aynı zamanda epistemik ve etik düzeyde de kaybetme riskiyle karşı karşıya kalmaktadır. Bu dönüşüm, yalnızca bireyin veriye indirgenmesiyle ilgili değil; aynı zamanda bilincin, eylemin, duygunun ve ilişkiselliğin –kısacası “insan olanın”–

sistematik bir şekilde araçsallaştırılması anlamına gelmektedir. Sosyal medya platformlarının teknik yapısı, mahremiyeti yalnızca korunması gereken bir özel alan olarak değil, platform ekonomisinin kurucu ögesi olan bir sömürü nesnesi olarak konumlandırmakta; bu da dijital özneyi özgürlük yanılsamasıyla kuşatılmış bir gözetim döngüsüne hapsedmektedir. Burada Kant'ın insanı hiçbir zaman yalnızca bir araç olarak değil, aynı zamanda daima bir amaç olarak görme buyruğu (1997: 38) açıkça ihlal edilmekte; dijital öznellik, insanın kendi rızasına rağmen pazarlanabilir davranış kalıplarına dönüştürülmektedir.

Bu noktada, mahremiyetin kaybı yalnızca bireyin özel alanına yönelik bir ihlal değil, aynı zamanda Arendt'in (1958: 52) *ortak dünya (the common world)* olarak tanımladığı ortak varlık alanının da aşındırılması anlamına gelir. Zira kamusal olan ile özel olan arasındaki sınırın silinmesi, yalnızca görünürlüğün artması değil; eylemin, düşüncenin ve birlikte yaşama etiğinin anlamını kaybetmesiyle sonuçlanır. Dijital platformlarda sürekli "görünür olma" zorunluluğu, Arendt'in özgür eylem nosyonunu olanaksız kılar; zira eylem, başkalarıyla birlikte, spontane biçimde ve amaçsızca başlatıldığında politikleşir. Oysa algoritmik zamansallık içinde eylem, performatif zorunluluklara indirgenmiş, özgünlüğünü yitirmiş bir tekrar hâlini alır. Bu nedenle etik bir sosyal medya tahayyülü, yalnızca mahremiyetin teknik olarak korunmasıyla değil; kamusal alanın özgürlük, eşitlik ve sorumlulukla yeniden inşasıyla mümkündür.

Ne var ki etik, bu bağlamda yalnızca ödev ahlakı veya haklar söylemiyle sınırlanamaz. Levinas'ın (1969: 51) *radikal etik ontolojisi (totality and infinity)*, dijital çağın yüzüsüzleştirdiği ötekiliğe karşı derin bir sorumluluk çağrısıdır. Öteki'nin yüzüyle karşılaşma, dijital medyanın soyutladığı etik ilişkilenenmenin en somut biçimidir. Ancak platformların algoritmik yapısı, kullanıcıları yankı odalarına ve filtre balonlarına hapsederek, farklılıkla karşılaşma olasılığını ortadan kaldırmakta ve böylece Levinas'ın sorumluluk etiğini felce uğratmaktadır. Bu durum, dijital öznelliği yalnızca narsistik bir benliğe dönüştürmekle kalmaz, aynı zamanda ötekiyle kurulan etik ilişkiyi de simülasyon düzeyine indirger. Dolayısıyla, dijital etik ancak görünürlükten önce gelen bu sorumluluğu –ötekinin talebine verilen yanıtı– merkeze aldığında anlamlı olabilir.

Zuboff'un gözetim kapitalizmi kavramı, bu etik aşınmanın iktisadi zeminini ifşa eder. Kullanıcıların davranışsal verilerinin metalaştırılması, yalnızca piyasa mantığının dijitalleşmiş bir formu değil; aynı zamanda Bauman'ın (2000: 3) *akışkan modernlik (fluid modernity)* dediği, ilişkilerin, değerlerin ve kimliklerin sürekli çözülüp yeniden kurulduğu bir varlık durumunun dijital uzantısıdır. Bu bağlamda mahremiyet, artık yalnızca korunması gereken bir alan değil, kaybı içselleştirilmiş ve hatta arzu edilir hâle getirilmiş bir deneyimdir. Kullanıcı, sürekli

gözetlenme koşullarında kendi mahremiyetini ifşa etmeye yönlendirilir; böylece mahremiyet, tüketim nesnesi olarak dolaşıma girer. Burada etik, yalnızca teknik düzenlemelerle sağlanabilecek bir güvenlik protokolü değil; bireyin kendi ifşa ekonomisine direnebilme kapasitesi olarak ortaya çıkar.

Bu direnişin ilk sahnesi ise çocuklukta kurulur. Ebeveynlik, bu bağlamda yalnızca dijital güvenlik sağlamakla sınırlı bir sorumluluk olarak değil; çocuklara özgürlüğün, sınırın ve sorumluluğun ne anlama geldiğini kavratmaya yönelik etik bir görev olarak anlaşılmalıdır. Sema Çınar Alevli'nin (2023: 49-50) ortaya koyduğu “farkında ebeveynlik” yaklaşımı, bu noktada belirleyici bir çerçeve sunar. Çınar Alevli'ye göre ebeveynlik, çocuğun gelişimsel sürecini, bireysel karakterini ve toplumsal etkileşimlerini dikkate alan bilinçli bir yönlendirme süreci olmalıdır. Çocukluk yalnızca bireysel deneyimlerin kaydedildiği bir dönem değil; aynı zamanda toplumsal karakterin inşasına katkıda bulunan bir evredir. Bu nedenle ebeveynler, çocuklarını dijital dünyanın edilgen tüketicileri olarak değil, bu dünyanın etik ve kültürel boyutlarını sorgulayabilen kurucu özneleri olarak yetiştirmelidir. Çocukların mahremiyetin anlamını kavrayan, ötekine saygı temelinde ilişki kurabilen ve kamusal alanı birlikte paylaşmanın ahlaki boyutlarını düşünebilen bireyler olmaları, ancak bu farkındalık temelli yaklaşımla mümkündür. Böylece aile, yalnızca koruyucu bir yapı olmaktan çıkar; aynı zamanda etik düşüncenin ve kamusal sorumluluk bilincinin ilk biçimlendirildiği toplumsal bir alan hâline gelir.

Ancak bireysel bilinç yetmez. Dijital kamusal alanın etikleşmesi, çok paydaşlı, demokratik ve hesap verebilir yönetim modellerini de gerekli kılar. Platformların sadece algoritma geliştiricileriyle değil; kullanıcılar, etik kurullar, sivil toplum, hukukçular ve eğitimcilerle birlikte şekillendirilmesi, Rousseau'nun (1762/2002: 16) *toplumsal sözleşme* (the social contract) düşüncesinin dijital çağdaki yeniden yorumudur. Birey, yalnızca bir kullanıcı değil; ortak bir dijital dünyanın eşit haklara sahip yurttaşı olarak yeniden konumlandırılmalıdır. Etik bir sosyal medya yapısı, işte bu sözleşmenin normatif yükünü taşıyan, kamusal sorumluluğu kolektif bilince yerleştiren bir yapı olabilir.

Bu nedenle etik bir dijital gelecek, yalnızca mahremiyeti korumakla değil; özneliği, ötekiliği ve kamusalılığı etik bir düzlemde yeniden kurmakla ilgilidir. Dijital çağın bireyi, Heideggerci anlamda (Heidegger 1962: 276) artık *dünyaya fırlatılmış* (Geworfenheit (thrownness)) değildir; aksine, kendini sürekli olarak ifşa eden ve bu ifşanın sonuçlarını yaşam alanının tamamına yayan bir varlıktır. Bu varlığın etik sorumluluğu ise yalnızca neyi paylaştığıyla değil, paylaşmaktan neden vazgeçebildiğiyle, susmanın, gizlenmenin,

görünmezliğin ne zaman etik bir tavır olduğunu da kavrayabilmesiyle ölçülür. Kısacası, dijital etik yalnızca kurallara değil, varoluşun kendisine dair bir farkındalığa dayanmalıdır: Kendini göstermek değil, kendini sınırlandırmak da bir eylemdir; görünmek kadar geri çekilmek de etik bir tercihtir.

SONUÇ

Bu çalışmada, dijital çağın karakteristik bir örüntüsü hâline gelen sosyal medya platformlarında mahremiyetin sistematik biçimde ticarileştirildiği ele alınmış; bu sürecin bireysel öznellik, veri güvenliği ve toplumsal normatif düzen üzerindeki çok katmanlı etkileri analiz edilmiştir. Mahremiyetin yalnızca bireysel bir hak olarak değil, aynı zamanda dijital kamusal alanın ve demokratik toplumsal yapının kurucu bir bileşeni olarak ele alınması gerektiği savunulmuş; bu bağlamda birey-toplum-devlet ekseninde önleyici ve düzenleyici önlemler alınmasının gerekliliği vurgulanmıştır.

Elde edilen bulgular, sosyal medya platformlarının kullanıcı davranışlarını gözetim ve yönlendirme amacıyla yapılandırılmış sistemler üzerinden işlediğini açık biçimde ortaya koymuştur. Bu platformlar, kullanıcıların rızasını biçimsel ve teknik metinlerle alma yoluna giderek, fiiliyatta bilgilendirilmiş onamın anlamını boşaltmakta; verilerin işlenmesi sürecini şeffaflıktan uzak ve çoğu zaman kullanıcı aleyhine işleyen bir algoritmik ekonomiye dönüştürmektedir. Rıza, teknik bir onay kutusuna indirgenmiş; mahremiyet, ekonomik çıkarın nesnesi hâline getirilmiştir.

Elde edilen bulgulardan, mahremiyetin ticarileştirilmesinin yalnızca bireysel alanı tehdit etmediği, aynı zamanda kolektif düzeyde demokratik işleyişi, kamusal akı ve toplumsal güven duygusunu da aşındırdığı görülmektedir. Bu çerçevede, bireyin veri üzerindeki denetiminin azalması, yalnızca bireysel özerkliğin değil; aynı zamanda eleştirel düşüncenin, dijital yurttaşlığın ve kolektif sorumluluğun da zayıflamasına neden olmaktadır. Özellikle yapay zekâ destekli yönlendirme sistemleri, bireylerin yalnızca neyi tükettiklerini değil, neyi düşündüklerini, nasıl düşündüklerini ve neye inandıklarını da belirleme gücüne sahiptir.

Çalışma, etik bir dijital düzenin inşasının yalnızca yasal reformlarla ya da teknik araçlarla sınırlandırılmaz olduğunu göstermiştir. Platform tasarımlarına gömülü olan niyetlerin, kullanıcıya dayatılan davranış kalıplarının ve ekonomik modellerin etik bir süzgeçten geçirilmesi; daha da önemlisi, dijital okuryazarlığın bireyler ve toplumlar için içselleştirilmiş bir yaşam pratiğine dönüşmesi elzemdir. Burada özellikle ebeveynlerin ve yetişkin bireylerin rolü merkezi bir önemdedir. Çünkü dijital çağın değer aktarımı, yalnızca

okul müfredatlarında değil, gündelik yaşamın etkileşim alanlarında gerçekleşmektedir. Ebeveynler çocuklara sadece teknik sınırlar koymakla değil; aynı zamanda onlara dijital dünyada nasıl düşünmeleri, neye dikkat etmeleri ve neye direnç göstermeleri gerektiğini öğretmekle yükümlüdür. Bu bağlamda ebeveynlik, gözetimci bir kontrol mekanizmasından ziyade, birlikte öğrenmeye ve etik duyarlılık geliştirmeye dayalı bir farkındalık biçimi olarak kurgulanmalıdır.

Çalışma verileri göstermektedir ki, yetişkin bireyler açısından da mahremiyet, yalnızca korunacak bir alan değil; aynı zamanda sürekli yeniden düşünülmesi gereken bir etik sorumluluktur. Sosyal medyada paylaştığımız her içerik, yalnızca kendimizi ifade etmenin değil, aynı zamanda başkalarıyla olan ilişkimizin, ötekiyle kurduğumuz mesafenin ve kamusal alana duyduğumuz saygının bir yansımasıdır. Bu nedenle, dijital öznellik yalnızca “görünürlük” üzerinden değil, “sınır koyma” ve “görünmezliğin değerini bilme” kapasitesi üzerinden de yeniden tanımlanmalıdır. Mahremiyet, bazen geri çekilme hakkıdır; bazen de susma eyleminin politik gücüdür.

Geleceğe dair bir perspektif geliştirildiğinde, dijital mahremiyetin korunması adına üç temel eksende ilerlenmesi gerektiği görülmektedir: birincisi, platform ekonomisinin yeniden yapılandırılması; reklama dayalı modellerin yerine daha şeffaf ve kullanıcı merkezli ekonomik yapılar inşa edilmelidir. İkincisi, dijital tasarım süreçlerinin etik ilkelere göre yeniden tanımlanması; özellikle “mahremiyet odaklı tasarım” ilkesi platform mimarisinin merkezine yerleştirilmelidir. Üçüncüsü ise, bireylerin ve toplumların dijital farkındalık düzeyinin artırılması; medya okuryazarlığı, eleştirel dijital düşünme ve etik eğitim programlarının sistematik biçimde yaygınlaştırılmasıdır.

Dijital çağda insanı yalnızca “veri sağlayıcı” ya da “hedef kitle” olarak değil; irade sahibi, düşünebilen ve karar verebilen bir özne olarak yeniden konumlandırmak, etik bir dijital gelecek tahayyülünün temelidir. Bu gelecek, yalnızca teknolojinin değil, insanın merkezde olduğu; algoritmaların değil, değerlerin yön verdiği bir dijital düzenle mümkündür. Temiz bir dijital gelecek, sadece güvenli değil; adil, kapsayıcı ve anlamlı olmalıdır. Bu gelecek için sorumluluk yalnızca teknoloji şirketlerinde değil; aynı zamanda yasa koyucularda, eğitimcilerde, ebeveynlerde ve her bir dijital yurttaşın vicdanındadır.

EXTENDED ABSTRACT

The digital age has profoundly reshaped the contours of public and private life, largely through the rise of socio-technological infrastructures. At the forefront of this transformation are social

media platforms like Facebook, Instagram, TikTok, and X (formerly Twitter), which have evolved far beyond their initial roles as tools for interpersonal communication. Today, they are complex digital ecosystems where political activity, cultural expression, identity formation, and economic transactions unfold simultaneously. What makes these platforms particularly powerful is their foundational reliance on data-driven systems. Every interaction—whether a “like,” a comment, a share, or simply scrolling—is captured, analyzed, and monetized. These algorithmic architectures are optimized to collect as much personal data as possible, structuring entire user experiences around predictive analytics and behavioral manipulation. As a result, traditional understandings of privacy are being dismantled, replaced by new norms that normalize pervasive surveillance and commodification of user behavior.

This transformation is not merely technological; it is also political and ethical. The study at hand examines how privacy is systematically turned into a marketable asset by these platforms and explores the deeper consequences of this shift. It considers how informed consent is manipulated, how data is extracted and weaponized, and how these practices ultimately affect democratic integrity and digital justice. At its core, this research interrogates a fundamental tension: the conflict between individual autonomy and platform power in a digital environment where the lines between public participation and private exposure are increasingly blurred.

The research poses several pressing questions. First, how do social media platforms operationalize the collection and commodification of user data? This involves an exploration of both visible mechanisms—such as terms of service and data tracking cookies—and more hidden dynamics like dark patterns and behavioral nudges. Second, the study asks how the economic exploitation of privacy affects data security and user agency. By converting intimate personal data into tradeable commodities, platforms gain immense power over users, who often lack the tools or knowledge to resist. Third, it questions the efficacy of informed consent: do users genuinely understand what they are agreeing to, or are they merely clicking through legal jargon to access a service? Fourth, the study interrogates whether current legal and regulatory frameworks such as the GDPR (General Data Protection Regulation), the CCPA (California Consumer Privacy Act), and Turkey’s KVKK (Personal Data Protection Law) are sufficient to hold platforms accountable. Finally, it asks whether a more ethical and inclusive digital system is possible—and if so, what it would require.

The research draws on critical theory and political economy to frame these issues. The methodological approach is qualitative and document-based, incorporating regulatory texts, privacy policies, academic literature, and landmark case studies, most notably the Cambridge

Analytica scandal. The theoretical lens is informed by figures like Alan Westin, Ruth Gavison, Helen Nissenbaum, and Anita Allen, as well as Shoshana Zuboff's work on surveillance capitalism. These perspectives help conceptualize privacy as not only an individual entitlement but also a collective, relational construct embedded in structures of power.

One of the key findings is the illusion of consent that pervades digital platforms. While users are nominally given choices about their data, those choices are often constrained by opaque language, interface design tricks, and social pressure to conform. Consent is therefore more performative than substantive. Privacy policies are written in legal language few can understand, and design elements like pre-ticked boxes and urgent notifications encourage users to opt into data sharing without genuine understanding. The result is a coerced form of compliance, cloaked in the rhetoric of personal freedom.

Another critical insight is the transformation of privacy into an economic asset. Under surveillance capitalism, personal data is the raw material that fuels algorithmic engines. Platforms track both explicit behaviors (likes, follows, shares) and implicit ones (hover time, search queries, device location) to build psychometric profiles of users. These profiles are then used to personalize content, target advertisements, and influence political opinions. This process turns users from autonomous agents into predictable data generators, raising significant ethical concerns about manipulation, exploitation, and the erosion of individuality.

Data security is another area of concern. The infrastructures of social media platforms are often riddled with vulnerabilities, ranging from poorly secured databases to inadequate encryption protocols. High-profile data breaches, such as the exposure of millions of Facebook users' personal information, illustrate how profit motives frequently trump security considerations. Compounding this issue is the fact that most users are unaware of how long their data is stored, how it is anonymized, or whether it can be re-identified. Digital literacy remains low, leaving users defenseless against increasingly sophisticated data exploitation practices.

Legal and regulatory frameworks, while crucial, often fall short of their intended goals. The GDPR, CCPA, and KVKK have introduced meaningful protections, such as the right to be forgotten and requirements for data minimization. However, enforcement remains inconsistent. Companies frequently find ways to circumvent regulations, and jurisdictional complexities make international compliance difficult. Moreover, these laws tend to emphasize individual rights, failing to address the collective dimensions of data exploitation. In this way, they provide

a false sense of security while doing little to dismantle the structural incentives driving data commodification.

The ethical and societal implications of these developments are profound. When privacy becomes a market good, it loses its normative function as a safeguard for human dignity and autonomy. People begin to internalize surveillance, adapting their behavior to what they think algorithms expect of them. This leads to performative online identities, a collapse of the distinction between public and private life, and a culture of self-monitoring. Digital inequalities also deepen: marginalized communities, who often lack access to education, legal support, or technology, are the most exposed to exploitative practices. In addition, content recommendation algorithms reinforce ideological silos, eroding public discourse and contributing to political polarization.

Against this backdrop, the study argues for a reconceptualization of privacy as an ontological and ethical condition, not merely a legal right. Drawing on philosophical insights from thinkers like Hannah Arendt, Michel Foucault, Emmanuel Levinas, and Martin Heidegger, the research highlights how algorithmic visibility erodes spontaneity, moral responsibility, and political agency. The individual in the digital age is no longer simply a private person who sometimes goes public, but rather a datafied subject whose identity is continually shaped by algorithmic logics and commercial imperatives. In such a world, privacy is essential not only for individual freedom but also for preserving the possibility of meaningful political life.

To address these complex challenges, the study outlines a multi-dimensional strategy. First, structural reforms are needed to disrupt the economic logic of surveillance. Alternative platform models—such as subscription-based services, platform cooperatives, or publicly funded digital infrastructures—could offer viable paths forward. These models would shift the value proposition away from data extraction and toward user empowerment. Second, ethical and transparent design must become standard practice. This includes embedding privacy-by-design principles, eliminating manipulative user interfaces, and ensuring algorithmic accountability. Third, there must be a concerted effort to foster digital literacy and cultural awareness. Educational initiatives should teach not only technical skills but also the ethical dimensions of digital participation, enabling users to navigate digital spaces with critical consciousness.

In conclusion, privacy must be reasserted as a cornerstone of democratic life in the digital era. It is not a nostalgic holdover from a pre-digital world, but a vital condition for human

dignity, trust, and collective responsibility. Protecting privacy means more than preventing data breaches—it requires rethinking the very foundations of how digital platforms are built, governed, and used. A just digital future demands that individuals be seen not as mere data points but as full ethical and political subjects, capable of agency, deliberation, and resistance. Only then can the digital commons become a space of genuine freedom and democratic possibility.

KAYNAKÇA

- Arendt, H. (1958). *The Human Condition*, Chicago: University of Chicago Press.
- Barocas, S., Nissenbaum, H. (2014). Big Data's End Run Around Anonymity and Consent, J. Lane vd. (Der.), *Privacy, Big Data, and the Public Good* içinde (44-75). Cambridge: Cambridge University Press.
- Bauman, Z. (2000). *Liquid Modernity*, Cambridge: Polity Press.
- BBC News. (2019). Facebook Admits Storing Millions of Passwords in Plain Text. <https://www.bbc.com/news/technology-47683082> (Erişim: 29.04.2025).
- Bok, S. (1982). *Secrets: On the Ethics of Concealment and Revelation*, New York: Pantheon Books.
- Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*, New Haven: Yale 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> (Erişim: 29.04.2025).
- Cavoukian, A. (2010). Privacy by Design: The 7 Foundational Principles. Ontario: Information and Privacy Commissioner of Ontario. <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> (Erişim: 23.04.2025).
- Cinelli, M., De Francisci Morales, G., Galeazzi, A. vd. (2021). The Echo Chamber Effect on Social Media, *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. Doi: <https://doi.org/10.1073/pnas.2023301118>
- Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, New Haven: Yale University Press.
- Çınar Alevli, S. (2023). Dijital Zorbalık Problemi ve Çözüm Önerileri, Üsküdar Üniversitesi İletişim Fakültesi 10. Uluslararası İletişim Günleri: Dijital Kapitalizm ve İletişim Sempozyumu Bildiriler Kitabı içinde (30-55), Üsküdar Üniversitesi Yayınları.
- Del Vicario, M., Vivaldo, G., Bessi, A. vd. (2016). Echo Chambers: Emotional Contagion and Group Polarization on Facebook, *Scientific Reports*, 6(37825), 1-9. Doi: <https://doi.org/10.1038/srep37825>
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York: St. Martin's Press.
- European Commission. (2024a). Artificial Intelligence Act: Regulation (EU) 2024/1689 of the European Parliament and of the Council, *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>
- European Commission. (2024b, 21 Mayıs). Landmark AI Act Gets Final Green Light from the Council. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2785
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*, New York: Vintage Books.
- Gavison, R. (1980). Privacy and the Limits of Law, *The Yale Law Journal*, 89(3), 421-471. Doi: <https://doi.org/10.2307/796891>
- GDPR. (2018). Regulation (EU) 2016/679. <https://gdpr.eu> (Erişim: 12.03.2025).

- Giddens, A. (1992). *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford University Press.
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven: Yale University Press.
- Gomez-Urbe, C. A., Hunt, N. (2015). The Netflix Recommender System: Algorithms, Business Value, and Innovation, *ACM Transactions on Management Information Systems (TMIS)*, 6(4), 1-19. Doi: <https://doi.org/10.1145/2843948>
- Gray, C. M., Kou, Y., Battles, B. vd. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Doi: <https://doi.org/10.1145/3173574.3174108>
- Heidegger, M. (1962). *Being and Time*, J. Macquarrie ve E. Robinson (Çev.), New York: Harper ve Row.
- Holvast, J. (2009). History of Privacy, S. Fischer-Hübner, P. Duquenoy, A. Zuccato ve L. Martucci (Der.), *The Future of Identity in the Information Society* içinde (13-42). Springer. Doi: https://doi.org/10.1007/978-3-642-03315-5_2
- Inness, J. C. (1992). *Privacy, Intimacy, and Isolation*, Oxford: Oxford University Press.
- Kant, I. (1996). *The Metaphysics of Morals*, M. J. Gregor (Çev.), Cambridge University Press.
- Kant, I. (1997). *Groundwork of the Metaphysics of Morals*, M. Gregor (Çev.), Cambridge University Press.
- Kosinski, M., Stillwell, D. ve Graepel, T. (2013). Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, *Proceedings of the National Academy of Sciences*, 110(15), 5802-5805. Doi: <https://doi.org/10.1073/pnas.1218772110>
- KVKK. (2016). 6698 Sayılı Kişisel Verilerin Korunması Kanunu. <https://www.kvkk.gov.tr> (Erişim: 20.02.2025)
- Lanier, J. (2013). *Who Owns the Future?*, Simon ve Schuster.
- Levinas, E. (1969). *Totality and Infinity: An Essay on Exteriority*, Pittsburgh: Duquesne University Press.
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*, Cambridge: Polity Press.
- Mathur, A., Acar, G., Friedman, M. G. vd. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1-32. Doi: <https://doi.org/10.1145/3359183>
- McDonald, A. M., Cranor, L. F. (2008). The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543-568.
- Nissenbaum, H. (2011). A Contextual Approach to Privacy Online, *Daedalus*, 140(4), 32-48. Doi: https://doi.org/10.1162/daed_a_00113
- Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*, NYU Press.
- Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review*, 57, 1701-1777.
- Posner, E. A., Weyl, E. G. (2018). *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*, Princeton: Princeton University Press.

- Rousseau, J.-J. (2002). *The Social Contract*, G. D. H. Cole (Çev.), Mineola: Dover Publications.
- Scholz, T. (2016). *Platform Cooperativism: Challenging the Corporate Sharing Economy*, New York: Rosa Luxemburg Stiftung.
- Sevignani, S. (2013). The Commodification of Privacy on the Internet, *Science and Public Policy*, 40(6), 733-739. Doi: <https://doi.org/10.1093/scipol/sct082>
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma, *Harvard Law Review*, 126(7), 1880-1903.
- Tufekci, Z. (2015). Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency, *Colorado Technology Law Journal*, 13, 203-218.
- Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*, Oxford: Oxford University Press.
- Warren, S. D., Brandeis, L. D. (1890). The Right to Privacy, *Harvard Law Review*, 4(5), 193-220.
- Westin, A. F. (1967). *Privacy and Freedom*, New York: Atheneum.
- Wirth, L. (1938). Urbanism as a Way of Life, *American Journal of Sociology*, 44(1), 1-24.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs.

Makale Bilgileri/Article Information

<i>Etik Beyan:</i>	Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan edilir.	<i>Ethical Statement:</i>	It is declared that scientific and ethical principles have been followed while carrying out and writing this study and that all the sources used have been properly cited.
<i>Çıkar Çatışması:</i>	Çalışmada kişiler veya kurumlar arası çıkar çatışması bulunmamaktadır.	<i>Conflict of Interest:</i>	The authors declare that declare no conflict of interest.
<i>Yazar Katkı Beyanı:</i>	Çalışmanın tamamı yazar tarafından oluşturulmuştur.	<i>Author Contribution Declaration:</i>	The entire study was created by the author.
<i>Mali Destek:</i>	Çalışma için herhangi bir kurum veya projeden mali destek alınmamıştır.	<i>Financial Support:</i>	The study received no financial support from any institution or project.
<i>Yapay Zekâ Kullanımı:</i>	Bu çalışmada herhangi bir yapay zekâ tabanlı araç veya uygulama kullanılmamıştır.	<i>Use of Artificial Intelligence:</i>	This study did not utilize any artificial intelligence-based tools or applications.
<i>İntihal:</i>	Bu makalede intihal taraması yapılmış ve intihal içermediği teyit edilmiştir. – İntihal.Net	<i>Plagiarism:</i>	This article has been scanned for plagiarism and it has been confirmed that it does not contain plagiarism. – İntihal.Net

