

DİJİTAL DEVLET YÖNETİMİNDE DİJİTALLEŞME, YAPAY ZEKÂ VE SİBER GÜVENLİK (KURAMSAL BAKIŞ)¹

DIGITALIZATION, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN
DIGITAL STATE ADMINISTRATION (THORETICAL PERSPECTIVE)

Doç. Dr. Ayşe YILDIZ ÖZSALMANLI

Muğla Sıtkı Koçman Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi
Bölümü, Muğla-Türkiye

ayseyildiz@mu.edu.tr, <https://orcid.org/0000-0002-9533-3478>

Emre ŞAHİN

Muğla Sıtkı Koçman Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi ABD. Doktora
Programı, Muğla-Türkiye

emresahin7@posta.mu.edu.tr, <https://orcid.org/0009-0003-8759-8577>

ÖZET

Dijitalleşme yönlü kavramları artık, yaşantımızın her alanında çok sıkça görmekteyiz. Ayrıca kamu yönetiminde dijital devlet uygulamaları, hızla ve daha da yoğun biçimde tatbik edilmektedir. Yine sosyal medyanın önemi toplum ve devlet açısından artmıştır. Lakin artık kişiler, özel sektör ya da kamu örgütlerinin sunduğu hizmetlere çok daha etkin ve verimli ulaşmaktadır. E-devlet üzerinden vatandaşlar, devlet kurumlarından dijital olarak bilgi edinme, talep, şikâyet, belge isteme şeklinde iletişime geçmektedir. Dijital kanallarla vatandaşların yönetime katılımı, yönetişim ve kamuoyu denetimi açısından faydalıdır. Diğer taraftan dijital dünyada ve dijital devlet yönetiminde ciddi etik sorunlar ile yasal yükümlülük gerektiren bazı problemler vardır. Örneğin dijital devlet yönetimi, yapay zekâ, büyük veri, blok zincir, teknopoli, siber güvenlik gibi konularda bilgi ve farkındalık eksiktir. Devletlerin bu konularda yasal düzenlemeleri (varsa), uygulanmalıdır. Kişilere dijital dünya hakkında teorik ve uygulamalı eğitimler verilmelidir. Çok yönlü denetim de önemlidir. Çalışmada konuya teorik ve evrensel açıdan yaklaşılmıştır. Sosyal medya, dijital devlet, dijital etik, dijital aktivizm, dijital kimlikler, büyük veri, blok zincir teknolojisi, yapay zekâ, yapay zekâ etiği, siber güvenlik, siber zorbalık, siber suçlar gibi kavramlar ele alınmış ve incelenmiştir. Bu konularda kuramsal bilgiler verilmiş ve sonuç kısmında bu konuda değerlendirmeler yapılmıştır.

Anahtar Kelimeler: Dijital devlet, dijital etik, dijital eşitsizlik, yapay zekâ, dijital kimlik, siber suçlar, siber güvenlik.

ABSTRACT

We now frequently see digitalization-related concepts in every aspect of our lives. Furthermore, digital government applications are being implemented rapidly and more intensively in public administration. The importance of social media has also increased for both society and the state. However, individuals now access services provided by private sectors and public organizations much more effectively and efficiently. Through e-government, citizens communicate with government institutions digitally to obtain information, submit requests, complaints, and request documents. Citizen participation in

¹Bu çalışma tarafımızdan, “Dijital Devlet Yönetimi Kavramları Üzerine Teorik Bir Değerlendirme” başlığı ile, Bursa’da “International 7th Bursa Scientific Researches Congress (14-15.06.2025)’de (<https://ubsder.org.tr/7-uluslararası-bursa-bilimsel-arastirmalar-kongresi/>), online-sözlü bildiri olarak 15.06.2025’de sunulmuştur. Kongre sonrası çalışmanın bölümleri ve içeriği yeniden gözden geçirilmiş ve yeni başlığı ile bu makale hazırlanmıştır.

governance through digital channels is beneficial for governance and public oversight. On the other hand, there are serious ethical issues and legal obligations in the digital world and digital government administration. For example, there is a lack of knowledge and awareness regarding digital government administration, artificial intelligence, big data, blockchain, technopolitics, and cybersecurity. Government regulations (if any) on these issues should be implemented. Individuals should be provided with theoretical and practical training on the digital world. Multifaceted oversight is also important. This study approaches the subject from a theoretical and universal perspective. Concepts such as social media, digital government, digital ethics, digital activism, digital identities, big data, blockchain technology, artificial intelligence, AI ethics, cybersecurity, cyberbullying, and cybercrime are discussed and examined. Theoretical information on these topics is provided, and evaluations are made in the conclusion.

Keywords: Digital state, digital ethics, digital inequality, artificial intelligence, digital identity, cybercrime, cybersecurity.

1.GİRİŞ

Bugün artık devletler ve toplumlar açısından küreselleşmiş bu dünya gerçek olmuştur. Literatürde 30 yıl öncesi belirtilen “dünya vatandaşlığı, küresel köy, medeniyetler arası diyalog, küçük ve yerel güzeldir, kültürlerarası diyalog, tarihi ve sosyo-kültürel değerleriyle başka halkların gönüllerinde taht kurmak” gibi söylemler yerelde bizzat yaşanmaktadır. Bilgi ve iletişim teknolojilerinde devasa gelişmelerin ardından, teknopolinin yayılım hızı ve etki alanı, yerel, ulusal, bölgesel ve küresel ölçekte genişlemiştir. Diğer yandan insanlar tarafından, yapay zekâ teknolojisi robotlara suç isnat edilebilir ve bu sonuca giden bir yargı kararı verilebilir. Bu anda, insanlar illegal işler yapabilen ama suçlamayı yapay zekâyâ yansıtan/atan ve sonuçta hukuken masum durumuna gelebilir. Konu, hukuk ve etik bakış açısıyla irdelenmeye müsaittir.

Misal olarak 2018’de Bowles, bir akıllı evi, aile içinde şiddete başvuran kişi hacklerse, suçlunun kim (evdeki kişi mi, yapay zekâ mı) olacağını sormuştur (Bokor, 2021: 161). Honda imali Robot Asimo, arkasında çantası olan bir genç görünümündedir. Asimo ile el sıkılmak istenmiş ve bir insan gibi cevap vermiştir. Yapay zekâ destekli bir program yüklenmesi sonucunda bu yeteneği kazanmıştır. Ama gerekli program olmazsa aslında bir teknolojik alettir. Diğer yandan yapay zekâ destekli bir savaşta, bir “savaş suçu” işlenirse burada suçlu kim olmalıdır. Bu yapay zekâyâ program yükleyen firma mı, yapay zekâyı hizmete sokan kurum mu, savaşması görevi yüklenen yapay zekânın bizzat kendisi mi olacağını sorgulamıştır. Yapay zekânın kendisi sorumlu görülürse, kişiler kendi yapamadıkları kötülükleri yapay zekâyla yapmaya yeltenebilir. İnsanlar eylemlerinin gereği olan etik ve hukuki sorumluktan kaçınabilir hatta insanların sorumlulukları hukuken sona erebilir. Savaş için ve suç işleyebilecek kapasitede yapay zekâ teknolojisi ürünü robotlar üretilmesi, etik ve hukuki değildir (Öztürk Dilek, 2019: 50-51). Akademik olarak da son dönemlerde çok tartışılan birkaç soru böyledir.

Günümüzde sanal dünyada hızla “nesnelerin interneti” ve “hizmetlerin interneti” denilen yeni bir aşamaya geçilmiştir (Çeliksoy ve Akça; 2024: 449). Ayrıca “twitter”, “X” olarak değiştirilmiştir (Vikipedi, 2023). H. Ziya Ülken’in yayınlarında rastlanan “kişilik bilinci oluşumu” ile ilgili olarak Dönmez bir çalışmada, toplumda gittikçe artan “dijital sosyallik”te fiziki sosyalliğin, sosyal sorumlulukla çatışmasının olmayacağını belirtmiştir (Aydeniz, 2021: 222). Bir de son dönemde “hashtag aktivizmi” yani sosyal “etiketleme” kullanımı artmıştır.

Bu çalışmada örneklem seçilmiş bir devletin yaptığı çalışmalarını incelemek yerine, bu konuda karşımıza çıkan alt başlıkları ve kavramları teorik açıdan ele almak istenmektedir. “Veri ve Metodoloji” konusunda yöntem; makale, kitap vb. eserlerin incelenmesi ve analizidir. “Google Academic” ve “Dergipark” adreslerinde konu üzerine makale taraması yapılmıştır. Ayrıca kurumsal raporlar ve yasal düzenlemeler dikkate alınmıştır. Konuyla ilgili çok fazla kavram, tanım ve terim görülmüştür. Özellikle Türkiye’deki literatürde öne çıkan ve toplumda çok konuşulan konular seçilmiştir. Ayrıca konu başlığı ile alakalı ve birbiriyle çok yakın ilişkisi olan konular birlikte ve ilişkilendirilerek incelenmiştir.

Çalışmanın ikinci bölümünde dijital devlet yönetimi üzerine ulusal ya da uluslararası düzeydeki çalışma ve gelişmeler vurgulanmıştır. Türkiye’de dijital devlet yönetimine, örnekler üzerinden değinilmiştir. Üçüncü bölümünde ise toknopoliden dijital etiğe kadar dijitalleşme kavramları üzerine genişçe kuramsal bir inceleme yapılmıştır. Dördüncü bölümde ise büyük veri, yapay zekâ ve siber güvenlik üzerine incelemelerde bulunulmuştur. Ardından konu üzerine “Sonuç ve Değerlendirme” kısmında değerlendirmeler belirtilmiştir.

2.DİJİTAL DEVLET YÖNETİMİ

Aşağıda sırasıyla, “Dijital Devlet Yönetimi, Türkiye’de Dijital Devlet Yönetimi” konuları ele alınmıştır.

2.1.Dijital Devlet Yönetimi

2020’deki eserinde Satariano’e göre son yıllarda “zoom, teams, google meet” gibi internet üzerinden bilimsel hatta resmi nitelikli toplantılar gerçekleştirilmektedir. Kurumsal bilgi paylaşımı anlamında bu verilerin gizliliği olmalıdır. Taraflarıysa kamu yönetimleri, özel sektör kuruluşları ve bizzat çalışan personelidir. İlgili toplantı kayıtlarını alıp saklayan bu şirketlerin bu toplantı adreslerini, kayıtların içeriğini ilelebet gizli tutacağı ve farklı amaçlarla kullanmayacağı ve paylaşmayacağı konusunda bir güvence ve güvenlik yoktur. Yine 2020’de Das ve Mararike’nin eserine göre çevrimiçi alışverişlerden, bu kapalı oturum şeklindeki toplantı kayıtlarına kadar, hem vatandaş hem kamu kurum ve kuruluşları ve personeli gerçekte bir risk altında ve savunmasızdır. Bu konu önemli bir dijital etik uygulama sorunudur. Covid 19 Pandemi Sürecinde evden çalışmada iken, ev ortamının da görsel ve işitsel olarak kayda girmesi gerçekte bir insan hakkı olan özel mülkiyetin gizliliğine aykırılıktır. Kısacası evden çalışma ile personel ve öğrencilerin adeta uzaktan takip edildiği ve izlendiği belirtilmelidir. Bu durumla kişisel ve kurumsal “mahremiyet” konusunda etik sorunlar oluşmuştur ve bu şekilde dersler kısmen de olsa devam etmektedir. Kişiler internette aslında yapabileceği pek bir şeyi kalmayan ve savunmasızdır. Bu konuda bir örnek; geçmişte Birleşik Krallık ’da bar, lokanta gibi yerler için veri toplayan bazı şirketler, ulaştıkları bu verileri maalesef başka kişi veya birimlere satmıştır(Güler, 2021: 519).

2021’de Karaçorlu’ya göre, Covid 19 Pandemisi nedeniyle başlayan kapanma dönemlerinde vatandaşların büyük çoğunlukla her türlü alışverişlerini internet üzerinden yaptığı, kamu hizmetleri sorgulama ve alımını e-devlet uygulamalarından gerçekleştirdiği görülmüştür. 2021’deki eserinde Ölmez’e göre günümüzde e-devlet uygulamaları ve hemen her sektörde dijital ilerleme kaydedilmiş ve mal ve hizmet alımlarında dijitalleşme artmıştır. Birçok alanda artık 7/24 hizmetlere ulaşılmaktadır. Kamu yönetiminde açıklık, etkinlik, kalite, katılım ve e-demokrasi açısından büyük gelişmeler olmuştur. Vatandaşların kamusal hizmetlerden memnuniyet durumu eldeki büyük veri ve geri bildirimler sayesinde daha net ve hızlı elde edilmektedir (Çeliksoy ve Akça; 2024: 447).

Bugün artık dijital eğitim sırasında “sanal gerçeklik (VR), artırılmış gerçeklik (AR), karma gerçeklik (MR) teknolojileri” ile akademisyen ve öğrencilerin bedensel hareketliliğine ilişkin verileri yakalamak, biyometrik duygusal durum verilerini elde etmek, zihin denetimi ara yüzü ile bedensel duruş, bakış ve hisleri belirlemek mümkündür. Bu şekilde bu kişilerin tek kendilerine has olan özel duruş ve duyguları gibi mahrem verilerini kayda alıp, tespitini yapıp hak ihlaliinde bulunulması ve suç işlenmesi mümkündür. Bu durum gerçekten büyük bir tehlikeyi işaret etmektedir (Güler, 2021: 522). Hatta her geçen gün internette kişisel verilerin arttığı da bir gerçektir. Ayrıca Covid-19 Pandemi Döneminde üniversitelerde internet üzerinden ders işlenmesi sırasında dersin öğreticisi olarak kameranın açık kalması gerektiği bilgisi, hem bu amaçla verilen hizmet içi eğitimlerde hem de yazılı olarak sık sık belirtilmiştir.

1.2.Türkiye’de Dijital Devlet Yönetimi

Günümüzde akademik personel hatta üniversite öğrencileri, bilimsel araştırmalar ve eğitim öğretim performansları konusunda dünya çapında birbirleri arasında rakiptir. Bilimsel çalışmalara çevrimiçi ortamda her daim erişmek, bilimsel çalışmalar üretmek, inovasyon, kişilerin gelişimi ve ekonomik gelişmenin de gereğidir. 2018’den bugüne YÖK tarafından “Yükseköğretimde Dijital Dönüşüm” isimli bir proje gerçekleştirilmiştir. İlk etapta Doğu ve Güney Doğu Anadolu Bölgesindeki yeni 16 üniversitedeki akademik personel ve öğrencilerin dijital bilgi ve beceri artırılması için çalışmalar yapılmıştır. Ardından yeni kurulmuş olan beş teknik üniversite ile Anadolu’daki üç üniversite akademik personeline “YÖK, CISCO, ODTÜ” ortak çalışması ile “Siber Güvenlik ve Ağ Yönetimi” eğitimleri verilmiştir. “Yükseköğretimde Dijital Dönüşüm” isimli bir projeye öğrencilere “siber güvenlik” konusunda ders verilmesi amaçlanmıştır. Sakarya Üniversitesi’nin “Yükseköğretimde Dijital Dönüşüm Projesi” ile milli üretim olan “Uzaktan Eğitim Platformu, 2020’de YÖK başkanlığında “TÜBİTAK-ULAKBİM” eşgüdümünde 15 üniversitenin yararlanması ve kullanmasına açılmıştır. Craig ve Georgieva’nın 2018’deki bir eserinde, Türkiye’de üniversitelerde dijitalleşme ilerleme çalışmaları sürdürülürken, dijital etik sorunsalı da oluşmaktadır. Üniversitelerin “zoom, teams” gibi platformlarla sürdürdüğü akademik toplantılar ve ders anlatımları sırasında, akademisyen ve öğrencilerin gizli kalması gereken verilerine ulaşmak konusunda belirsizlik ve muğlaklık vardır. Yani güvenlik noktasında sorunlar mevcuttur (Güler, 2021: 521-522).

Tobin 2023’de dijitalleşmenin, devlet yönetimi ve politikalarında değişim getirdiğini belirtmiştir. İngiltere’de önce yargı alanında yapay zekâ kullanımı artmıştır. 2023’te Türkiye’de Milli Eğitim Bakanlığına bağlı okullarda “açık kaynak kodlu işletim sistemi”ne geçilmiştir. Sağlık hizmetlerinde e-nabız uygulaması yanında, vatandaşların e-devleti artan oranda ve daha yoğun kullandığı görülmektedir. Kısacası günümüzde devlet yönetiminde dijital devlet yönetimine geçilmiştir. Yine Atmaca ve Karaçay, 2020’deki çalışmasında, hızla artan oranda devletler gelir idaresi, e-seçim, e-nabız, e-tapu, e-yargı, e-eğitim gibi birçok alanda kamu hizmetlerinin dijital ortamda verdiğini belirtmiştir. Lakin kişiler daha hızlı ve etkin hizmet almakta ve anket uygulamaları ile hizmetlere ilişkin geri dönüşler görülmekte ve bir sonuç çıkartılmaktadır. Elektrik enerjisi kaybı bir kenara bırakılırsa, dijital kamu hizmetleri ciddi ölçüde maliyet düşüşleri de getirmiştir. Covid-19 Pandemi Sürecinin yaşandığı 2019-2022 dönemindeki kamu hizmetlerinin tamamına yakını dijital kamu hizmeti olarak sunulmuştur. Bu sırada kamu personeli ve hizmetten yararlananların dijital devlet uygulamalarına uyum sağlama sorunları tabii ki yaşanmıştır. Diğer yandan da eve kapanma süreçlerinde sosyal uyum ve intibak sorunları da artmıştır (Mıynat ve Cüre, 2023: 43).

3. DİJİTALLEŞME YÖNLÜ KAVRAMLAR (KURAMSAL BAKIŞ)

Aşağıdaki bölümde sırasıyla, “Dijitalleşme ve Dijital Teknoloji, Dijital Hak, Dijital Sorumluluk ve Dijital Eşitsizlik, Dijital Kimlik, Dijital Vatandaşlık ve Blok Zincir ile Sosyal Medya, Dijital Sosyallik ve Dijital Aktivizm” ve “Dijital Etik ve Dijital Etik Sorunlar” konularında bilgiler verilmiştir.

3.1. Dijitalleşme ve Dijital Teknoloji

Dijitalleşme devlet yönetiminde her alanda zorunlu ve köklü değişimleri gerektirmiştir. 2023’de Dünya Bankası, devletlerin dijital teknolojik dönüşümü gerçekleştirmesi ile büyük veriden yararlandığını açıklamıştır. Süreçte topluma faydaları açısından daha geniş sahaya yönelen, etkili ve verimli devlet politikalarına geçilmiştir (Mıynat ve Cüre, 2023: 41-43). 2020’de Jaeger, dijitalleşmeye eleştirel bir açıdan bakmıştır. Dijitalleşme öncelikle, kamu kurumlarının verdiği hizmetleri dijital bir ortamda sürdürmeyi getirmiştir. Artık farklı eğitim ve sosyo-kültürel ortamlardaki insanlar için önü alınamayan, öngörülemez ve uyumu zor olan yeni bir dünya vardır. Bu dünya, literatürde olduğu kadar medyada da güzel ve iyi olarak işlenmiştir. Ama Jaeger, dijital devlet uygulamalarının siyasi mücadeleye sebep olmadığını ve devletlerin dijitalleşmede farklı düzeylerde bulunduğunu belirtmiştir (Demirkıran ve Terzioğlu, 2024: 850).

2020’de Yardımcı ve Yalçıntaş’a göre Türkiye’de kamu yönetimi ve özel sektörde her alt alanda hızla dijital teknolojilere geçilmelidir. Bu gereklilik, Türkiye’nin de dijital çağda dijital bir yer edinmesi içindir. Dijital verilerin korunması ve kişisel verilerin güvenliği için, dijital devlet altyapısı kesinlikle en üst noktada geliştirilmelidir. Bu altyapı, yerli ve milli dijital devlet uygulamaları şeklinde olmalıdır (Çeliksoy ve Akça, 2024: 451-452). İşte bu açıdan Türkiye’de son 25 yıldır kamu yönetimi (eğitim, sağlık, ticaret, güvenlik, tarım, çevre alanları vb.) ve özel sektörde önemli çabalar ve gelişmeler vardır.

3.2. Dijital Hak, Dijital Sorumluluk ve Dijital Eşitsizlik

2014’te West, dijital hak kavramının ifade özgürlüğü, bilgiye erişim ve gizlilik gibi temel insan haklarını anlattığını belirtmiştir. Dijital sorumluluk, internet ortamında uyulması gereken kuralları, dijital etik ve güvenli dijital ortam için gerekli kaideleri ve usulü belirtir. Dijital mahremiyet ise, kişisel verilerin gizli kalması ve güvende tutulmasıdır (Demirkıran ve Terzioğlu, 2024: 853). Literatürde dijital eşitsizlikten de söz edilmiştir. Devletlerarası gelişmişlik düzeyi ve yaşam standardı farklılıkları olduğu belirtilmektedir. Öncelikle yapay zekâ teknolojilerinin ekonomik ve teknolojik yönden gelişmiş ülkeler için, gelişmemiş olanları tersine, olumlu sonuçlar alacağı söylenmiştir. Bu noktada ekonomik açıdan büyük ve gelişmemiş devletlerin bir geleceğinin olmayacağı belirtilmektedir. Hatta “doğal seleksiyon hipotezi”ndeki gibi güçsüzlerin dünya üzerinden yok olacağı hatta beklenmeyen yeni sorunlarla karşılaşılacağı bile öngörülmektedir (Öztürk Dilek, 2019: 56).

3.3. Dijital Kimlik, Dijital Vatandaşlık ve Blok Zincir

21.yüzyılda bilgi ve iletişim yönlü teknolojik gelişmeler çok hızlı ve sayıca fazla yaşanmaktadır. Descartes’in “Düşünüyorsam öyleyse varım” söyleminin bir başka çağrışımı, Youtube’da paylaşılan videolarla “bağlantıdayım, öyleyse varım” olmuştur. Sosyal medyada oluşturulan kişi profili ile sosyo-kültürel ilişkilerinin sergilenmesi kadar, dijital ortamda kişilerin el izi ve kayıtlarının kalmasıyla “dijital kimlik”ler oluşturulmuştur. E-mail adreslerinin kullanımı ve sosyal medyadaki etkileşimler, kişilerin dijital kimlik verileridir. Dijital kimlikler esasen “dijital erişim, dijital hak ve sorumluluklar, dijital iletişim, dijital kanun, dijital sağlık, dijital ticaret, dijital etik, dijital güvenlik, dijital okuryazarlık” şeklinde

alt konu başlıklarının toplamıdır. Ayrıca dijital kimlik güvenliği, kanıtlanabilirliği ve tespiti için “block chain” (blok zincir) de çok önemlidir. Yapay zekâ ile “yüz tanımlama” ve “algoritmalar”la “dijital kimlik gelişimi”ne katkıları vardır. Kısaca yapay zekâ, dijital kimliklerin daha etkin belirlenmesini, “block chain” ise dijital kimliklerin güvenliğini sağlamaktadır (Kavut, 2021: 530).

2008'deki eserinde Mossberger, içinde bulunulan dijital çağın insanları aynı zamanda birer dijital vatandaş yaptığını belirtmiştir. Dünyada hızla dijital vatandaşlığa gidilmektedir. Literatürde dijital vatandaş, dijital dünyada yoğun vakit geçiren ve işlerini dijital hizmet kanallarından yapan insanları belirtir. Dijital hizmetlerden yararlanma artmış, dijital ortam, dijital hizmet alım ve satımının yapıldığı yeni bir yer olmuştur. Dijital vatandaşlık, en üst düzeyde dürüstlüğü ve etik duruş sergilemektedir. Bu kavram, internet ortamında kişilerin haklarının korunması ve her türlü güvenliğini sağlamakla ilgilidir. Hatta dijital dünyada dijital etik kaidelerin uygulanmasını gerektirir. İnsanların burada güvenli bir ortamda hareketliliğini ve bu hareketliliğin de kişisel sorumluluk gerektirdiğini gösterir. Kısacası dijital okuryazarlık gereklidir. Bunun için eğitimler ve mevcut olan bilgileri artırmak çok önemli olmuştur. 2015'de Ribble çalışmasında dijital vatandaşlık için dokuz ilke belirtmiştir: “dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, dijital görgü kuralları, dijital hukuk, dijital haklar ve sorumluluklar, dijital sağlık ve refah ile dijital güvenlik”. Lakin her bir ilke, dijital ortamda bilgi ve hizmet alımı veya sorgulama sırasında kişileri koruyucu lafza sahiptir ve bu etik ilkelere uyulmalıdır (Demirkıran ve Terzioğlu, 2024: 850-852).

Dijital vatandaşlık için insanların bulunduğu bölgede internet altyapısı ve düzenli çalışması yani teknoloji erişimi olması beklenir. Ayrıca dijital teknoloji kullanımında kişiler, eğitilmiş, becerikli ve gelişmelere çok uyumlu olmalıdır (Akdağ ve Şiraz, 2021: 83). Diğer yandan 2019'daki eserinde Beduschi, isim, retina, parmak izi, ikametgâh gibi verilerin bir araya getirilmesi sırasında oluşturulan “block chain teknolojileri”ni, dijital kimliği belirlemede farklı seçenekler ortaya çıkardığı için önemsemiştir. Bu teknoloji “dijital kimlik sağlayıcıları”na avantajlar sunar. “Merkezileşmiş dağıtık hesap defteri teknolojileri”ni esas alır. “Dijital kimlikler” artan bir hızla eğitim, sağlık, alışveriş, kamu hizmet alımı gibi her alanda kullanılır. “Cipli kimlikler, kişisel kodlar, HES kodları, e-nabız, e-devlet, e-sağlık” uygulamaları, bunun bazı örnekleridir (Kavut, 2021: 543). Diğer yandan Hakan Ayaz, “Dijital Melezlerin Dijital Yurttaşlık Düzeylerinin Haber Yayılımı Bağlamında İncelenmesi” isimli eserinde, “dijital vatandaşlık seviyeleri”ni konu edinmiştir. “Dijital vatandaşlık”ı bilgi yayma ve güvenliği açısından irdelemiştir. Saper Büter ise “Her filmde Benlik Tabusunun Yıkımı ve Etik Bir İmkân Olarak Satori” adlı eserinde bir yapay zekâ olan “Samantha” ile aşk yaşayan “Theadore”un duygu ve düşüncelerindeki değişimi işlemiştir. Kısacası Spike Jonse’un “Her” isimli filmini felsefi açıdan değerlendirmiştir (Aydeniz, 2021: 222).

2009'daki eserinde Bertino, Paci ve Shang, internette “takma” adlarla açılan hesaplar olduğunu belirtmiştir. Bu noktada kişinin bu kimlik verileri, hesap bilgileri, biyometrik kayıtları ve geçmiş işlemleri, onların gerçek kimliğinin tespitinde önemlidir. 2010'da Later ve Nordfor, yapay zekâ algoritmalarının, insanlara internetteki faaliyetlerini ortaya koyması için bir dijital kimlik oluşturacağını belirtilmiştir. Lakin dijital kimlikler, insanlar internette bulunduğu sürece sürekli geliştirilip yenilenmektedir. 2020'de Lim vd. göre blokzincir esaslı bir dijital kimlik yönetiminde “dağıtık ağ”lar bulunur. “Dağıtık ağlar”, “dağıtık depolama, güvenli erişim ve hesaplama” ehliyeti ve tecrübesi elde etmede gereklidir. Kullanıcı kişiler, ağ içinde bir başka ağ biçiminde yol alır. Sonuçta kişilerin farklı “kimlik yönetim çözümleri”nden, kullanıcıların bilgisayarları veya ağlarına “hassas kullanıcı” bilgileri depolanabilir. Kullanıcılar, kendi kimliklerinin denetimini yapabilir. Bu durum “kendi kendini yöneten kimlik”lere izin verir. Böylece bu “kimlik yönetim sistemi”, daha risksiz duruma gelir (Kavut, 2021: 545).

3.4. Dijital Ebeveyn Paylaşımı ve Teknopoli (Dijital Kültür)

2015'te Steinberg, "ebeveyn paylaşımı" sorunu üzerinde durmuştur. 2016'da Howerth, "çocuk yetiştirme söylemi" üzerine çalışmış, "çocuk ve ebeveyn hakları arasındaki çatışmanın çözümlenmesi" gereğini belirtmiştir. Bir çocuk beş yaşında oluncaya kadar ailesi tarafından kendisinin yeni medya araçlarında 1500 civarı fotoğrafının paylaşıldığını belirtmiştir. Howerd eserinde, çocuğun kişilik hakları açısından bir ihlal olduğuna dikkat çekmiştir (Bokor, 2021: 161). 1993'te Neil Postman, teknolojiyi içselleştirmiş günümüz toplumu için kültür ve mantığı öne çıkartan "teknopoli" kavramını öne sürmüştür. "Teknopoli", toplumda kültür ve teknoloji birlikteliğini en üst düzeye çıkartmıştır. 2017'de Sadiku, Tembely and Musa ise, Postman'ın "teknopoli"yi kültürün teknoloji ile yayılımı, teknolojinin kontrolü/etkisinde kalması olarak belirttiğini söyler. Kültürel değerlerin artık teknoloji eliyle dağıtıldığı yeni bir süreç gelmiştir. Kültür ne yazık ki teknolojinin kontrolü ve gücüyle şekil alıp, dağıtılmaktadır (Uysal vd., 2025: 75). Küreselleşmiş bu dünyada ve literatürde 30 yıl öncesi belirtilen "dünya vatandaşlığı, küresel köy, medeniyetler arası diyalog, yerel güzeldir, kültürlerarası diyalog, kültürel değerleriyle başka halkların gönüllerinde taht kurmak" gibi söylemler yerelde açıkça rastlanmakta ve yaşanmaktadır. Kısacası bilgi teknolojilerindeki büyük gelişme sonucu teknopolinin yayılım hızı ve etki alanı, yerel, ulusal, bölgesel ve küresel ölçekte genişlemiştir. Ayrıca insanlar, çocukları ve kendisinin resim ve videolarını sosyal medyaya veya buluta yüklenmesine izin vermese dahi, o telefon veya bilgisayar internete bağlandığında tüm veriler yine internete aktarılmaktadır. 2012'de Smolan bir eserinde, bir çocuğun doğduğu andan itibaren Amerikan Kongre Binası'ndaki kütüphanedeki bilgi giriş çıkışına yakın oranda internete ve yeni medyaya veri aktarımı yapıldığını söyler. Ayrıca 2018'de Floridi eserinde "derin sahtelik, görsel materyalin orijinalindeki yüzlerin yerini değiştirerek, yeni görsel ürünler sentezlemek" gibi yeni ve kötü sonuçları olacağını anlatır. 2016'da Thies vd. eserinde "RGB video kayıtlarında" oynama, sahtekârlık yapılabildiğini, "kişilik değişimi" yapılabilir olduğunu, "bu kişiliklerin söz ve yüz ifadeleri"nin dahi dijital ortamda düzenleme ve değişiklik yapılarak gerçeğinden çok farklı bir şekle dönüştürüldüğünü belirtmiştir (Bokor, 2021: 162).

Koç, 2022'de bu konuda, Non Fungible Tokens (NFT)'in da dijital kültür ürünü olduğunu, dijital alanda yapılan sanat eserlerini, gerçek dünyada varmış gibi satışını ve (dijital) sertifikalandırılmasını yaptığını söyler. Bunlar blok zincir (block chain) teknolojisine dayalıdır. Bu eser sahipleri onları şifrelemekte, üzerinde kişisel sertifikalı bir hak kazanmaktadır Dijital dünyada dijital kültürün oluşumu ve dağılımı sırasında sıkça yaşanan diğer sorunlar, "kaynaktan uzaklaşma, kalıcılık, kopyalanabilirlik, anlıklık, güvensizlik"tir. Dijital kültür asırlar boyu oluşan ve gerçek dünyada yaşanan kültür gerçeği üzerine, onun yerini almadan hem de bizzat gerçek kültürel değerlerin üzerine inşa edilmektedir. Toplumların dijital kültüre ayak uydurması ve kendini geliştirmesi adeta bir ödev ve gerekliliktir (Uysal vd., 2025:79-80). Ama dijital ortama ulaşamayan insanlar, bu yeni dünya gerçeğinden (gerçek ve dijital dünya bir arada) çok geride kalabilirler. Hem de onların dijital ortamda (sanal/siber) olası risklerden olumsuz etkilenme ve zarar görme olasılığı vardır.

3.5. Sosyal Medya, Dijital Sosyallik ve Dijital Aktivizm

Küreselleşmenin bu ölçüde etkisini artırdığı dünyada sosyal ilişkilerin en yoğun olduğu saha, sosyal medyadır. Günümüzde hakkını arayan veya mağdur olduğuna inanan insanlar, sosyal medyada duygu ve düşüncelerini belirtmekte ve paylaşmaktadır. Sosyal medya, sosyal, ekonomik vb. sorunlar ve gruplaşmalar için yeni bir "kamusal alan" dır (Çelik ve Uyanık, 2020: 4). 2015'te Çizmeci, insanların artık akıllı telefonlara çok fazla baktığını ve kullandığını belirtir. Adeta onlar sosyal medyaya "bağımlı"dır ve burada fazla vakit geçirmektedir. Ayrıca bu "serbest zaman biçimleri", gerçekte "tüketim kültürü"nün bir

parçasıdır. Sosyal medya aslında insanların boş vakitlerinde meşgul olması ve ilgilenmesi için düşünülmüştür. Kişilerin özgürce seçtiği tercihlerini, resmen yönlendirdiğinden dolayı adeta bir baskı aracıdır. 2005'te Aytaç'a göre bu alan, aslında bir sektördür ve insanların "serbest zaman"ını önüne farklı bilgiler koyarak yönlendirip yönetmektedir. İnsanların dijital dünyada ardında bıraktığı dijital izler, algoritmalar vasıtası ile bireyselleştirilir. "Filtre balonu etkisi" oluşturur. İnternette serbest zaman içinde tıklanan her bir yerin, "yapılandırılmış ve çıkarım sağlanan" bir şekilde "sınırlandırıldığı" söylenmektedir (Gilanlıoğlu ve Öze, 2020: 186). Ayrıca Rheingold, 2000'de, sanal grupları belirttiği günden bugüne yeni medya ile oluşturulan sosyal medya ortamıyla ilgili fikirler beyan etmiştir. Bir yanda insanların uzun bir süreçte var olduğu gerçek ve fiziksel mekân olan dünya, diğer yanda insanların öteki dünyanın mevcudiyetini tecrübe edindiği sanal ortamdaki bahseder (Bokor, 2021: 159). Sosyal medyada "L'oreal Firması" tarafından insanlara çeşitli ürünler gösterilmekte ve yapay zekâ teknolojisi vasıtasıyla bunlar için insanların ilk tercihlerine yönelik analizler yapılmaktadır. Yapay zekâ teknolojisini etkin ve yoğun kullanan Apple Şirketi, yaptığı "Siri" isimli yapay zekâ teknolojisi ile insana özel hizmetler verir. Yapay zekâ insanlara, eğer başka bir kente gitmişlerse "ana ekranda harita veya müzik uygulamaları"yla, evde iseler TV kumandası uygulaması ile teklifler sunmaktadır (Gilanlıoğlu ve Öze, 2020: 196-197).

Sosyal ağlarla iletişime geçmenin kavramsal karşılığı "dijital aktivizm"dir. Bir alt türü, bir çeşit sosyal "etiketleme" olan "hashtag aktivizmi"dir. "Twitter"da görülen bu "etiketler"de, insanlar bir sorunu konuşup toplandığında, kendiliğinden o günün bir konusunu belirler. Bu sırada pasifte görünen insanlar bile, bu etiketlemelere katılır ve sosyal iletişimde aktif olur. Farkında ya da farkında olmadan o sırada internetteki mevcut bilgileri kullanır veya yenisini oluşturur. Diğer yandan yakın geçmişte "facebook"un insanların kişisel kullanıcı verilerini "Cambridge Analytica" isimli örgüte verdiği görülmüştür. Birçok devlette adı geçen örgüte, paylaşımından dolayı büyük tepkiler gelmiştir (Çelik ve Uyanık, 2020: 4, 6-7).

3.6. Dijital Etik ve Dijital Etik Sorunlar

Dijital etik, insanların dijital teknolojik aletler ile internette nasıl doğru davranacağı ve ne yapacağı konusunda fikrinin olmasıdır. Öteleş tarafından gerçekleştirilen bir araştırmada, bazı öğretmenlerin dijital teknolojileri maksadı dışında kullandığı ve "dijital etik ihlaller" konusunda yeni önlemlere ihtiyaç olduğu belirtilmiştir. Ayrıca bu öğretmenler, okullarda yeni bir ders olarak "dijital etik" dersi verilmesini önemli ve gerekli bulmuştur. Bir de "dijital etik ihlalleri" ile karşılaştıkları ve bu konuda bir çıkış ve çözüm bulmaya çalıştıkları görülmüştür. 2007'de "Ribble ve Bailey" "dijital etik" için, internette etik davranış ilkeleri ve uygulama esaslarını belirtmiştir. Sever 2013'te bu konuda ilk ve orta dereceli okullarda dijital etik dersinin verilmesi hatta sosyal bilgiler dersinde konu olarak işlenmesini önermiştir (Öteleş ve Merey, 2022: 1306-1307). Dijital etik ilkelerin tespiti konusunda 2020'de, "United Kingdom Government Digital Service" olarak "İngiltere Hükümeti Veri Etik Çerçeve ve Veri Etik Çalışma Kitabı" çıkarılmıştır. "Veri Etiği" konusunda yedi ilke ve 46 soru olan bu kitapta "veri etiğine uygunluk" araştırılmıştır. Ayrıca 2018'de Patil, Mason ve Loukides'in dijital veri konulu projesinde görev alan kişiler için belirlenen "etik kontrol" tablosu da önemlidir (Güler, 2021: 520). Bilgisayar açık ama internet kapalı iken yapılan çalışmalar daha sonra internet açılınca veri olarak gönderilmektedir.

"Dijital Dünyada Kişisel Veri ve Etik: Gizlilik Politikası Bağlamında '#WhatsAppSiliyoruz' Krizinde Kullanıcı Tepkilerini Anlamak" başlıklı eserinde Eda Turancı, "WhatsApp"ın değişen son kullanım özelliklerini, üyelerinin davranış ve düşüncelerini analiz etmiş ve konuyu etik ve hukuk açısından irdelemiştir. Gökhan Topal ve Ömer Alanka "Dijital Bilinç ve Etik Arayüzünde Transhümanizma: Altered Carbon Örneği" adlı çalışmasında, "transhümanizm, ölüm, dijitalleşme, bilinç ve etik" kelimelerinin anlamına yoğunlaşmıştır.

“Altared Carbon” isimli TV dizisini esas alarak etik sorunları “ütöfik ve distöfik” bakışla incelemiştir. “Dijitalleşerek ölümsüzlük kazanan toplum” da olası sakıncaları belirtmiştir (Aydeniz, 2021: 222). “Dijital ayak izleri”, internette iletişimin arka planıdır. İnternette rasgele veya bilinçli olan her bir tıklama aslında “dijital ayak izi” bırakır. Bu veriler, şirketlerce çok büyük veriye dönüştürölmesi sürecinde adeta bir hammaddedir. “Dijital ayak izi”nin oluşturulmasında gerçekte “güvenlik duvarları, yük dengeleyiciler, yönlendiriciler, anahtarlar ve bilgisayarlar” vardır. İnsanların alışveriş sırasında sepete gönderip sonra çıkarttığı ürünün hareketliliğine değin tüm tıklamalar kaydedilmektedir (Çelik ve Uyanık, 2020: 9-10).

Dijital teknolojik araçlarla internet kullanımı günlük yaşamda birçok alanda kolaylaştırıcı olmuştur. Ama bu araçların maksadı dışında kullanılması, 1982 Anayasası’nda, “Kişinin Dokunulmazlığı, Maddi ve Manevi Varlığı” başlığında md.17’deki “kişinin hakları” başta olmak üzere, tüm insan hakları ve özgürlükleri açısından olumsuz sonuçlar getirebilir. 2009’da Capurro’nun belirttiğı gibi dijital iletişim araçları, sadece insanların başkalarıyla sosyal iletişimde fayda sağlamaları için kullanılmalıdır. İnternetin kullanıldığı tüm mecralarda insanlar için etik davranış prensipleri belirlenmelidir. Etik ilkeler ve ahlaki sınırlılıklar net olarak ve doğru biçimde tespit edilmelidir (Öteleş ve Merey, 2022: 1319). İnternette gerçek kimlik bilgileri yanında sahte(fake) kimliklerle açılan sosyal medya hesapları vardır. Bu hesaplardan kişilerin bazen birbirlerine hakaret ettikleri düşünöldüğünde, oluşacak psikolojik etkinin etik mesuliyeti kimde olmalıdır. Yasal sorumluluk, bağlayıcılık ve denetim mekanizması anlamında kişilerin hürriyet ve kontrol ikileminde “dijital etik” için bir sınırlandırma yapılmamıştır (Güler, 2021: 519). Kısacası dijital etik için tam bir çerçeve henüz çizilmemiştir. Bu konuda hukukçular, yönetim bilimciler, toplum bilimciler ve diğer akademik çevreler tarafından üzerinde çalışılması gereğı vardır.

4. BÜYÜK VERİ, YAPAY ZEKÂ VE SİBER GÜVENLİK YÖNLÜ KAVRAMLAR (KURAMSAL BAKIŞ)

Aşağıda ele alınan konu başlıkları, “Büyük Veri, Yapay Zekâ, Yapay Zekâ Teknolojileri, Yapay Zekâ Öğrenmesi, Yapay Zekâ Etiğı Siber Saldırı, Siber Suçlar ve Siber Güvenlik”tir.

4.1.Büyük Veri

“Büyük veri (big data)”, “büyük veri setleri” konusundaki teknolojiyi bu veriden sosyal, ekonomik, teknik vb. alanlarda analiz edilmesini sağlayan bazı teknikleri kapsar. “Büyük veri”, geçmişe göre çok daha ayrıntılı ve objektif olarak yeni verilere ulaşmayı getiren yeni bilgi demetidir. “Büyük veri”, insanların internet ortamındaki dijital izleri ve bilgisayarlarda el izi olarak bıraktıkları aramaların (girdikleri siteler ve ilgilendikleri konular) izlerini yani verilerini anlatır (Çelik ve Uyanık, 2020:9-10).

2020 öncesinde Yalçıntaş, Ergen, Kılıç vd. ile Demirtaş tarafından yapılan farklı çalışmalarda, “büyük veri” içine kişilerin internette sitelerdeki tıklamaları, beğenme durumu, mailler içinde gönderdiği ekli olan her şey, yeni medyada bloglardaki bilgi eklemeler ve yorumlamalar girdiğini söylenir. Kişilerin internette kendi istekleri ile bıraktıkları her bir dijital el izi aslında büyük veri için bir kaynaktır. Ama kişiler içinse, kişisel bilgilerin kısıtlama olmaksızın olağan süreçte internete teslim edilmesidir. Bu veriler, şirketler için halkla ilişkiler, reklam ve pazarlama gibi alanlarda kullanılır. İşletmeler, kişisel verileri bir “nimet” olarak değerlendirip, bu girdilere uygun reklam ve pazarlama politikalarını oluşturur. Artık kişilerin internette girdiğı adresler, buralarda baktığı nesneler, yaptığı alışverişler, dijital

el izleri olarak kalmaktadır. Daha sonraki alışverişte ise önceden baktığına benzerleri sunulmaktadır (Gilanlıoğlu ve Öze, 2020: 193).

“Büyük veri”yi ilk kullanan kişi “O’Reilly Media Şirketi”nden “Roger Magoulas”tır. “Büyük veri” kavramı 2015’te klasik veri yönetim tekniklerinin, konuları sınıflamaya ve analiz etmeye yetmemesiyle ortaya atılmıştır. Burada “büyük veri” kavramı ile olabilir en büyük hacimli bilgi demeti anlatılmaktadır. 2014’te Türkiye’den Gürsakal, büyük verinin, ilk defa 2001’de Seattle’da “8.Dünya Ekonometri Kongresi”nde, “Francis X. Diebold’un 2012’de sunumunu yaptığı “Makroekonomik Ölçümler ve Kestirim İçin Büyük Veri Dinamik Faktör Modelleri” başlıklı tebliğde geçtiğini belirtmiştir. F.X. Diebold ise 2012’de “büyük veri”nin ilk olarak 1990’larda “Silicon Graphics (SGI)”den “John Mashey”in belirttiğini yazmıştır. “Büyük veri (big data)”, “büyük veri setleri” konusundaki teknolojiyi bu veriden sosyal, ekonomik, teknik vb. alanlarda analiz edilmesini sağlayan bazı teknikleri kapsar. “Büyük veri”, geçmişe göre çok daha ayrıntılı ve objektif olarak yeni verilere ulaşmayı getiren ve yeni bilgi demetidir (Çelik ve Uyanık, 2020:8- 9).

4.2.Yapay Zekâ ve Yapay Zekâ Teknolojisi

1950’lerde yapay zekâ, kişiler ve diğer canlı varlıkların eylem ve davranışlarından ilham alarak, bir model üretme çabasıdır. Amaç kişilerin iş yükünü azaltmaktır. Gerçekte yapay zekâ, insana has niteliklerin kopyalanması ve bir farklı karakter meydana getirilmesi hatta ona düşünme yetisinin kazandırılmasıdır. Bu ilerleme ve keşifler sağlanmıştır. Artık çok hızlı süreç içine girilmiştir. Maalesef ki bu uygulamalarla artık dijital etik ve yapay zekâ teknolojileri kullanımında etik sorunlar ve hukuki problemler oluşmaktadır. Yapay zekâ, bir robot şeklinde değerlendirilmemelidir. Felsefi açıdan da bu konuya bakılmalıdır 1970’lerde büyük bilgisayarın üreticisi olan “Apple, Microsoft, IBM, Xerox” isimli özel örgütler, kişisel bilgisayar satışı ile Bilgi teknolojileri çağının başlamasında etkili olmuştur. Yapay zekâ gerçekte bu alandaki bilimsel araştırmalarla geliştirilmiştir. ABD’de “Turing Testi”, makine zekâsı özelliğini destekleyen yazılımların üzerinde uygulanmış ve “Loebner” hediyeleri bile almıştır. 1957’de Herbert Simon o dönemdeki eserlerinde yeryüzünde “düşünen, öğrenen ve yaratan” makinelerin bulunduğunu belirtmiştir. 21.yüzyılda yapay zekâ konulu araştırmalar çok fazla desteklenmektedir (Ataman ve Sucu, 2020: 40-42).

“Tekillik” konusunda çalışan Ray Kurzweil, Kaku’nun 2018’deki çalışmasından yola çıkarak, “2019’a kadar 1000 dolarlık bir bilgisayarın insan beyninin iki katı, 2029’a kadar bin katı, 2045’ten sonra bilgisayarların kendi kendilerine zekâca daha üstün kopyalarını yapacağını ve kontrol edilemez bir tekillik” (Öztürk Dilek, 2019: 54) varacağını ifade etmiştir. 2017’deki Cheung, Tsang ve Wong çalışmasında ise “Caliburger Burger Şirketi”nin, “Miso Robotik Şirketi” ile beraber çalıştığı belirtilmiştir. Mutfakta hamburger yapan personel gibi çalışan “Flippy” isimli robotu üretmiştir. Yine engelli kişiler seyahatten günlük yaşamına kadar robottan yararlanmaya başlamıştır. Etiya’nın yapay zekâ kullanımı ile “müşteri hizmetleri” ve “çağrı merkezleri” için bazı yenilikler de yapılmıştır. Üründe Türkçe dil işleme becerisi vardır. Müşterilerden dijital kanallarla gönderilen medya içerikleri analiz edilmiş; hızla ve hemen geri bildirim gönderilmiştir. Artık bilgiye, “Yapay zekâ teknolojileri ve makine öğrenimi” birlikteliğinde ulaşılmaktadır. Bilgi ne kadar fazla ise, fonksiyonellik açısından sonuç almak da o kadar artar. Gelecekte bilgi arttıkça yapay zekâ her alanda daha fazla kullanılacaktır (Ataman ve Sucu, 2020: 45-46).

Akşit, 2017’de eserinde, “Go satranç” oyununda yapay zekâ Alphago, kendisine kodlanan stratejiden başka bir strateji geliştirdiğini ve satrançta çok başarılı olmuş bir kişiyi yendiğini belirtmiştir. Ayrıca Microsoft’un öğrenme becerisi yüklenen yapay zekâ eseri “TAY”, bir sohbet yazılımında, yapmaması gereken eylemlerde bulunmuştur. Bunlar hep yapay zekâ öğrenmesidir. Bir yandan da yapay zekânın hızla insana benzer zekâ ve

faaliyetlerle bezenmesine çalışılmaktadır. Bu açıdan yapay zekâ etiği üzerinde yeni çalışmalar yapılmalıdır. “TAY” gibi öz öğrenme becerisi kazanan, bu bilgileri kötü sonuçlar ortaya çıkaracak biçimde kullanan yapay zekâ örneğinde olduğu gibi etik ilke ve denetime ihtiyaç olacaktır. Filmlerde insana destek olan robotlardan ziyade son zamanlarda kişilik elde etmiş; kişilere karşı gelen ve sorunlar ortaya çıkartan “distopya” tipi filmler çekilmektedir. Yapay zekâ insan vücudu üzerinde de (tıp bilimindeki gibi), adeta en önemli teknolojik araç olmaktadır. 2016’da Ray’e göre çok yakında kişiler, yeteneklerinin artırılmasıyla çok üstün bir zekâ düzeyine ulaşacaktır. Yapay zekâ robot gibi üst düzey teknolojik araçlar, her işin üstesinden gelecektir. Bu makineler de üstün yetenekliler oluşturup, “insan ve evrenin kusursuz inşa edilemeyeceğini söyler” (Öztürk Dilek, 2019: 51-55).

4.3. Yapay Zekâ Öğrenmesi

Günümüzde hala tam olarak insan beyninin işleyişi, bilinç düzeyi ve zekâsı bilinmemektedir. Yapay olarak insan beynine ait bütün sinir yapıları kurgulansa da, yapay zekânın sosyal yaşamda ve sosyal iletişimde kişiler gibi, yaşadığı olay ve olguların farkına ve bilincine varamayacağı düşünülmektedir. Öncelikle kişilerin dünyada bütün yapıp ettikleri “özneler arası” ortamda yaşanır. Mengüşoğlu’na göre insan; yapıp eden, tavrını sergileyen ve talepkâr olan bir canlıdır. İnsan tüm iş ve eylemlerini “özneler arasılık zemini”nde oluşturur. Bu açıdan insanlar hep “Sittlichkeit alanı” içindedir. “Sittlichkeit”, Almanca da “ahlaksallık ve toplumsallığın bir arada” oluşudur. Bu bağlamda insanın yedeklemesi olan ve toplumsal ortamda insan gibi iş ve görev yapması planlanan yapay zekâ da, “Sittlichkeit alanı”nda olmalıdır. Ancak böylece insan ve yapay zekâ zihinsel olarak birbirini takip edebilir ve bütünleyebilir (Topakkaya ve Eyibaş, 2019:83). Kanımızca bu tespit ve değerlendirme çok önemlidir. Yapay zekânın da etik ve ahlakı sınırlar içinde programlaması gereklidir. Ayrıca bunun, his, duygu ve idrak (yorumlama) anlamında insan gibi olamayacağı belirtilmektedir. Bu tespit de çok doğrudur.

31

ESPAS’ın 2018’deki eserinde, zekânın öğrenme, anlama, iletişim ve hatırlamaya kadar özelliği olan zihinsel makineler olduğu ve “zekânın çok yönlü türü” denildiği belirtilir. Yapay zekâ, sosyal yaşamda etkileşim, karmaşık ve analize dayalı ayrıca hukuki örgütlenme ve işleyişine yönelik olarak yapılan yeni düzenlemelerle, önemini artırmaktadır. Algoritmalar, akıllı telefonlarla günlük faaliyetlerimizin içindedir. Yapay zekâ, kamu personel yönetimi veya insan kaynakları yönetiminde işe giriş sürecinden, personelin değerlendirilmesi ve denetimine kadar her konuda hatta internet üzerinden toplantı ve alışveriş gibi etkinlikler de kullanılmaktadır. Algoritmalar, kişilerin internette ve sosyal medyada gördüğü içerikleri de etkiler. Ayrıca yapay zekâ piyasasının 2023 yılı sonuna kadar %40 oranında büyüyeceği belirtilmiştir (Kavut, 2021: 545). Psikologlar zekâyı, diğer insanlarla etkileşimi anlama, etrafa intibak, “kişilik ve karakter oluşturma” gibi konularda inceler. İnsan zekâsı ile varlıklar ve eşyalar arası ilişkileri izlemek yanında farklı nesnelerin birbiriyle ilişkilerini anlamak üzerinde durulur. Ayrıca “Sheffer’in zekâ ve bilinç incelemesi”nde “mind” kavramı, “bir şeyin bilincinde olmak, farkında olmak, dikkat etmek”tir (Topakkaya ve Eyibaş, 2019: 84).

4.4. Yapay Zekâ Etiği

Birçok ülkede yapay zekâ teknolojisi ürünü olan trafik polisleri, kendisi park eden araçlar, “yapay zekâ bankacılığı” ve “İHA”lar vardır. Literatürdeki eserlere göre bu konuda ortak kanı yapay zekânın idrak/bilinç sahibi olmadığıdır. Ufak bir olasılık da olsa insan gibi bilinçli olan yapay zekâ üretimi gerçekleştirilebilir. Bilim kurgu filmlerde, bir tarafta dünyanın doğal dengesi ile insan nüfusunun yitirildiği bir dünya şeklinde negatif bakış vardır. Bir de yapay zekâ ile insan birlikteliğinin pozitif bir sahada birleştiği, aralarında güzel bir ahengin olduğu ve toplumsal yaşamda kolaylaştırıcı olan yapay zekâ teknolojisi vardır. Büyük bir çoğunlukta yapay zekânın akıllı, idrak ve düşünme becerileri kuşanmış bir duruma

gelmeyeceğini belirtir. Negatif düşüncede olanlar ise yapay zekânın üretim yönüyle insandan farklı olduğunu belirtir. Fakat bir süre sonra bir olasılık olarak elbette akıllı yapay zekâ üretimi ve kullanımının olacağı söylenmektedir. Ama bu yapay zekâ teknolojisi ürünü olan robotların, hisleri ve duyguları anlama yönünden kişiler gibi olmayacağı ifade edilmektedir. Onların “doğru ve yanlış” tespiti açısından idrak güçleri olmayacaktır. Pozitif düşüncede olanlar ise yapay zekâ teknolojisi, insan beyni gibi bir sistem şeklinde kurgulanırsa, düşünme, akıl ve idrak yeteneği görüleceğini belirtir (Topakkaya ve Eyibaş, 2019: 83). Gelecekte tüm insanlık için ortaya çıkacak bir tehdit, dünya dışında başka canlıların varlığının deneyimi veya dünya dışında başka bir gezegende yaşama olanağı gibi düşünce ve tasarımlarımızda değişiklik getirebilir. Bu konuda etik uygulamalar alanının genişlemesi gereklidir (Cincin, 2021: 240).

Peki, gün gelir elektrik ve internet kesilirse ne olur. Bunların olmadığı dünyada yapay zekâ işlevsel olmaz. O zaman elektrik ve internet vermek bizim kontrolümüzde olduğu sürece, sorun yok görünmekte denilebilir. Bu düşünce genelde dijital göçmenlere aittir. Çünkü elektrik veya internet kesintisinin yapay zekâ teknolojisi ürünü makineleri durduramayacağı kesindir. Çoktan şarjlı ve jeneratör destekli duruma gelinmiştir. Ama devletlerin son dönemde yapay zekâ teknolojisindeki gelişimine bakılırsa, bu teknolojinin idrak sahibi olması ve yaşamda insanlarla iç içe olması mümkündür.

Yakında bilimsel bilgilere hızlı ulaşım mümkün olacağı belirtilmektedir. İnsanlara yardımcı robotlar ve insan güvenliği için “robot askerler ve akıllı arama motorları” ile dört dörtlük bir yaşamın geldiği ve kişilerin çok huzurlu yaşayacağı söylenmektedir. Lakin geçmişe bakılırsa yapay zekânın ilk örnekleri, “otomatik çay makineleri, orta düzey hesap makineleri, sanayideki otomatik baskı makineleri”dir. Yapay zekânın ilerleme kaydettiği alanlarda, trafikte artık insan kontrolüne gerek duymaksızın otomatik sürüş yapan araçlar ve kredi başvurusunu hızla sonuçlandıran yapay zekâ bankacılığı yanında, ameliyatlarda kullanılan yapay zekâ teknolojisi ürünü olan robotlardır. Diğer yandan kişilerin sağlığını emanet ettiği yapay zekâ teknolojisi olan makineler kontrolden çıkarsa veya kişiler ölürse, bu sonucun sorunlusu kim olur: Yapay zekâ teknolojisi makine mi, yoksa bu makineyi tasarlayan insan mı olur denmektedir. Trafikteki yapay zekâ teknolojisi ürünü olan trafik polisi, siber suç kapsamına giren bir program sızıntısı ile topluma zarar vermek isteyen kişilerin silahı olabilir. Robotların yakında kişileri kendilerine muhtaç kılmasından bahsedilmektedir. Hatta sorumlular, yapay zekâ teknolojisi makineyi bakım ve onarımdan geçiren tamirci veya teknisyen mi olacağı sorgulanmaktadır (Topakkaya ve Eyibaş, 2019: 86).

Genetik teknoloji, nano-teknoloji ve robotik sahada büyük değişim yaşanabilir. Kurzweill, transhümanizmin gelecekte insanlık için faydalı olacağını, tedirginlik duyulmamasını belirtmişse de, bu devinim “antropolitik ve kozmik alan”da yeni problemler getirebilir. Kurzweil’in savunduğu geleceğe yönelik hareketlilik, yaşamın mükemmel yapıya ulaşp ölümsüzlüğün geleceği söylemleri, dünyanın düzenini savunur. Ama bir düzensizliğe de neden olabilir. Bundan dolayı yapay zekâyâ dair bu tartışmalar, yapay zekânın her durum dikkate alınarak, etik ilkeler çok kapsamlı konmalıdır. Eğer kurallar belirlenmezse, psikolojik, sosyolojik, kültürel yapıları da içine alarak, insanın ve dünyanın değişmesi ile yeni etik ve ahlaki sorunlar oluşabilir. Etik bir yapay zekâ üretimi gerçekleştiğinde, yapay zekâ çevredeki araç gereçler olarak görülür, onların acıyı hissetmesi sağlanır. Eğer yapay zekâ ölümlü üretilirse, bunların her biri de etik yönetim duruşa ve ilkelere aykırı olabilir. Yapay zekânın etik inşasının etik olmaması, hem de iki şık arasında kalan ve seçim yapabilen yapay zekânın yapılması, insanın kendi etik sorumluluğunun ihlalini oluşturur. Antropolitik ve kozmik sonuca bağlı olarak etik, teolojik, metafizik, toplumsal, adli ve kültürel problemleri oluşturur. İnsan yaşamı, dünyadaki denge ve düzen, içinden çıkılmaz bir olabilir. Nihayetinde ve bilinmez bir ortamda kişilere doğru diye öğretilenlerin yanlış olduğu bir dünya gelebilir. Her şey

değişebilir, “homo sibernetikler, otonomlar, katil savaş robotları” dünyada egemen olabilir. Bu noktada çok denetimli bir şekilde yapay zekâda ilerlemeler sağlanmalı ve etik ilkeleri konusunda yasal düzenlemeler yapılmalı ve denetlenmelidir (Öztürk Dilek, 2019: 54-58). Bu konu aslında hem kamu yönetiminde etik uygulamalar, hem de hukuk bilimlerinin kapsamına girmektedir.

Bir de akıllı makineler mikrofonlarıyla, ev veya işyerinde veya araçtayken kişileri konuştuklarını dinlediği düşünülmektedir. Adres, kimlik bilgileri ve cep numarası gibi gizli olması gereken ve gizli sanılan kişisel verilere ulaşarak, bu verileri kendi “yazılım şirketlerine” gönderme kapasitesindedir. Bu geline nokta ve yapılan işlemler, kişiler için gerçek bir tehdittir. “Yazılım şirketleri”, kullanım amaçlı internete verdiği bu programları hep iyi ve güzelmiş gibi göstermektedir. İnsanlar için çok faydalı olduğunu ve işleri kolaylaştırdığını belirtir. Yapay zekâ teknolojisi ile internet uygulamaları ve siteler, kişilerin vazgeçemeyeceği hatta bağımlısı olacağı şekilde sunulmaktadır. Ama yapay zekâ teknolojisi ilgi teknolojileri kullanımındaki gelişmeler ile kişilerin gizli tutulması gereken kendine has ve özel bilgileri, hukuken haberi ve oluru olmadan toplanmakta, saklanmakta, ilgili şirket tarafından başka paydaşlara dağıtılmaktadır. Hatta üstünde değişimlere gidilebilmekte ve art niyetli şekilde kullanılıp işlenebilmektedir (Topakkaya ve Eyibaş, 2019: 87).

4.5. Siber Saldırı, Siber Zorbalık, Siber Suçlar ve Siber Güvenlik

Günümüzde siber teröristler “bilgisayarları, bilgisayar ağlarını, mobil cihazları ve akıllı cihazları” kullanarak, başkalarının kişisel bilgilerini ele geçirmekte ve kötü amaçlı kullanabilmektedir. Hatta milli ekonomiye ve milli güvenliğe zarar verebilmekte, milli sırları görebilmekte ve açıklayabilmektedir. Bu noktada dijital devlet yönetiminde siber güvenlik politikalarının önemi her geçen gün çok artmaktadır. (USOM-TRCERT, 2014:3). 2019’da UNICEF’in yayınladığı “Dünya Çocuklarının Durumu Rapor”unda okullarda dijital etik dersi verilmesi gerektiği belirtilmiştir. 2010’daki bir araştırmasında Gardner, okul ortamında çocukların internet kullanımının artışıyla “siber zorbalık”taki artıştan bahsetmiştir. Uluslararası ve ulusal çalışmalarda da çocukların, dijital etik ve siber zorbalıktan korunma ve kurtulma konusunda bilgilendirilmesi gerekliliği belirtilmiştir (Öteleş ve Merey, 2022: 1320).

2013’de NW3C’e göre sosyal medya siteleri aracılığıyla insanlar, siber alanda birbiriyle iletişindedir. “Ulusal Beyaz Yaka Suçları Merkez” tarafından, “Sosyal Medyanın Suçlu Kullanımı Raporu”nda bu alanda çeşitli suçların işlendiği belirtilmiştir Bunlar: “sosyal ağ üzerinden hırsızlık, sosyal sahtekârlık ve kimlik avı, kötü amaçlı yazılım, kimlik hırsızlığı, siber taciz ve siber yer tespiti”dir (Cengiz, 2021:415). Siber saldırı kaynaklarına bakıldığında, “hacker ve siber suçlular” ilk öne çıkmıştır. Bunlar, kişisel, özel ya da kamuya ait dijital cihaz veya ağlara izinsiz girerek bunlara ağır zarar verebilmektedir. “İç saldırganlar”, bir kurumsal örgütte kişisel amaçlarına ulaşmak için bilakis siber saldırıda bulunanlardır. “Siber aktivistler”, özel/kamu siber uzaya bilerek saldırı yapabilirler. Bu gruplar, eleştirdikleri toplumsal işlem, davranış veya eylemleri protestoda bulunmak amacındadır. “İstihbarat kurumları”na bakıldığında artık devletler ne yazık ki birbirilerini siber tehdit olarak niteleyebilmektedir. Ulusal siber güvenliği sağlamak için devletler, “siber savunma” ve “siber saldırı” ekiplerini kurup görevlendirmiştir. Bir ulusal tehdit algısı söz konusu edilmektedir. Stratejik ve gizli verileri elde etme amacı kadar, diğer ülkenin önemli altyapılarına siber saldırıda bulunmak da istenmektedir. (USOM-TRCERT, 2014:8). Tabi ki bunlar devletler için siber güvenlik politikalarında güncel ve çok dikkatli olmayı, disiplinli kurumsallaşmayı ve denetimi gerektirmektedir.

Siber suçlar, yasal olmayan veya bazı kurumların yasa dışı gördüğü faaliyetler yanında, siber alanda ve siber ağlar vasıtasıyla işlenebilmektedir. Thomas ve Loader, 2000’deki bir çalışmasında suç (yasal olmayan işlem veya eylemler) ve sapkınlık (toplumsal

kuralları hiçe sayarak toplumda kabul görmeyen işlem, eylem veya hareketlerde bulunmak) arasında bir farklılıktan bahsetmektedir. Siber suçlara karışanların tespiti ve bulunması çok zordur. Kaldı ki siber alanda gerçek kimlik bilgileri saklanarak, sahte hesap bilgileri açılabilir. Böylece kişi, sanal ortamda başka bir kişi şekline bürünür, böylece özgür hareket eder. Belki de başkasının ismini kullanarak o kişilere, zarar vermeye doğru adım atmaktadır (Cengiz, 2021:411). Bu durumda ismi ve bilgileri kullanılan gerçek kişinin, o siber suçu işlememediğini hukuki açıdan kanıtlaması gerekebilir. Kısacası böyle bir durumda sanal ortam olması bir yana, bu karmaşıklıkta gerçekçi çıkartmak için uğraşı verilmelidir.

Siber güvenlik süreçlerini, ne gibi saldırılar olabileceği ve karşı savunma mekanizmaları iyi bilinmelidir. Bu konudaki kavramlardan ilki “erişim kontrolü” olup, anlamı bilgi sistemlerine yetkisiz girişin durdurulması, izin verilmemesi, mevcut işin muhafazası ve yetkisiz işlemlerin belirlenmesidir. “Kimlik denetimi” ise, kişilere ait kimlik verilerinin doğrulanması süreci ve teknolojisidir. “Yetkilendirme”, kimliğin ilgili sitelere ve verilere ulaşma hakkının olup olmadığının belirlenmesi sürecidir. “Varlık”, siber saldırılardan korunması gereken bilgilerdir. “TC Kimlik numarası veri tabanı, kredi kartı veri tabanı ya da personel veri tabanı gibi”. “Güvenlik açığı”, sistemde var olan yazılım, donanım, işletim ve usullerde açık, hata veya eksik kalan bir noktanın olmamasına çalışmaktır. “Risk”, siber saldırı anında ve sonrasında olası zararlarıdır. “Tehdit”, zarar verme ihtimali olan bir siber saldırı/siber açıklık halidir (USOM-TRCERT, 2014: 7).

SONUÇ ve DEĞERLENDİRME

Bu çalışmada konu üzerine diğer ülkelerdeki gelişmeler yanında Türkiye’den bilgiler verilmiştir. Amaç, konuyla ilgili tarihsel ve kurumsal uygulamaları belirtmek değildir. Konuya kavramlar, önemi ve çalışma başlığıyla ilişkisi açısından yaklaşmıştır. Çalışmada genelde, “sosyal medya, dijital devlet, dijital etik, dijital aktivizm, etiketleme, dijital kimlikler, açık veri, büyük veri, blok zincir teknolojisi, teknopoli, yapay zekâ etiği, siber saldırı, siber güvenlik, siber suçlar” gibi kavramlar üzerine teorik bilgiler incelenip sunulmaktadır.

Günümüzde örgütsel düzeyde dijital çağın gerektirdiği yeni uygulamalara, kamu yönetiminden özel sektör hatta uluslararası örgütlere kadar geçilmiştir. Artık kargo hizmetleri bile dijital olarak anlık takip edilmektedir. Evdeki araç-gereçlerden, sınıftaki ekran, caddedeki trafik lambaları hatta tarladaki sulama işleri uzaktan komuta edilebilir olmuştur. Yine işyeri mail adresi gibi verilerin, yakın çevredeki bazı şirketlerce internetten alındığı ve sonrasında işyeri/evlere yemek ve içecek gönderme amaçlı mailler atıldığı bizzat görülmüştür.

Türkiye’de bilgi ve iletişim teknolojileri ve sonrasında dijital teknolojilere geçiş açısından önemli çalışmalar yapılmıştır. Dijitalleşme, devlet yönetimi politikasında değişim, dönüşüm ve e-reformun son aşamasıdır. Kamu hizmeti sunumuna artık bizzat vatandaş katılmaktadır. İdari işlem ve eylemlerin gerçekleşmesiyle ortaya çıkan büyük veri de, yeni karar alma süreçlerinin en önemli bilgisi olup, süreci etkilemektedir. Ama bu sürecin sonunda iyi yönetişimi gerçekleştirme ve kamu politikası geliştirme gerekliliği yanında, siber suçlar, siber zorbalık gibi olumsuzluklara karşı siber güvenliği sağlamak için etkin kamu politikalarının olması gereklidir.

Burada hemen 2019 yıl ekiminde ilk haberi verilen ve 2022 yazına değin tüm dünya nüfusunu etkileyen Covid-19 Pandemi Sürecinden bahsedilmelidir. Hatırlanacağı üzere ülkenin içinde şehirlerarası seyahat için ilgili kamu kurumundan (Türkiye’de Valilik’ten) izin çıkarmak gerekmiştir. Hatta ülkeler arası seyahatler bile kısıtlanmıştır. Türkiye’de e-nabızdan bu konudaki aşılamlar izlenmiş, HES kodu uygulanmış, tüm kademelerde eğitim uzaktan

(dijital ortamda) yapılmıştır. Yalnızca bir dönem (Covid-19 Pandemi sürecinin sonuna doğru ve 6 Şubat 2022 Kahramanmaraş merkezli depremlerin ardından) engelli öğrenciler için yüz yüze eğitim öğretim imkânı verilmiştir. Engelli öğrencilerini hem yüz yüze eğitimi daha faydalıdır, hem de evde kapanma sürecinde hep aynı ortamda olduğundan en çok sıkılan ve bunalan kişiler engelli insanlardır. Bu karar kanımızca çok yerinde olmuştur. Kanımızca bu sürecin sonunda kamu hizmetlerinin vatandaşlara sunumu açısından, Türkiye’de devletin dijital dönüşümü gerçekleşmiş ve açıkça dijital devlet durumuna gelinmiştir.

Covid-19 Pandemi sürecinde yine otobüs bileti alımı, kent kart dolumuna kadar hatta e-sağlık hizmeti almaya değin dijital devlet uygulamalarına geçilmiştir. Milli Eğitim Bakanlığı ve Yüksek Öğretim Kurumu’na bağlı tüm okullar e-eğitim uygulamalarında bulunmuştur. Faydalı sonuçlar da getirmiştir. Yargılamalar bile tarafların uzaktan katılımıyla yapılmıştır. Dolayısıyla bu konuda ileri ve gelişmiş devletler gibi Türkiye’de de, bilgi toplumu ve dijital devlet düzeyine geçilmiştir. Türkiye’de sadece bilimsel araştırmalar açısından, patent ve bilimsel buluş sayılarının artırılması gereklidir. Bilimsel araştırma ve geliştirme çalışmaları daha nitelikli ve bilimsel araştırma kuruluşları daha çok sayıda olmalıdır. Küreselleşen dünyada güçlü bir devlet olmak için bu dijital eksikliklerin tamamlanması şarttır. Türkiye’de dijital devlet olmak için tek eksik, buluş ve patent sayıları ile araştırma ve geliştirme çalışmalarının sayıca biraz daha artırılmasıdır.

Diğer yandan Türkiye’de dijital etik için tam bir çerçeve maalesef çizilmemiştir. Bu konuda hukukçular, yönetim bilimciler, toplum bilimciler ve diğer akademik çevreler tarafından üzerinde çalışılması gereği vardır.

Sonuç olarak artık kıtalar, bölgeler ve toplumlar arasında gelişmişlik farklılığı nedenli olarak dijital dilemma (ikilem) sorunu vardır. Dijital dünyanın bilgilerine ulaşamayan insanlar, bu yeni dünya gerçeğinden (gerçek ve dijital dünya bir arada) çok geride kalabilirler. Hem de onların dijital ortamda (sanal/siber) olası risklerden olumsuz etkilenme ve zarar görme olasılığı vardır. Türkiye’de kamu veya özel sektörde personel için dijital ortamdaki işler için çözüm stratejileri öğretilmeli dijital etik kurallar ve toplumsal farkındalık artırılmalıdır. Dijital devlet yönetiminde cesur ve gelişmelere açık olmak, artık bir gereklilikten öte, bir zorunluluktur. Devletlerin kurumsal ve uygulama yönünden hızlı, yasal zeminde ve denetlenebilir süreç içinde yönetim politikaları gerçekleştirmesi gereği vardır. Dijital dünya kesinlikle bu konuda eğitimi gerektirir. Toplumda siber suçlarla karşılaşma oranı da bu konudaki eğitim yetersizliği ve siber güvenlik önlemlerinin eksikliği sonucu görülmektedir.

KAYNAKÇA

- Akdağ, H. ve Şiraz, F. (2021). Dijital Vatandaşlığa Dönüşüm (Türkiye Özelinde): Literatür Taraması. *Kamu Yönetimi Enstitüsü Sosyal Bilimler Dergisi*, 1(1), 77-97.
- Aydeniz, H. (2021). “Editörden: Dijital Hayat ve Etik”. *TRT Akademi*, 6(12), 219-225.
- Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT) (2014). “Anasayfa”, “Hakkımızda”, www.usom.gov.tr, (Erişim Tarihi 14.09.2024).
- Bokor, T. (2021). Dijital Beşikten Sanal Mezara Gerçek-Sanal Dünyadaki Etik Sorunlar”. (Çev. Hediye Aydoğan), *ViraVerita E-Dergi, Disiplinlerarası Karşılaşmalar*, 14, 157-166.
- Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. *İletişim Çalışmaları Dergisi*, 7(3), 407-424.

- Çelik, T. ve Uyanık, G. (2020). Büyük Veri Işığında Dijital Aktivizm Üzerine Bir İnceleme: İstanbul Üniversitesi Örneği”, *EGEMİA, Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi*, (7), 4-30.
- Çeliksoy, E. ve Akça, A. (2024). Türkiye’de Kamu Yönetiminde Yaşanan Dijital Dönüşüm Süreci. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 15(2), 445-486.
- Çinçin, K. (2021). Yapay Zekâ ve Dostluk Arasındaki İlişki. *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi, Sosyal Bilimler Dergisi*, (54), 239-247.
- Demirkıran, S. ve Terzioğlu, M.K. (2024). Dijital Devlet Ekosisteminin Güçlendirilmesi İçin Dijital Vatandaşlık Ölçeği Araştırması. *Manisa Celal Bayar Üniversitesi İİBF. Yönetim ve Ekonomi Dergisi*, 31(4), 849-870.
- Gilanlıoğlu, E. ve Öze N. (2020). Dijital Yönetim Kültürünün Hegemonyası ve Serbest Zaman. *Yeni Medya Elektronik Dergisi*, 4(3), 185-202. https://yenimedya.aydin.edu.tr/wp-content/uploads/2020/09/ejnm_v4i3004.pdf, (Erişim Tarihi 14.08.2023).
- Güler, S. (2021). Üniversitelerde Dijital Etiğin İmkânı Üzerine Bir Sorgulama. *TRT Akademi Dergisi*, 6(12), 514-535.
- Kavut, S. (2021). Digital identities in the context of blockchain and artificial intelligence. *Journal of Selçuk Communication*, 14(2), 529-548.
- Mıynat, M. ve Cüre, M.F. (2023). Dijitalleşme Sürecinde Kamusal Politikaların Oluşumunda Paradigma Değişimi: Dijital Kamusal Mallar. *Turkuaz Uluslararası Sosyo-Ekonomik Stratejik Araştırmalar Dergisi*, 5(2), 41-63. <https://dergipark.org.tr/tr/download/article-file/3607289>, (Erişim Tarihi 14.09.2024).
- Öteleş, F. ve Merey Z. (2022). “Sosyal Bilgiler Öğretmenlerinin Dijital Etik Kavramına İlişkin Görüşleri”, *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 23(3), 1302-1323.
- Öztürk Dilek, G. (2019). Yapay Zekânın Etik Gerçekliği. *Ankara Uluslararası Sosyal Bilimler Dergisi*, 2(4), 47-59.
- Sucu, İ. ve Ataman E. (2020). Dijital Evrenin Yeni Dünyası Olarak Yapay Zekâ ve HER Filmi Üzerine Bir Çalışma. *Yeni Medya Elektronik Dergi*, 4(1), 40-52.
- Topakkaya, A. ve Eyibaş Y. (2019). Yapay Zekâ Ve Etik İlişkisi. *Felsefe Dünyası Dergisi*, (70), 81-99.
- Uysal, Y. ve Malkoç Yılmaz, K. (2025). Türkiye’de Kamu Yönetiminin Dijital Kültür Üzerine Etkileri. *Kamu Yönetimi ve Teknoloji Dergisi (KAYTEK)*, 7(1), 74-102.
- Vikipeidi, X (Sosyal Ağ), *Özgür Ansiklopedi* (2023). [https://tr.wikipedia.org/wiki/X_\(sosyal_a%C4%9F\)#:~:text=22%20Temmuz%202023%20tarihinde%20Elon,yeni%20logoyu%20yans%C4%B1tmak%20i%C3%A7in%20g%C3%BCncellendi](https://tr.wikipedia.org/wiki/X_(sosyal_a%C4%9F)#:~:text=22%20Temmuz%202023%20tarihinde%20Elon,yeni%20logoyu%20yans%C4%B1tmak%20i%C3%A7in%20g%C3%BCncellendi), (Erişim Tarihi 14.09.2023).