

Dijitalleşme, Güvenlik ve Aile: Toplumsal Sözleşmeye Yeni Yaklaşımlar

Gülşah ÖZDEMİR¹

DOI: 10.5281/zenodo.21744553

Özet

Dijitalleşme, toplumsal kurumların işleyişini köklü biçimde dönüştürerek aile yapısını yeniden şekillendirmektedir. Klasik toplumsal sözleşme teorileri birey–devlet ilişkisini güvenlik, özgürlük ve mülkiyet temelinde açıklarken, dijital çağda büyük teknoloji şirketleri ve platformlar bu sözleşmenin yeni dolaylı aktörleri hâline gelmiştir. Bu makale, dijitalleşmenin aile kurumuna etkilerini ve toplumsal sözleşme anlayışını nasıl yeniden tanımladığını incelemektedir. Kuramsal çerçeve, Hobbes’un güvenlik, Locke’un mülkiyet ve doğal haklar, Rousseau’nun genel irade ilkeleriyle; Zuboff’un gözetim kapitalizmi, Berners-Lee’nin veri egemenliği ve Castells’in ağ toplumu kavramlarını bir araya getirmektedir. Analiz, dijitalleşmenin ailede mahremiyet sınırlarını yeniden çizdiğini, ebeveynlik rollerini dönüştürdüğünü, çocukların dijital vatandaşlık kimliklerini öne çıkardığını ve kuşaklar arası dijital eşitsizlikleri derinleştirdiğini göstermektedir. Bu bağlamda çalışma, dijital çağın gereksinimlerine uygun yeni bir toplumsal sözleşme ihtiyacını ortaya koymaktadır. Sözleşmenin temel ilkeleri; dijital mahremiyet hakkı, eşit erişim, çevrim içi güvenlik, dijital okuryazarlık ve kullanıcıların platform politikalarında temsil edilmesi olarak belirlenmiştir. Politika düzeyinde ulusal düzeyde anayasal güvenceler ve çocuk odaklı veri koruma yasaları; uluslararası düzeyde Avrupa Birliği, Birleşmiş Milletler ve UNICEF’in normatif çerçeveleri; çok paydaşlı düzeyde ise devlet–şirket–sivil toplum iş birlikleri öne çıkmaktadır. Sonuç olarak dijitalleşme, yalnızca teknik bir süreç değil; aileyi merkeze alan yeni bir toplumsal sözleşmenin inşasını zorunlu kılan kapsamlı bir toplumsal kırılmadır.

Anahtar Kelimeler: Dijital yönetim, Toplumsal sözleşme teorisi, Gözetim kapitalizmi, Dijital egemenlik, Dijital güvenlik.

¹ Dr. Öğr. Üy. Balıkesir Üniversitesi, Burhaniye Uygulamalı Bilimler Fakültesi, gulsah.ozdemir@balikesir.edu.tr, ORCID: 0000-0001-8900-2560

Digitalization, Security, and the Family: New Approaches to the Social Contract

Abstract

Digitalization is a transformative process that reshapes the functioning of social institutions, including the family. While classical social contract theories explained the relationship between individuals and the state through security, freedom, and property, in the digital age major technology companies and platforms have become new indirect actors of this contract. This article examines how digitalization affects the family institution and redefines the social contract.

The theoretical framework combines Hobbes's notion of security, Locke's focus on property and natural rights, and Rousseau's principle of the general will with Zuboff's surveillance capitalism, Berners-Lee's data sovereignty, and Castells's network society. The analysis shows that digitalization redraws the boundaries of privacy, transforms parenting roles, brings forward children's digital citizenship identities, and deepens intergenerational inequalities.

The study highlights the need to establish a new social contract adapted to the digital age. Its core principles include the right to digital privacy, equal access, online security, digital literacy, and user representation in platform governance. Policy implications involve constitutional guarantees and child-centered data protection at the national level; European Union and United Nations frameworks at the international level; and multistakeholder cooperation across governments, corporations, and civil society.

In conclusion, digitalization is not merely a technical shift but a profound societal rupture that necessitates a new social contract centered on the family.

Keywords: Digital governance, Social contract theory, Surveillance capitalism, Digital sovereignty, Digital security.

Extended Abstract

Digitalization has transcended being merely a technical process involving the development of technological infrastructure; it has become a comprehensive transformative dynamic restructuring political, economic, and social relations. With the penetration of information and communication technologies into every aspect of daily life, individuals' perceptions of privacy, family communication patterns, children's socialization processes, and states' understanding of security have changed significantly. In particular, the decisive position of large technology companies in data production and management has created new power centers beyond the classic individual-state relationship, necessitating a reassessment of the social contract concept. This study aims to analyze the effects of digitalization on the family institution within the framework of classical social contract theories. In this study, Thomas

Hobbes's security-oriented approach, John Locke's understanding of natural rights and property, and Jean-Jacques Rousseau's concept of the general will are reinterpreted in light of the dynamics of the digital age. Thus, it is argued that the family institution is not merely a sociological structure; it has transformed into a strategic actor at the center of digital security, data sovereignty, and global governance processes. In this respect, the study aims to fill a significant gap in existing studies by integrating the relationship between digitalization and family with the literature on international security and digital governance. The research is theoretical in nature and relies on a comparative analysis method. In the first stage, the social contract approaches of Hobbes, Locke, and Rousseau are examined; in the second stage, these theories are re-evaluated within the framework of surveillance capitalism, data sovereignty, and network society, which are fundamental concepts of the digital age. In this context, Shoshana Zuboff's approach to surveillance capitalism, Tim Berners-Lee's understanding of data sovereignty, and Manuel Castells' network society theory are used as key reference points. Furthermore, the European Union's General Data Protection Regulation (GDPR), the United Nations and UNICEF's regulations on children's rights, and NATO's cybersecurity policies are evaluated to explain the international dimension of the digital social contract.

The findings of the study show that digitalization is transforming the family institution in a multi-dimensional way. Firstly, the understanding of privacy within the family is being reshaped. Data generated through digital platforms and smart devices is shifting a significant portion of family life online; children's personal data is becoming part of the digital ecosystem even before their conscious consent is obtained. This situation is transforming family privacy from a matter of protecting private life into a subject of national and international security policies. Secondly, parenting roles are changing significantly with digitalization. Traditional parental supervision is giving way to digital guidance and digital literacy skills. Children's use of social media, online games, AI-powered applications, and algorithmic content suggestions necessitate parents acquiring new knowledge and skills. Intergenerational differences in digital competence are deepening communication problems within families and creating new security risks. Thirdly, digitalization is placing the family at the center of international security discussions. States are developing digital sovereignty strategies while trying to establish new balances between individual privacy and national security. While the European Union develops data protection policies based on individual rights, China adopts a more state-centric understanding of digital sovereignty. NATO, on the other hand, considers digital security an integral part of collective defense. These different approaches highlight the fundamental challenges to establishing a universal social contract in the digital age. The study's most significant theoretical contribution is its reinterpretation of classical social contract theories within the context of the digital age, explaining the concept of a "digital social contract" from a family-centered perspective. The research demonstrates that digitalization not only transforms the relationship between the state and the individual but also creates a new multi-actor governance structure between the state, technology companies, international organizations, and the family. Therefore, in the social contract of the digital age, the principles of security, freedom, and equality should be considered together with the concepts of digital privacy, data rights, digital citizenship, and platform governance.

The policy recommendations developed within the scope of the research are addressed at three levels. At the national level, it is recommended that digital rights be constitutionally guaranteed, child-focused data protection regulations be developed, and family-centered cybersecurity strategies be created. At the international level, it is emphasized that the GDPR, child rights-focused digital norms developed by UNICEF and the United Nations should be disseminated and international cooperation strengthened. At the multi-stakeholder governance level, it is argued that new governance mechanisms should be developed where states, technology companies, academia, and civil society organizations act together, based on transparency and accountability.

In conclusion, the study reveals that digitalization is not only a technological transformation but also a comprehensive social upheaval that redefines the understanding of security, rights, and governance. The family institution holds a central position in building a new social contract suitable for the needs of the digital age. Protecting digital privacy, guaranteeing children's rights, promoting digital literacy, and increasing democratic participation in platform governance are considered fundamental elements of a sustainable and inclusive social order in the digital society of the future. In this respect, the study offers a unique theoretical contribution to both international relations and digital governance literature by reinterpreting digitalization, security, and family relations within the framework of classical social contract theories.

GİRİŞ

Dijitalleşme, 21. yüzyılın en kapsamlı ve derinlemesine toplumsal dönüşüm süreçlerinden biridir. Bilgi ve iletişim teknolojilerinin yaygınlaşması yalnızca ekonomik ve siyasal yapıları değil; gündelik yaşam pratiklerini, mahremiyet algılarını ve toplumsal ilişkilerin temel yapılarını da köklü biçimde dönüştürmektedir. Bireyler arası iletişim biçimlerinden kimlik inşasına, sosyalleşme pratiklerinden aidiyet ilişkilerine kadar pek çok alanda yeni toplumsal dinamikler ortaya çıkmakta; özel ve kamusal alanlar giderek daha fazla iç içe geçmektedir (Castells, 2000).

Bu bağlamda dijitalleşmeden en yoğun biçimde etkilenen yapılardan biri aile kurumudur. Aile, modern toplumlarda hem özel alanın merkezinde konumlanmakta hem de kamusal politikaların doğrudan konusu hâline gelmektedir. Dijitalleşme ile birlikte aile içi iletişimde dijital araçlar belirleyici hâle gelmiş, ebeveynlik rolleri yeniden tanımlanmış, çocukların çevrim içi ortamlarda sosyalleşmesi yaygınlaşmış ve mahremiyet sınırları giderek bulanıklaşmıştır (Hiniker v.d., 2016, s. 1378). Bu dönüşüm, ailenin yalnızca biyolojik ve duygusal bağlara dayalı bir yapı olmaktan çıkıp, dijital teknolojilerle şekillenen çok aktörlü bir toplumsal sözleşmenin parçası hâline gelmesine neden olmaktadır.

Bu çok katmanlı değişim, klasik siyasal kuramların yeniden değerlendirilmesini gerekli kılmaktadır. Özellikle Hobbes'un güvenlik, Locke'un mülkiyet ve bireysel haklar, Rousseau'nun ise genel irade temelli toplumsal sözleşme anlayışları tarihsel bağlamda devlet-

birey ilişkisini açıklamakta önemli referans noktaları sunmuştur. Ancak dijital çağın özgün koşulları, bu kuramsal çerçevelerin yeniden yorumlanmasını zorunlu kılmaktadır. Bugün yalnızca birey ile devlet arasında değil; birey, aile, devlet ve dijital aktörler (teknoloji şirketleri, çevrim içi platformlar, algoritmik sistemler) arasında yeni bir sözleşme ilişkisi oluşmaktadır (Berners-Lee v.d., 2021; Zuboff, 2019).

Dijitalleşme yalnızca toplumsal ilişkileri dönüştürmekle kalmamakta, aynı zamanda uluslararası güvenlik, dijital egemenlik ve küresel norm inşası açısından da yeni tartışmaları gündeme getirmektedir. Avrupa Birliği (AB)'nin Genel Veri Koruma Tüzüğü (GDPR) düzenlemeleri, Çin'in veri güvenliği stratejileri ve NATO'nun siber politikaları, dijitalleşmenin aile odaklı insani güvenlik boyutunu doğrudan uluslararası ilişkiler gündemine taşımaktadır.

Mevcut literatürde dijitalleşme ve aile ilişkileri daha çok sosyolojik bir perspektiften ele alınırken, bu sürecin uluslararası güvenlik, norm inşası ve küresel yönetim boyutları henüz yeterince tartışılmamıştır. Bu çalışma, söz konusu boşluğu doldurmayı amaçlamakta; klasik sözleşme kuramlarını dijital çağ bağlamında yeniden yorumlayarak aile kurumunu bu perspektiften analiz etmektedir. Çalışma, kuramsal bir analiz sunmakta ve klasik sözleşme teorileri ile dijitalleşme tartışmalarını karşılaştırmalı bir yöntemle ele almaktadır.

Kuramsal Çerçeve

Toplumsal sözleşme kuramları, modern siyasal düşüncenin temel yapı taşlarını oluşturarak birey ile devlet arasındaki ilişkinin nasıl kurulması gerektiğine dair kuramsal açıklamalar sunar. Bu teoriler yalnızca siyasal otoritenin meşruiyetini değil, aynı zamanda toplumsal düzenin ahlaki ve hukuki temellerini de tanımlar. Ancak dijitalleşme ile birlikte toplumsal yapılar, iletişim biçimleri ve iktidar ilişkileri köklü biçimde dönüşmektedir. Özellikle birey, aile ve devlet arasındaki ilişkiler dijital teknolojiler, veri politikaları ve platform dinamikleri aracılığıyla yeniden şekillenmektedir. Bu dönüşüm, klasik sözleşme anlayışlarının çağdaş bağlamda yeniden ele alınmasını gerekli kılmaktadır.

Bu bölüm, kuramsal bir inceleme olarak kurgulanmış; klasik sözleşme kuramları ile dijital çağın yönetim sorunlarını karşılaştırmalı bir yaklaşımla ele almaktadır. Çalışma, hem Thomas Hobbes, John Locke ve Jean-Jacques Rousseau gibi kurucu düşünürlerin klasik sözleşme yaklaşımlarını incelemekte; hem de bu yaklaşımları dijital çağda aile kurumu, mahremiyet, veri mülkiyeti ve platform yönetimi gibi güncel kavramlarla ilişkilendirerek yeniden değerlendirmektedir. Bu üç yaklaşımın günümüz dijital bağlamındaki izdüşümleri, sırasıyla devletlerin siber güvenlik politikalarında Hobbesçu bir güvenlik anlayışının, veri mülkiyeti ve veri koruma düzenlemelerinde Lockeçu hak kavramının, dijital platformlarda katılım ve eşitlik sorunlarında ise Rousseaucu genel irade tartışmalarının yeniden gündeme geldiğini göstermektedir.

Klasik Toplumsal Sözleşme Anlayışı

Thomas Hobbes, toplumsal sözleşme teorisinin kurucu isimlerinden biri olarak, siyasi otoritenin meşruiyetini bireylerin güvenlik arayışına dayandırır. Leviathan (1651) adlı eserinde formüle ettiği kuram, bireylerin mutlak özgürlük içinde yaşadıkları ve herhangi bir merkezi

otoritenin bulunmadığı “doğa durumu” (state of nature) kavramıyla başlar. Hobbes’a göre bu ortam, sürekli çatışma ve güvensizlik halidir ve bireyler bu kaostan kurtulmak için özgürlüklerinin bir kısmını egemene devreder. Egemen, kolektif güvenliğin teminatı olarak yasaları koyma ve uygulama konusunda mutlak yetkilere sahiptir (Baumgold, 2010; Karaduman, 2020, s. 125).

Hobbes’un bu modelinde güvenlik, bireysel özgürlüklerin önünde gelir. Bu yönüyle, günümüzde devletlerin siber güvenlik stratejileri, gözetim teknolojileri ve dijital denetim politikalarında Hobbesçu bir mantığın izleri görülmektedir. Özellikle bireylerin çevrim içi güvenlik gerekçesiyle mahremiyetlerinden feragat etmesi, Hobbes’un güvenlik-özgürlük dengesi tartışmasını dijital bağlamda yeniden güncel kılmaktadır.

John Locke’un siyasal teorisi, bireylerin yaşam, özgürlük ve mülkiyet gibi devredilemez doğal haklara sahip olduğu varsayımına dayanır. Bu hakların güvence altına alınması meşru bir siyasal düzenin ön koşuludur. Locke’a göre mülkiyetin kaynağı emektir; birey doğadaki ortak kaynakları emeğiyle dönüştürdüğünde, o kaynak üzerinde mülkiyet hakkı kazanır (Marguerat, 2014; Waldron, 1984, s. 101). Bu nedenle devletin temel görevi, bireylerin doğal haklarını ve mülkiyetini korumaktır (Heyman, 2018, ss.711-712; Yolton, 1958, s. 479).

Dijital çağda Locke’un mülkiyet teorisi, veri mülkiyeti tartışmaları üzerinden yeniden gündeme gelmiştir. AB’nin GDPR düzenlemeleri, Türkiye’deki KVKK gibi veri koruma yasaları, bireylerin dijital varlıklarını Lockeçu bir mülkiyet hakkı olarak tanımlamakta ve koruma altına almaya çalışmaktadır. Ancak küresel ölçekte teknoloji şirketlerinin asimetrik gücü, bu hakların fiilen nasıl korunabileceğine dair önemli soru işaretleri yaratmaktadır.

Jean-Jacques Rousseau, adil bir toplumun inşasında genel irade (*volonté générale*) ve eşitlik ilkelerini merkeze alır. Toplum Sözleşmesi (1762) adlı eserinde, bireylerin doğa hâlindeki özgürlüklerinden vazgeçerek sivil toplum içinde ahlaki ve siyasal özgürlüğe ulaşabileceklerini savunur. Genel irade, bireylerin yalnızca kendi çıkarları doğrultusunda değil, toplumun ortak yararı için karar almasını gerektirir (Sreenivasan, 2000, s. 558; Song, 2013, s. 96).

Rousseau’nun eşitlik vurgusu, dijital çağda platform temelli katılım süreçleri ve dijital eşitsizlik tartışmaları ile yeniden gündeme gelmiştir. Algoritmik yönlendirmelerin şeffaf olmaması ve platform politikalarında kullanıcıların sınırlı söz hakkına sahip olması, Rousseau’nun katılımcı yurttaşlık ideali ile tezat oluşturmaktadır. Bugün platform yönetişimi ve dijital demokrasi tartışmaları, Rousseaucu genel irade anlayışının dijital izdüşümleridir.

Hobbes, Locke ve Rousseau’nun sözleşme yaklaşımları, farklı tarihsel bağlamlarda şekillenmiş olsa da ortak bir sorunsalı paylaşıyor: birey ile otorite arasındaki ilişki nasıl meşrulaştırılacak ve bu ilişkide güvenlik, özgürlük ve eşitlik nasıl dengelenecektir? Dijitalleşme, bu kuramların sınırlarını zorlamaktadır. Hobbes’un güvenlik anlayışı, devletlerin dijital gözetim kapasiteleri üzerinden; Locke’un mülkiyet yaklaşımı, veri sahipliği ve kişisel verilerin korunması üzerinden; Rousseau’nun genel irade ilkesi ise platform demokrasisi ve dijital eşitsizlikler üzerinden yeniden tartışılmaktadır.

Dijital Toplumsal Sözleşme Yaklaşımı

Dijitalleşme, birey ile devlet arasındaki klasik sözleşme ilişkisini köklü biçimde dönüştürmekte; bu ilişkiye özel sektör, dijital platformlar ve veri altyapıları gibi yeni aktörler dahil olmaktadır. Bu bağlamda geliştirilen Dijital Sosyal Sözleşme (DSC), toplumsal sözleşme düşüncesinin dijital çağ koşullarına uyarlanmış bir versiyonunu temsil etmektedir. DSC, bireyler arasında dijital ortamda yürütülen, teknolojik altyapılar tarafından tanımlanan ve uygulanan karşılıklı yükümlülöklere dayalı gönüllü bir uzlaşma biçimidir (Cohen, 2019).

Bu noktada Zuboff'un (2019) "gözetim kapitalizmi" analizi, dijital sosyal sözleşmenin neden gerekli olduğunu en güçlü biçimde ortaya koyar. Zuboff'a göre, bireylerin dijital ortamlardaki tıklama, arama ve etkileşimlerinden üretilen "davranışsal fazlalık" veriler, kullanıcıların rızası ya da karşılıklı bir fayda ilişkisi olmadan toplanmakta ve şirketler tarafından öngörü modelleri geliştirmek ile kullanıcı davranışlarını yönlendirmek için kullanılmaktadır. Bu süreç, bireylerin özgür seçimlerine dayalı olması gereken dijital etkileşimleri, asimetrik bir güç ilişkisine dönüştürmektedir (Venkatesh, 2021, s.366). Böylece Locke'un doğal haklar ve rıza anlayışı, dijital ekonomide büyük ölçüde zayıflamıştır.

Buna karşılık, Tim Berners-Lee'nin veri egemenliği vizyonu daha kapsayıcı ve kullanıcı merkezli bir dijital sözleşme önerisi sunmaktadır. *Solid* projesi ile bireylerin kendi verileri üzerindeki kontrolünü yeniden kazanması, Lockeçu hakların dijital bağlamda yeniden işlerlik kazanmasını amaçlamaktadır (Berners-Lee, 2019). Ancak Zuboff'un işaret ettiği sistemsel asimetrikler, Berners-Lee'nin önerisinin uygulanabilirliğini tartışmalı kılmaktadır (Foini, 2023; Mishra, 2023). Bu nedenle, yalnızca bireylerin verileri üzerindeki kontrolünü güçlendiren çözümler yeterli değildir; dijitalleşmenin doğurduğu sorunlar çok daha geniş bir kurumsal ve küresel düzenleme ihtiyacını ortaya koymaktadır.

Dijital toplumsal sözleşme bu noktada yalnızca ulusal düzeyde birey-devlet ilişkisini değil; aynı zamanda uluslararası örgütlerin, teknoloji şirketlerinin ve sivil toplumun ortak sorumluluk üstlendiği çok aktörlü bir küresel yönetim düzenini zorunlu kılmaktadır. AB'nin veri koruma politikaları, Çin'in dijital egemenlik stratejileri ve NATO'nun siber güvenlik vizyonu, bu sözleşmenin giderek küresel bir norm inşasına dönüştüğünü göstermektedir. Aile ise bu düzenin merkezinde, insani güvenliğin en kırılgan odağı olarak konumlanmaktadır. Çocukların verilerinin korunması, ebeveynlerin dijital yeterliliklerinin artırılması ve kuşaklar arası mahremiyet sınırlarının yeniden tanımlanması, dijital toplumsal sözleşmenin temel bileşenleridir (Metra & Dobelniece, 2022, s. 320; UNICEF, 2023).

Sonuç olarak, dijitalleşmenin aile kurumunu dönüştüren dinamikleri salt koruyucu tedbirlerle yönetilemeyecek kadar kapsamlıdır. Bu nedenle, çok aktörlü işbirliğine dayanan ve aileyi merkeze alan yeni bir toplumsal sözleşme, hem toplumsal istikrarın hem de insani güvenliğin dijital çağda sürdürülebilirliğini sağlamanın en önemli dayanaklarından biri olarak ortaya çıkmaktadır.

Bu kuramsal çerçeve doğrultusunda çalışma şu temel soruya yanıt aramaktadır: "Dijitalleşme sürecinde aile kurumunun karşılaştığı dönüşümler, klasik toplumsal sözleşme

teorilerinin güvenlik, hak ve eşitlik eksenlerinde nasıl yeniden yorumlanmasını gerektirmektedir ve bu süreç uluslararası güvenlik ile küresel yönetim açısından ne ifade etmektedir?” Bu soru ekseninde makale, klasik sözleşme yaklaşımlarını dijital çağın çok aktörlü yapısıyla karşılaştırarak, özellikle aile kurumunu insani güvenlik odağı olarak merkeze almakta; devletlerin dijital politikaları, teknoloji şirketlerinin küresel etkisi ve uluslararası örgütlerin normatif düzenlemeleri üzerinden yeni bir toplumsal sözleşmenin unsurlarını tartışmaktadır.

Dijital Toplumsal Sözleşmenin Uluslararası Boyutları ve Politika Analizi

Dijital dönüşüm, devletlerin egemenlik ve güvenlik anlayışlarını köklü biçimde dönüştürmektedir. Geleneksel anlamda fiziksel sınırların korunmasına dayalı ulusal güvenlik, yerini dijital altyapıların, veri akışlarının ve siber uzayın kontrolüne bırakmaktadır. Bu bağlamda dijital egemenlik, modern devletlerin ulusal güvenlik stratejilerinde temel bir unsur olarak ortaya çıkmaktadır. Devletlerin dijital alan üzerindeki hâkimiyetini sağlama çabaları; veri güvenliğinden teknolojik bağımsızlığa, siber tehditlerden dijital sömürgecilığe kadar çok boyutlu bir mücadeleyi içermektedir (Shoker, 2022, s. 59; Zinovieva & Shitkov, 2023, s. 78).

Dijital egemenlik, yalnızca teknik değil; aynı zamanda siyasi, ekonomik ve kültürel boyutları olan çok katmanlı bir egemenlik türünü temsil eder. Veri çağın yeni stratejik kaynağı haline gelirken, siber güvenlik ulusal güvenliğin ayrılmaz bir bileşeni olmuştur. Bu durum, Hobbes’un güvenlik için güçlü merkezi otorite ihtiyacının dijital çağda yeniden gündeme gelmesine yol açmaktadır. Devletler, vatandaşlarının çevrim içi güvenliğini sağlamak adına gözetim ve denetim araçlarını genişletmekte; bireyler ise mahremiyetlerinden feragat ederek güvenliği öncelemektedir. Bu gelişmeler, Hobbesçu güvenlik–özgürlük dengesinin dijital bağlamda yeniden tartışılmasına neden olmaktadır.

Buna karşılık, Locke’un doğal haklar ve mülkiyet vurgusu dijital çağda veri hakları bağlamında yeniden yorumlanmaktadır. AB’nin GDPR düzenlemeleri ve Türkiye’deki 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), bireysel veriyi bir hak olarak tanımlamakta ve korumaya çalışmaktadır. Ancak Çin’in yaklaşımı, bireysel haklardan ziyade devlet güvenliği ve toplumsal düzeni öncelemekte; veriyi bir kamu varlığı olarak konumlandırmaktadır. Bu normatif çeşitlilik, veri egemenliğinin evrensel değil, kültürel ve jeopolitik bağlamlara göre farklı şekillendiğini göstermektedir.

Rousseau’nun genel irade anlayışı da dijital egemenlik bağlamında yeni bir tartışma alanı açmaktadır. Özellikle AB’nin veri politikaları, bireylerin dijital alandaki kolektif çıkarlarını gözetme çabasıyla Rousseaucu bir “ortak yarar” anlayışını yansıtmaktadır. Öte yandan, platformların kullanıcı katılımını sınırlayan algoritmik işleyişi, genel iradenin dijital dünyada ne ölçüde temsil edilebildiğini sorgulatmaktadır.

Dijital egemenlik çabaları aynı zamanda Zuboff’un “gözetim kapitalizmi” analizinde işaret ettiği güç asimetrisini de görünür kılmaktadır. Küresel teknoloji şirketlerinin dijital altyapı üzerindeki hâkimiyeti, “dijital kolonizasyon” riskini beraberinde getirmekte; kritik verilerin ve altyapıların yabancı aktörlerin kontrolüne geçmesine yol açmaktadır (Kurochkin &

Morozova, 2024, s. 68). Dijital teknolojilerin sınır ötesi doğası, siber saldırıların sıklığını artırmış; jeopolitik gerilimlerin dijital alana taşınması ise siber alanın giderek militarize edilmesine yol açmıştır (Kaloudis, 2024, s. 75; Timmers, 2023, s. 581; Zadorozhna, 2023, s. 24).

Devletler bu tehditleri bertaraf etmek için çok katmanlı stratejiler benimsemektedir. Çin, Rusya ve ABD gibi ülkeler, dijital altyapılarını güvence altına almak ve teknolojik bağımsızlıklarını artırmak amacıyla ulusal politikalar ve stratejik belgeler oluşturmuştur. Türkiye de benzer şekilde “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023)” ile kritik altyapıların korunması, yerli teknoloji üretiminin teşviki ve siber güvenlik kapasitesinin güçlendirilmesini hedeflemiştir. Yerelleştirme politikaları sayesinde hem ekonomik sürdürülebilirlik sağlanmakta hem de stratejik bağımlılıklar azaltılmaktadır (Shoker, 2022, ss. 70-71).

Küresel ölçekte ise farklı aktörler dijital egemenliği farklı araçlarla inşa etmektedir. ABD, dijital altyapılar ve yapay zekâdaki üstünlüğünü stratejik bir güç unsuru olarak kullanırken; AB, düzenleyici kapasitesiyle “dijital normatif güç” rolünü üstlenmektedir. Çin ise “Dijital İpek Yolu” girişimiyle, yalnızca kendi dijital bağımsızlığını pekiştirmeyi değil, aynı zamanda küresel düzeyde veri egemenliği vizyonunu yaygınlaştırmayı amaçlamaktadır. Türkiye gibi orta ölçekli güçler için ise dijital egemenlik, ulusal güvenlik stratejilerinin vazgeçilmez bir bileşeni haline gelmiştir.

Sonuç olarak, dijitalleşme devletlerin egemenlik ve güvenlik anlayışlarını yeniden şekillendirmiştir. Dijital egemenlik, yalnızca teknik bir kapasite değil; ulusal güvenlik, birey hakları ve uluslararası istikrarın kesişim noktasında yer alan stratejik bir kavramdır. Bu doğrultuda devletlerin, veri odaklı güvenlik politikalarını birey haklarını da gözetken dengeli bir dijital toplumsal sözleşme anlayışıyla bütünleştirmesi gerekmektedir. Küresel işbirliği ile ulusal çıkarların uyumlaştırılması, dijital egemenliğin hem iç hem dış güvenliğe katkı sunmasını sağlayacaktır.

Küresel Aktörler: Teknoloji Şirketleri ve Uluslararası Örgütler

Dijital egemenlik, artık yalnızca devletlerin ulusal dijital altyapıları üzerindeki kontrolüyle sınırlı değildir. Musiani (2022)’nin vurguladığı gibi, dijital teknolojilerin sınır aşan doğası egemenliğin salt devlet temelli bir yapı üzerinden tesis edilmesini zorlaştırmakta; bu boşluğu giderek daha fazla Büyük Teknoloji (Big Tech) şirketleri ve uluslararası örgütler doldurmaktadır. Bu aktörler, hem teknik kapasite hem de norm üretimi bağlamında dijital düzenin kurucu unsurlarına dönüşmüştür.

Teknoloji şirketleri, dijital ekosistemin yeni güç merkezleri haline gelmiştir. Google, Amazon, Meta, Apple ve Microsoft gibi ABD merkezli şirketler ile Alibaba ve Tencent gibi Çinli firmalar, sahip oldukları altyapı ve veri yönetimi kapasitesiyle birçok devletin ekonomik gücünü aşan bir etki yaratmaktadır. Zuboff (2019), bu süreci “gözetim kapitalizmi” olarak tanımlar; bireylerin dijital etkileşimlerinden elde edilen davranışsal veriler, ekonomik ve politik güce dönüştürülmekte ve devletlerin düzenleyici kapasitesini zorlamaktadır. Roberts (2024), bu

şirketlerin karar alma süreçlerinin demokratik meşruiyet eksikliğine dikkat çekerken, özellikle yapay zekâ geliştirme süreçlerinde şirketlerin belirleyici konumu meşruiyet sorununu daha da görünür kılmaktadır. Buna karşılık, Costa-Barbosa (2024), sivil toplumun ve yerel toplulukların katılımına dayalı alternatif dijital yönetim modellerini önererek platform kapitalizmine karşı daha kapsayıcı bir dijital egemenlik vizyonu geliştirmektedir.

Uluslararası örgütler ise dijital alanın normatif çerçevesini şekillendirmektedir. AB GDPR ve Dijital Hizmetler Yasası aracılığıyla bireysel veri haklarını Lockeçu anlamda “mülkiyetin korunması” ilkesi üzerinden güvence altına alırken (Lehuede, 2024), NATO siber güvenliği kolektif savunmanın ayrılmaz bir parçası olarak tanımlamıştır. Birleşmiş Milletler (BM) ise dijital hakları kalkınma hedefleriyle ilişkilendirerek Rousseaucu anlamda “genel irade” ve “ortak yarar” anlayışını dijital alana taşımaktadır (Pohle & Santaniello, 2024, s.675). Bununla birlikte, normatif çeşitlilik ciddi bir gerilim yaratmaktadır. AB’nin hak merkezli yaklaşımı ile Çin’in devlet güvenliği odaklı modeli arasındaki farklılık, küresel bir dijital toplumsal sözleşmenin inşasını zorlaştırmaktadır (“Data Sovereignty”, 2023).

Dijital egemenlik tartışmalarında altyapı meselesi de giderek ön plana çıkmaktadır. Yerel olarak kontrol edilen dijital altyapılar, devletlerin öz belirleme hakkını dijital alanda tesis etmeleri için kritik görülmektedir (Allgayer, 2022, s.791; Musiani, 2022, s. 788). Ancak bu hedefe ulaşırken temel zorluk, egemenlik ile yenilik arasındaki dengeyi kurabilmektir. Frattini ve arkadaşları (2024)’nın belirttiği gibi, teknolojik gelişmeyi engellemeden dijital özerkliği sağlamak, sağlam ve esnek yönetim modelleri gerektirmektedir.

Sonuç olarak, dijital toplumsal sözleşmenin uluslararası boyutu, devletler, teknoloji şirketleri ve uluslararası örgütler arasında sürekli yeniden şekillenen bir güç ve otorite dengesi üzerinden ilerlemektedir. Zinovieva ve Shitkov (2023), bu çok katmanlı yapının küresel dijital düzen için kalıcı olduğunu belirtir. Türkiye de bu çerçevede, NATO üyeliği kapsamında yürütülen siber güvenlik işbirliklerine ve uluslararası platformlardaki düzenleyici tartışmalara katılımıyla, dijital egemenliği yalnızca ulusal değil aynı zamanda küresel güvenlik meselesi olarak ele almaktadır. Ancak bu süreç yalnızca jeopolitik çıkarlarla sınırlı değildir; aynı zamanda toplumların en kırılgan birimlerinden biri olan aileyi de doğrudan etkilemektedir. Mahremiyet, çocuk hakları ve dijital eşitlik gibi insani güvenlik alanları, dijital egemenlik tartışmalarının ayrılmaz bir parçası haline gelmiştir. Dolayısıyla, dijitalleşmenin geleceği için çok taraflı, şeffaf ve insani güvenliği gözetten bir yönetim modeli kaçınılmazdır.

Ailenin İnsani Güvenlik Boyutu

Dijitalleşme, aileyi insani güvenlik açısından yeni kırılganlıkların merkezine yerleştirmektedir. Özellikle çocukların çevrim içi ortamlarda maruz kaldığı veri toplama uygulamaları, bireysel özgürlüklerin yanı sıra aile bütünlüğü açısından da ciddi riskler doğurmaktadır. Metra ve Dobelniece (2022), dijital mahremiyetin yalnızca bireysel bir hak değil, aynı zamanda ailevi ilişkilerin sürdürülebilirliği için kolektif bir güvenlik alanı olduğunu vurgulamaktadır.

Daha önceki bölümde tartışılan GDPR ve Big Tech düzenlemelerinden farklı olarak, aile bağlamında mahremiyet daha somut bir nitelik taşımaktadır. Çocukların dijital ortamlarda rızaları olmaksızın veri toplanması, ebeveynlerin çevrim içi davranışlarının aile içi dinamiklere yansımaları ve ev yaşamının sosyal medyaya taşınması, aile mahremiyetinin özgün kırılganlık alanlarını oluşturmaktadır. Bu nedenle mahremiyet, aile için yalnızca veri koruması değil, aynı zamanda kuşaklar arası güvenliğin, ev içi sınırların ve toplumsal değerlerin korunması anlamına gelmektedir.

Sosyo-ekonomik farklılıklar, dijital araçlara erişim ve okuryazarlık düzeylerindeki uçurumlar, özellikle düşük gelirli hanelerde çocukların eğitim ve güvenlik açısından dezavantajlı konuma düşmesine yol açmaktadır. UNICEF (2023) raporu, dijital uçurumun yalnızca teknik bir erişim meselesi olmadığını; çocuk hakları, fırsat eşitliği ve kuşaklar arası adalet gibi daha geniş kapsamlı sorunları tetiklediğini ortaya koymaktadır. Türkiye’de Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve MEB’in yürüttüğü projeler çocukların güvenli internet kullanımını desteklemeye çalışsa da, ebeveynlerin dijital yeterlilik eksiklikleri aile güvenliğinde boşluk yaratmaktadır.

Siber zorbalık, çevrim içi istismar, yanlış bilgilendirme ve dijital bağımlılık gibi tehditler, yalnızca bireyleri değil doğrudan aile kurumunu da zayıflatmaktadır. Zadorozhna (2023), bu tehditlerin aile kurumunun işlevselliğine zarar verdiğini ve politika yapıcılarının aile merkezli stratejiler geliştirmesi gerektiğini vurgulamaktadır. Devletlerin dijital egemenlik uygulamaları bu noktada aile güvenliğini koruma amacını taşısa da, koruma ile aşırı gözetim arasında hassas bir denge kurulması gerekmektedir (Chander & Sun, 2023, s.78). Bu denge, klasik Hobbesçu güvenlik vurgusunun ötesinde, doğrudan aile bireylerinin özerkliği ve mahremiyetine yönelik güncel bir tartışmayı gündeme getirmektedir.

Dijitalleşme, ebeveynler ile çocuklar arasındaki bilgi ve deneyim farkını büyütmekte, bu da aile içi iletişimde yeni gerilimler yaratmaktadır. Ebeveynlerin dijital okuryazarlığının artırılması, çocukların çevrim içi risklerden korunması ve güvenli dijital kullanımın teşvik edilmesi, aileyi bir bütün olarak güçlendirecek politika alanlarının başında gelmektedir. AB’nin Better Internet for Kids girişimi bu yönde iyi bir örnek oluştururken, Türkiye’de de benzer programların sürdürülebilir şekilde yaygınlaştırılması önem arz etmektedir.

Sonuç olarak, aile kurumu dijital çağda yalnızca toplumsal yapının temel taşı değil, aynı zamanda güvenlik riskleri karşısında en kırılgan birimdir. Mahremiyetin korunması, dijital eşitliğin sağlanması, çevrim içi tehditlere karşı koruma ve kuşaklar arası adaletin gözetilmesi, aile merkezli insani güvenliğin vazgeçilmez ilkeleridir. Devletin dijital egemenlik kapasitesini bu ilkeler doğrultusunda kullanması; birey hakları ile kolektif güvenlik arasında denge kuran kapsayıcı, etik ve sürdürülebilir politikaların geliştirilmesini zorunlu kılmaktadır.

Bu noktada, dijital toplumsal sözleşmenin yalnızca kuramsal bir tartışma değil, aynı zamanda somut politika tasarımları gerektiren bir alan olduğu açıktır. Bir sonraki bölüm, ulusal ve uluslararası düzeyde uygulanabilir politika önerilerini tartışarak aile merkezli dijital güvenlik yaklaşımını pratik bir yönetim çerçevesine dönüştürmeyi amaçlamaktadır.

Politika Önerileri: Aile Merkezli Dijital Güvenlik İçin Yeni Çerçeveler

Dijitalleşmenin aile yapısı üzerindeki çok boyutlu etkileri, ulusal düzeyde kapsamlı ve aile odaklı politika çerçevelerinin geliştirilmesini zorunlu kılmaktadır. Çocukların, ebeveynlerin ve aile bütünlüğünün çevrim içi risklere maruz kalması, yalnızca bireysel değil, aynı zamanda toplumsal güvenlik bağlamında da ele alınması gereken yapısal kırılganlıklar doğurmuştur. Türkiye gibi orta ölçekli devletler açısından bu kırılganlıkların etkin biçimde yönetimi, dijital hakların anayasal düzeyde güvenceye alınması, dijital okuryazarlığın güçlendirilmesi, aile odaklı siber güvenlik stratejilerinin oluşturulması ve yerli dijital çözümlerin geliştirilmesi yönünde politika üretimini gerekli kılmaktadır.

Bu doğrultuda atılması gereken ilk adım, dijital hakların anayasal düzeyde tanınmasıdır. Mahremiyet, veri güvenliği ve dijital eşitlik gibi hakların temel hak ve özgürlükler içinde düzenlenmesi, aile bireylerinin dijital ortamdaki konumunu hem hukuken hem de pratikte güçlendirecektir. Türkiye’de yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), bu alanda önemli bir temel sunmakla birlikte, özellikle çocukların verilerinin korunması konusunda yetersiz kalmaktadır (Liszkowska, 2024, s. 82). Bu nedenle, BM Çocuk Hakları Sözleşmesi ve Genel Yorum No. 25 ile uyumlu şekilde, çocuk odaklı özel bir Dijital Haklar Yasası’nın hayata geçirilmesi gerekmektedir (Roman-Urrestarazu v.d., 2022; Sommer, 2024, s. 125).

Dijital beceri eşitsizliğini azaltmaya yönelik bir diğer öncelik, ebeveyn ve çocuklara yönelik dijital okuryazarlık programlarının güçlendirilmesidir. Türkiye’de yapılan araştırmalar, hem çocukların yeterli dijital beceriye sahip olmadığını hem de ebeveynlerin çevrim içi riskleri yönetmede yetersiz kaldığını göstermektedir (Kaşıkçı v.d., 2014, s. 235). MEB ve BTK tarafından yürütülen mevcut programlar olumlu örnekler sunmaktadır; ancak bu eğitimlerin eleştirel dijital farkındalık, etik kullanım becerileri ve ebeveyn-çocuk iş birliğine dayalı içeriklerle daha kapsayıcı hâle getirilmesi gerekmektedir (Oshodi v.d., 2024, s. 2298).

Aileleri doğrudan etkileyen dijital tehditlerle mücadelede, aile merkezli siber güvenlik stratejilerinin oluşturulması bir diğer gerekliliktir. Siber zorbalık, çevrim içi istismar, yanlış bilgilendirme ve dijital bağımlılık gibi olgular yalnızca bireyleri değil, doğrudan aile kurumunu zayıflatmaktadır. Bu bağlamda, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023) gibi belgeler yeniden ele alınmalı; farkındalık kampanyaları, ebeveyn denetim araçları ve dijital ebeveynlik modelleri gibi uygulamalar ulusal stratejilerin merkezine yerleştirilmelidir (Yurdakul et al., 2013, s. 889; Gündoğdu, 2023, s. 1335).

Ulusal dijital güvenlik kapasitesinin güçlendirilmesinde yerli teknolojilerin rolü de göz ardı edilmemelidir. Kültürel değerlere duyarlı dijital platformların geliştirilmesi, stratejik dışa bağımlılığı azaltırken aynı zamanda ailelerin daha güvenilir hizmetlere erişimini sağlayacaktır. Tüm bu politika başlıkları, sadece mevzuat üretimine indirgenmemeli; çok sektörlü iş birliği, uygulamada denetim mekanizmaları ve sürekli değerlendirme süreçleri ile desteklenmelidir. Ancak bu şekilde hem sürdürülebilir hem de aile merkezli bir dijital güvenlik çerçevesi kurulabilir (Sommer, 2024, s.146).

Dijitalleşmenin sınır ötesi doğası, yalnızca ulusal politikalarla sınırlı kalan çözümlerin yetersizliğini ortaya koymakta; veri akışları, yapay zekâ uygulamaları ve dijital platformların karmaşık yapısı, devletlerin tek başına denetim kapasitesini aşmaktadır. Bu nedenle dijital güvenlik ve mahremiyetin korunması, çok aktörlü ve çok düzeyli uluslararası iş birliği gerektirmektedir. Özellikle aileler ve çocuklar gibi kırılgan grupların korunması, küresel normların uyumlaştırılmasını zorunlu hale getirmektedir.

AB, dijital hakların korunmasında en güçlü normatif örneklerden birini sunmaktadır. GDPR, kişisel verileri Locke’cu bir yaklaşımla mülkiyet hakkının uzantısı olarak tanımlayarak bireylerin dijital ortamda güçlendirilmesini hedeflemektedir. GDPR yalnızca AB vatandaşlarını değil, AB pazarıyla etkileşimde bulunan tüm şirketleri bağladığı için küresel ölçekte etki üretmektedir (Lehuede, 2024; Milkaite, 2023, s. 412). Buna ek olarak, “Çocuklar için Daha İyi İnternet” girişimi, güvenliğin ötesinde çocuklara daha anlamlı ve geliştirici çevrim içi deneyimler sunmayı amaçlamakta; kamu kurumları, teknoloji sektörü ve sivil toplum arasında işbirliğini teşvik etmektedir (O’Neill v.d., 2013).

BM ise dijital hakları yalnızca bireysel özgürlükler bağlamında değil, sürdürülebilir kalkınma hedefleri doğrultusunda da ele almaktadır. UNICEF’in çalışmaları, dijital uçurumun çocuk hakları ve kuşaklar arası adalet açısından küresel bir tehdit olduğunu göstermekte; bu nedenle çocukların çevrim içi güvenliğinin uluslararası düzeyde ortak normlarla güvence altına alınmasını zorunlu kılmaktadır (UNICEF, 2023). BM Çocuk Hakları Sözleşmesi (UNCRC) ve Genel Yorum No. 25, dijital çağda mahremiyet, güvenlik ve bilgiye erişim arasındaki dengeyi kuran ilkeleri ortaya koyarak politika yapıcılara yol göstermektedir (Sommer, 2024, s. 142; Roman-Urrestarazu v.d., 2022).

NATO ise dijitalleşmenin güvenlik boyutuna odaklanmakta ve siber tehditleri kolektif savunma stratejisinin merkezine yerleştirmektedir. 2021 ve 2023 zirvelerinde alınan kararlar, Hobbes’cu bir anlayışla dijital tehditlere karşı güçlü merkezi otorite ihtiyacını yansıtmaktadır (Hathaway, 2010, s. 22). Ancak bu devlet merkezli güvenlik yaklaşımı, aile gibi mikro düzeydeki insani güvenlik ihtiyaçlarını ikincil plana itmekte; bu nedenle daha kapsayıcı, çok paydaşlı normların gerekliliği ortaya çıkmaktadır (Kettmann & Müller, 2025, s. 115).

Bununla birlikte, büyük teknoloji şirketlerinin küresel ölçekte artan etkisi, uluslararası düzenlemelerin en büyük sınaması olarak öne çıkmaktadır. Zuboff’un (2019) tanımladığı “gözetim kapitalizmi” modeli, bireylerin davranışsal verilerini ekonomik güce dönüştürerek yalnızca devletlerin değil ailelerin de mahremiyetini tehdit etmektedir. Bu durum, yalnızca devletler arası işbirliğini değil, aynı zamanda yerel topluluklar, ebeveynler ve sivil toplum örgütlerinin katılımıyla çok katmanlı işbirliği mekanizmalarının güçlendirilmesini gerekli kılmaktadır (Costa-Barbosa v.d., 2024).

Bu çerçevede iki temel politika önerisi öne çıkmaktadır:

1. Çocuk Dijital Hakları Yasası: Ulusal düzenlemelerin küresel standartlarla uyumlu hale getirilmesi, yalnızca çocukların verilerinin korunmasını değil, aynı zamanda aile bütünlüğünün dijital ortamda güvence altına alınmasını sağlayacaktır. Böyle bir yasa,

ebeveynlerin sorumluluklarını netleştirirken, devletlerin ve teknoloji şirketlerinin çocuk dostu politikalar üretmesini zorunlu kılacaktır (Roman-Urrestarazu et al., 2022).

2. Dijital Vatandaşlık Eğitimi: Çocukların ve ebeveynlerin dijital ortamda karşılaşabilecekleri risklere karşı daha dirençli hale gelmesi için yalnızca teknik bilgi değil, aynı zamanda etik, kültürel ve toplumsal boyutları da kapsayan eğitim programları yaygınlaştırılmalıdır. Bu yaklaşım, aileyi bir bütün olarak güçlendirirken, kuşaklar arası güvenlik ve adaletin de temelini atacaktır.

Bu iki öneri, dijital güvenliğin yalnızca devletlerarası normlarla değil, aynı zamanda aile merkezli insani güvenlik politikalarıyla tamamlanması gerektiğini göstermektedir. Dolayısıyla bir sonraki bölüm, ulusal ve uluslararası düzeyde uygulanabilir politika çerçevelerini tartışarak, dijital toplumsal sözleşmenin aile odaklı bir yönetim pratiğine nasıl dönüştürülebileceğini ele alacaktır.

Dijitalleşmenin küresel ve çok katmanlı doğası, yalnızca devlet merkezli politikalarla yönetilemeyecek kadar karmaşık bir yapı oluşturmıştır. Veri akışları, algoritmik süreçler, yapay zekâ uygulamaları ve dijital platformların aile yapısı üzerindeki etkileri, daha kapsayıcı ve işbirliğine dayalı bir yönetim modelini zorunlu kılmaktadır. Çünkü dijital tehditler, yalnızca teknik değil, aynı zamanda sosyal, etik ve kültürel boyutlara sahiptir; bu nedenle çözüm de tek aktörlü olamaz. Bu çerçevede, çok paydaşlı yönetim, dijital çağda aile merkezli güvenliğin tesisinde temel yaklaşımlardan biri haline gelmiştir. Devletlerin düzenleyici gücü, teknoloji şirketlerinin teknik altyapısı ve yenilik potansiyeli ile sivil toplumun etik denetim ve katılım mekanizmaları, bu modelin üç temel ayağını oluşturmaktadır.

Öncelikli olarak, teknoloji şirketlerinin şeffaflık ve hesap verebilirlik sorumluluğu, bu yönetim modelinin temel taşıdır. Şirketler; veri toplama uygulamaları, algoritmik karar süreçleri ve kullanıcı profillemeye gibi işlemleri açık şekilde kamuoyuyla paylaşmalı, özellikle çocukların kişisel verilerinin korunması konusunda özel önlemler almalıdır. Veri kullanım pratiklerinin yaşa uygun gizlilik ilkeleriyle uyumlu hale getirilmesi, çocukların ve ailelerin dijital ortamda korunması için kritik bir gerekliliktir (Roberts, 2024; Pothong & Livingstone, 2023).

Bu noktada, çocuk verilerinin ticari kullanımının sınırlandırılması, çocuk merkezli dijital güvenliğin olmazsa olmazıdır. Zuboff'un (2019) ortaya koyduğu "gözetim kapitalizmi" bağlamında, çocukların çevrim içi etkileşimlerinden elde edilen verilerin ticarileştirilmesi, yalnızca mahremiyetin ihlali değil, aynı zamanda çocuğun gelişimsel bütünlüğüne yönelik bir tehdittir. Bu nedenle, çocuk verilerinin yalnızca onların yararına kullanılmasını esas alan, veri toplama sürecini en aza indiren ve aile dostu tasarım ilkeleriyle desteklenen bir yaklaşım benimsenmelidir (O'Neill v.d., 2013; Gupta v.d., 2023).

Aile dostu dijital tasarım anlayışı, yaşa uygun dijital ürün ve hizmetlerin geliştirilmesini; çocukları zararlı içeriklerden koruyan filtreleme, sınırlama ve yönlendirme mekanizmalarının dijital sistemlere entegre edilmesini içermelidir. Bu tasarım yaklaşımı, çocukların gelişim aşamalarına uygun çözümler sunmalı; zararlı içerikleri filtreleyen, ebeveyn rehberliğini teşvik

eden ve güvenli dijital deneyimleri destekleyen unsurları barındırmalıdır. Bunun yanı sıra, ebeveynlerin dijital okuryazarlıklarını ve rehberlik rollerini güçlendirecek araç ve eğitim programlarının sağlanması, ailelerin dijital dünyada daha bilinçli ve koruyucu bir tutum geliştirmesini kolaylaştıracaktır (Gupta v.d., 2023; Oshodi v.d., 2024, s. 2304).

Bu çerçevede, devlet–şirket–sivil toplum iş birlikleri, yalnızca teknik düzenlemeler değil, aynı zamanda demokratik meşruiyeti önceleyen bir dijital toplumsal sözleşmenin inşası için elzemdir. Devletler, çocuk haklarını ve dijital güvenliği koruyan yasal düzenlemeleri oluşturmalı; teknoloji şirketleri güvenli dijital altyapılar sunmalı, sivil toplum ise şeffaflık ve etik denetim mekanizmalarıyla sürece dahil olmalıdır (Costa-Barbosa v.d., 2024; Livingstone v.d., 2016). Böylece, dijital alanın sadece koruyucu değil, aynı zamanda kapsayıcı ve adil bir ortam haline gelmesi sağlanabilir.

Bu yaklaşım aynı zamanda küresel dijital haklar çerçevesi oluşturma yönünde bir adım olabilir. Roman-Urrestarazu ve arkadaşları (2022), dünya çapında çocukların dijital teknolojilere güvenli ve adil erişimini sağlamak üzere bir Çocuk Dijital Hakları Bildirgesi önerisinde bulunmuş; bu çerçevenin, ulusal ve bölgesel düzenlemelere yön verebileceğini savunmuştur. İnternet yönetim organlarının çocukların sadece korunma haklarını değil, katılım ve gelişim haklarını da gözetin bir yaklaşıma geçmesi gerektiği vurgulanmaktadır (Livingstone v.,d. 2016).

Ayrıca, dijital çocuk korumasına yönelik politikaların bilimsel araştırmalara dayandırılması, yani çocukların gelişimsel ihtiyaçları ve kırılganlıklarına uygun biçimde tasarlanması, düzenlemelerin etkinliğini artıracaktır (Gilad v.d., 2023, s. 1298). Bu tür çabalar, yalnızca çocukları dijital tehditlerden korumayı değil; aynı zamanda dijital fırsatlara eşit, güvenli ve anlamlı erişim sağlamayı da hedeflemelidir.

Ancak bu tür çok paydaşlı yönetim modellerinin uygulanmasında önemli zorluklar bulunmaktadır. Küresel standartlara ulaşma çabası, yerel bağlamların çeşitliliği nedeniyle esneklik ve adaptasyon gerektirirken; ticari çıkarlar ile çocuk hakları gibi etik sorumluluklar arasındaki denge, sürekli diyalog ve işbirliği gerektiren karmaşık bir süreçtir. Bu nedenle, sürdürülebilir ve çocuk dostu bir dijital ekosistem inşa edebilmek için tüm paydaşlar arasında güvene dayalı, şeffaf ve bilim temelli bir işbirliği modeli geliştirilmelidir. Sonuç olarak, çok paydaşlı yönetim yalnızca bir yönetim tercihi değil, dijital çağın karmaşık risk yapısı içinde çocukların ve ailelerin güvenliğini sağlayacak yegâne sürdürülebilir modeldir.

SONUÇ

Dijitalleşme, yalnızca teknolojik araçların artışı değil; birey, aile, devlet ve küresel aktörler arasındaki ilişkilerin mahiyetini kökten dönüştüren çok boyutlu bir toplumsal dönüşümdür. Bu çalışma, klasik toplumsal sözleşme teorilerinin (Hobbes, Locke, Rousseau) normatif mirasını dijital çağın özgün riskleriyle ilişkilendirerek, aile kurumunun insani güvenlik çerçevesinde nasıl yeniden konumlandığını analiz etmiştir. Böylece literatürde sıklıkla ayrı kulvarlarda ele alınan dijitalleşme, güvenlik ve aile ilişkileri arasında kuramsal bir köprü inşa edilmiştir.

Analitik olarak, dijitalleşme sürecinin güvenlik–özgürlük dengesi üzerinde üç düzeyli bir yeniden tanımlama yarattığı görülmektedir. Devletler açısından dijital egemenlik, yalnızca altyapı kontrolü değil; aynı zamanda bireysel hakların korunması, ulusal güvenliğin sürdürülebilirliği ve aile yapısının güçlendirilmesi bağlamında stratejik bir politika alanına dönüşmüştür. Teknoloji şirketleri ve uluslararası örgütler, norm üretimi ve altyapı denetimi yoluyla dijital düzenin yeni kurucu aktörleri haline gelirken, aileler dijital çağın en kırılgan ve en az hazırlıklı güvenlik birimi olarak öne çıkmaktadır. Bu kırılganlık, özellikle çocuk verilerinin ticarileştirilmesi, ebeveynlerin dijital yetersizliği ve kuşaklar arası iletişim kopuklukları üzerinden kendini göstermektedir. Nitekim AB’nin 2021’de yürürlüğe koyduğu Çocukların Çevrim İçi Güvenliği Stratejisi ve TikTok/Meta gibi platformlara açılan davalar, çocuk verilerinin rızasız toplanmasının hem hukuki hem de etik açıdan küresel bir tartışma konusu haline geldiğini göstermektedir Çalışmanın en belirgin katkısı, dijitalleşme sürecini sadece bireysel ya da teknik bir dönüşüm olarak değil, toplumsal sözleşmenin yeniden inşası olarak yorumlamasıdır. Klasik sözleşme teorilerinin kavramsal arka planına sadık kalarak geliştirilen bu yorum, hem literatürdeki kuramsal boşluğu doldurmakta hem de yeni bir araştırma gündemi önermektedir.

Politika düzeyinde, çok katmanlı bir yönetim çerçevesi önerilmektedir. Ulusal düzeyde, dijital hakların anayasal güvenceye alınması, çocuk odaklı veri koruma yasalarının geliştirilmesi ve aile merkezli siber güvenlik stratejilerinin oluşturulması gerekmektedir. Uluslararası düzeyde, AB’nin GDPR ve UNICEF’in çocuk hakları odaklı çerçeveleri gibi normatif örneklerin küresel çapta uyumlaştırılması kritik bir önceliktir. Çok paydaşlı düzeyde ise devlet, teknoloji şirketleri ve sivil toplum arasında şeffaflık, etik denetim ve eşgüdüm mekanizmalarının kurumsallaştırılması, dijital çağda aile merkezli güvenliğin sürdürülebilirliği açısından zorunludur.

Son olarak, bu çalışma, dijital çağın toplumsal sözleşmesini yeniden düşünmek için bir zemin sunmakta; ancak bu zemin yeni risk alanlarının derinlemesine incelenmesini de gerekli kılmaktadır. Yapay zekâ algoritmalarının karar alma süreçlerine etkisi, metaverse gibi alternatif dijital yaşam alanlarında çocukların maruz kaldığı tehditler, biyometrik gözetim teknolojilerinin aile içi dinamikleri nasıl dönüştürdüğü ve kuşaklar arası dijital eşitsizliklerin yarattığı sosyal gerilimler, geleceğin en acil araştırma alanları arasında yer almaktadır.

Dijital çağın toplumsal sözleşmesinin adil, kapsayıcı ve insani güvenliğe duyarlı biçimde kurulabilmesi için bu tür araştırmaların hem akademik araştırmalar hem de politika tasarımları açısından önceliklendirilmesi gerekmektedir.

KAYNAKÇA

Allgayer, H. (2022). Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, 25(6), 785–800. <https://doi.org/10.1080/1369118x.2022.2049850>

- Baumgold, D. (2010). *Contract Theory in Historical Context: Essays on Grotius, Hobbes, and Locke*. Brill's *Studies in Intellectual History*, 187. Brill. <https://doi.org/10.1163/ej.9789004184251.i-190.2>
- Berners-Lee, T. (2018, October 22). *One small step for the Web*, Inrupt Blog. Retrieved from <https://www.inrupt.com/blog/one-small-step-for-the-web>
- Castells, M. (2000). The rise of the network society: The information age. *Economy, society and culture*. Volume I (2nd ed.). Wiley-Blackwell. <https://doi.org/10.1002/9781444319514>
- Castells, M. (2004). *The network society: A cross-cultural perspective*. Edward Elgar Publishing.
- Chander, A., & Sun, H. (2023). Digital sovereignty as double-edged sword. In *Data sovereignty* (pp. 72–88). Oxford University Press. <https://doi.org/10.1093/oso/9780197582794.003.0004>
- Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
- Costa-Barbosa, A., Herlo, B., & Joost, G. (2024). Digital Sovereignty in times of AI: between perils of hegemonic agendas and possibilities of alternative approaches. *Liinc Em Revista*, 20(2). <https://doi.org/10.18617/liinc.v20i2.7312>
- Data Sovereignty*. (2023). Oxford University Press. <https://doi.org/10.1093/oso/9780197582794.001.0001>
- Foini, D. (2023, February 17). *Personal autonomy and surveillance capitalism: possible future developments* [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2302.08946>
- Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 3(59). <https://doi.org/10.1007/s44206-024-00146-7>
- Gilad, M., Fishbein, D., Nave, G., & Geslevich Packin, N. (2023). Science for policy to protect children in cyberspace. *Science*, 379(6639), 1294–1297. <https://doi.org/10.1126/science.ade9447>
- Gupta, S., Kumari, S., & Sugandh, U. (2023). *Protecting Children's Data from Cybersecurity Attacks to Prevent Child Sexual Abuse: A Techno-Legal Approach*. 1–7. <https://doi.org/10.1109/iccsai59793.2023.10421403>
- Gündoğdu, S. (2023). Uluslararası politikada bir etki aracı olarak siber güvenlik ve Türkiye'nin siber güvenlik politikası uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM), *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33(3), 1325–1337. <https://doi.org/10.18069/firatsbed.1261707>

- Hathaway, M. E. (2010). Toward a Closer Digital Alliance. *SAIS Review*, 30(2), 21–31. <https://doi.org/10.1353/SAIS.2016.0020>
- Heyman, S. J. (2018). The Light of Nature: John Locke, Natural Rights, and the Origins of American Religious Liberty. *Marquette Law Review*, 101(3), 705–758. Retrieved from <https://scholarship.law.marquette.edu/mulr/vol101/iss3/4>
- Hiller Marguerat, S. (2014). *The origins of property rights: A comparison on the basis of John Locke's concept of property and his natural law limits based on reason* (Doctoral thesis, University of Geneva). <https://doi.org/10.13097/archive-ouverte/unige:36849>
- Hiniker, A., Schoenebeck, S. Y., & Kientz, J. A. (2016). Not at the dinner table: Parents' and children's perspectives on family technology rules. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)* (s. 1376–1389). Association for Computing Machinery. <https://doi.org/10.1145/2818048.2819940>
- Hobbes, T. (2017). *Leviathan* (R. Tuck, Ed.). Cambridge University Press. (Original work published 1651)
- Kaloudis, M. (2024). Digital sovereignty as a weapon of diplomacy in cyber warfare in democracies. In *National security in the digital and information age* (pp. 72–88). IntechOpen. <https://doi.org/10.5772/intechopen.1005231>
- Karaduman, İ. C. (2020, 17 Mayıs). Thomas Hobbes ve Leviathan'ı Üzerine Bir İnceleme: Yönetim Bilimi'ni İçeriye Almak. *Uluslararası Yönetim Akademisi Dergisi*, 3(1), 114–137. <https://doi.org/10.33712/mana.687980>
- Kaşıkcı, D. N., Çağıltay, K., Karakuş Yılmaz, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim*, 39(171), 230–243.
- Kettemann, M. C., & Müller, M. (2025). 'This is not a drill': international law and protection of cybersecurity. 110–125. <https://doi.org/10.4337/9781035308514.00014>
- Konuk Sommer, B. (2025). Birleşmiş Milletler Çocuk Hakları Komitesi'nin 25 no'lu genel yorumu kapsamında dijital ortamda çocuk haklarının korunmasında mahremiyet, güvenlik ve bilgiye erişim dengesi , *İnsan Hakları Yıllığı*, 42(2), 123–154. <https://doi.org/10.69958/ihy.1593592>
- Kurochkin, A., & Morozova, S. (2024). Digital colonization as a threat to national security. *Politicheskaya Ekspertiza*, 20(1), 64–72. <https://doi.org/10.21638/spbu23.2024.105>
- Lehuedé, S. (2024). An alternative planetary future? Digital sovereignty frameworks and the decolonial option. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517231221778>

- Liszkowska, D. (2024). Türkiye's cybersecurity policy framework. *Cybersecurity and Law*, 11(1), 79–91. <https://doi.org/10.35467/cal/187262>
- Locke, J. (1988). *Two treatises of government* (P. Laslett, Ed.). Cambridge University Press. (Original work published 1689).
- Metra, R., & Dobelniece, S. (2022, May). *Society in the shackles of surveillance capitalism*. In *Proceedings of the 2022 International Conference "Economic Science for Rural Development"* (No. 56, pp. 319–329). Jelgava: LLU ESAF. <https://doi.org/10.22616/ESRD.2022.56.031>
- Milkaite, I. (2023). *Strengthening Children's Rights to Privacy and Data Protection in the Digital Environment: Walking the Tightrope in the EU*. 391–436. <https://doi.org/10.1017/9781839704543.014>
- Mishra, H. (2023). *Personal autonomy and surveillance capitalism: possible future developments*. <https://doi.org/10.48550/arxiv.2302.08946>
- Musiani, F. (2022). *Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices*. 25, 785–800. <https://doi.org/10.1080/1369118X.2022.2049850>
- Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance?, *Policy & Internet*, 16(4), 672–691. <https://doi.org/10.1002/poi3.426>
- Roberts, H. (2024). Digital sovereignty and artificial intelligence: a normative approach. *Ethics and Information Technology*, 26(4). <https://doi.org/10.1007/s10676-024-09810-5>
- Roman-Urrestarazu, A., Kinsey, J., & van Kessel, R. (2022). A Bill of Children's Digital Rights Is Required to Improve and Sustain Children's Futures Globally. *JAMA Pediatrics*, 176(11), 1064. <https://doi.org/10.1001/jamapediatrics.2022.3418>
- O'Neill, B., Staksrud, E., & McLaughlin, S. (2013). *Towards a better internet for children? Policy pillars, players and paradoxes*. Göteborg: Nordicom. ISBN 978-91-86523-72-5.
- Oshodi, A. N., Adelodun, M. O., Anyanwu, E. C., & Majebi, N. L. (2024). Combining parental controls and educational programs to enhance child safety online effectively. *International Journal of Applied Research in Social Sciences*, 6(9), 2293–2314. <https://doi.org/10.51594/ijarss.v6i9.1592>
- Pothong, K., & Livingstone, S. (2023). Child rights by design: unboxing children from the child-only digital corner. *AoIR Selected Papers of Internet Research*. <https://doi.org/10.5210/spir.v2022i0.13072>
- Rousseau, J.-J. (1997). *The social contract* (V. Gourevitch, Ed.). Cambridge University Press. (Original work published 1762).

- Sandel, Michael J, 'Locke: Property Rights', in Michael J Sandel (ed.), *Justice: A Reader* (New York, NY, 2007; online edn, Oxford Academic, 31 Oct. 2023), <https://doi.org/10.1093/oso/9780195335118.003.0004>, accessed 27 Aug. 2025.
- Shoker, A. (2022). *Digital Sovereignty Strategies for Every Nation*. *abs/2307.01791*(1), 56–72. <https://doi.org/10.5604/01.3001.0016.0943>
- Song, J. (2013). Freedom under the general will. *Philosophical Thought*, **49**, 85–113. Seoul National University, Philosophy Institute.
- Sreenivasan, G. (2000). What Is the General Will? *The Philosophical Review*, *109*(4), 545–581. <https://doi.org/10.2307/2693624>
- The Editors of Encyclopaedia Britannica. (2025, 31 Temmuz). Social contract: Definition, examples, Hobbes, Locke, & Rousseau. In *Encyclopaedia Britannica*. Retrieved from <https://www.britannica.com/topic/social-contract>
- Timmers, P. (2023). Sovereignty in the Digital Age. In H. Werthner, C. Ghezzi, J. Kramer, J. Nida-Rümelin, B. Nuseibeh, E. Prem, & A. Stanger (Eds.), *Introduction to Digital Humanism* (pp. 571–592). Springer. https://doi.org/10.1007/978-3-031-45304-5_36
- UNICEF. (2023). *Children's rights in the digital environment* [Discussion paper]. UNICEF Discussion Paper Series. Retrieved from <https://www.unicef.org/globalinsight>
- Venkatesh, N. (2021). *Surveillance capitalism: a Marx-inspired account*. *Philosophy*, *96*(3), 359–385. <https://doi.org/10.1017/S0031819121000164>
- Waldron, J. (1984). Locke, Tully, and the Regulation of Property. *Political Studies*, *32*(1), 98–106. <https://doi.org/10.1111/j.1467-9248.1984.tb00168.x>
- Yolton, J. W. (1958). Locke on the law of nature. *The Philosophical Review*, *67*(4), 477–498. <https://doi.org/10.2307/2182945>
- Yurdakul, I. K., Dönmez, O., Yaman, F., & Odabaşı, H. F. (2013). Dijital Ebeveynlik ve Değişen Roller. *Gaziantep University Journal of Social Sciences*, *12*(4), 883–896. <https://dergipark.org.tr/tr/download/article-file/223235>
- Zadorozhna, A. (2023). Digital technologies as a factor of national security of Ukraine. *Vadyba – Journal of Management*, *39*(2), 23–29. Retrieved from <https://www.ceeol.com/search/article-detail?id=1197198>
- Zinovieva, E., & Shitkov, S. (2023). Sovereignty as practice in digital age. In A. Baykov & E. Zinovieva (Eds.), *Digital International Relations* (pp. 75–90). Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-99-3467-6_5
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.