**T.C.**
**İSTANBUL ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**GAZETECİLİK ANABİLİM DALI**

**DOKTORA TEZİ**

# DİJİTAL DÜNYADA VATANDAŞLIK: BİLİNÇ, HAKLAR VE HAK İHLALLERİ ÇERÇEVESİNDE BİR ANALİZ

**Sehavet NECİYEV**

**2502190724**

**TEZ DANIŞMANI**

**Prof. Dr. Uğur GÜNDÜZ**

**İSTANBUL – 2024**

# ÖZ

## DİJİTAL DÜNYADA VATANDAŞLIK: BİLİNÇ, HAKLAR VE HAK İHLALLERİ ÇERÇEVESİNDE BİR ANALİZ

**SEHAVET NECİYEV**

Daha şeffaf bir dünya düzeni kurmak için dijital dünyada hak ve sorumluluklarının farkında olan, aktif, dinamik, sorumlu ve katılımcı bireylerden oluşan bir toplumun ortaya çıkması günümüzün bir realitesi durumundadır. Dijital dünyadaki dezavantajlara rağmen mevcut avantajlar insanların yaşam kalitesinin iyileştirilmesi hususunda mühim rol oynamaktadır.

Dijital dünyada gereken disiplin ve düzen sağlanırsa, maliyet, zaman ve emek tasarrufunun sağlanması, yolsuzlukların ve gelir dengesizliğinin azaltılması, şeffaflığın artırılması ve vatandaşlarla yöneticilerin karşılıklı etkileşimine dayalı olan "yönetişim" modelinin uygulanması da mümkün olacaktır.

Bu çalışmada, dijital dünyada temel hak ve sorumluluklarla ilgili farkındalığı artırmak, hak ihlallerine yönelik çözüm önerilerini ortaya koymak amacıyla dijital iletişim alanında bilim insanlarıyla ve uzmanlarla derinlemesine mülakatlar yapılmıştır. Temel dijital hak ve sorumluluklar irdelenmiş ve elde edilen bulgular ışığında dijital dünyadaki hak ihlallerine yönelik çözüm önerileri sunulmuştur. Bu çalışma, dijital hakların ve sorumlulukların farkında olmak, hak ihlallerine karşı bilinçlenmeye ve önlem alınması konusunda yapılacak çalışmalara katkı sağlayacaktır.

**Anahtar Sözcükler:** Dijital dünya, Dijital dünyada vatandaşlık, Dijital haklar ve sorumluluklar, Dijital dünyada hak ihlalleri

# ABSTRACT

## CITIZENSHIP IN THE DIGITAL WORLD: AN ANALYSIS OF CONSCIOUSNESS, RIGHTS AND VIOLATIONS OF RIGHTS

## SEHAVET NECİYEV

The emergence of a society consisting of active, dynamic, responsible and participatory individuals who are aware of their rights and responsibilities in the digital world in order to establish a more transparent world order is a reality today. Despite the disadvantages in the digital world, the existing advantages play an important role in improving people's quality of life.

If the necessary discipline and order are achieved in the digital world, it will be possible to save cost, time and labor, reduce corruption and income inequality, increase transparency and implement the "governance" model based on the mutual interaction of citizens and managers.

In this study, in-depth interviews were conducted with scientists and experts in the field of digital communication in order to raise awareness about fundamental rights and responsibilities in the digital world and to propose solutions to rights violations. Basic digital rights and responsibilities were examined and solution suggestions for rights violations in the digital world were presented in the light of the findings. This study will contribute to studies on being aware of digital rights and responsibilities, raising awareness against rights violations and taking precautions.



**Keywords:** Digital World, Citizenship in the digital world, Digital rights and responsibilities, Rights violations in the digital world

# ÖNSÖZ

Dijital dünyada var olabilmek için mevcut engelleri aşmak ve dijital olanaklardan faydalanırken bilinçli ve sorumlu davranışlar sergilemek her geçen gün daha da önemli hale gelmektedir. Günümüzde yaklaşık 2,6 milyar insanın dijital dünyanın dışında kaldığı ve bir kısmının da dijital olanaklardan kısmen faydalandığı bilinmektedir. Dünya toplumunun yaklaşık yarısı dijital eşitsizliklerden dolayı sağlık, finans ve eğitim gibi alanlarda kritik hizmetlerden mahrum kalmaktadır. Özellikle COVID-19 salgını döneminde dijital dünyadaki sorunların etkileri ve sonuçları global düzeyde belirginleşmiştir. Tüm paydaşların iş birliğiyle dijital hak ve sorumlulukların dünya genelinde kapsamlı bir şekilde güvence altına alınmaması düzensizliğe ve dijital eşitsizliğe neden olmaktadır. Dijital dünyadaki sorunları azaltmak amacıyla evrensel ve güvenli bir dijital ekosistemin oluşturulmasına ve bu bağlamda uluslararası bir kuruluşun yetkilendirilmesine çok ihtiyaç vardır. Hem gerçek hem de dijital dünyada sorunların üstesinden gelebilmek için dijital dünyada hak ve sorumluluklarının farkında olan, aktif, dinamik, sorumlu ve katılımcı bireylerden oluşan bir toplumun ortaya çıkması büyük önem taşımaktadır. Bu noktadan hareketle bu tezin konusu dünya toplumunun bilinçlenmesine ve dijital dünyadaki sorunların çözümüne katkı sağlamak amacıyla seçilmiştir.

Dünya toplumunun insan haklarını anlaması ve saygı duyması, zararlı içeriklerden korunması, çeşitliliği, yaşamı ve güzelliği desteklemesi, dijital olanakları kullanma becerilerine sahip olması, sorumlu bir şekilde etkileşimde bulunması, yaratması ve tüketmesi ve yeni gelişmelere ayak uydurabilmesi için yaşam boyu öğrenmesi gerekmektedir. Eğer dünya toplumu dijital hakları ve sorumluluklarıyla ilgili bilinçli davranışlar sergilerse yetkililer de sorumluluk üstlenerek çözüm üretmek zorunda kalacaklar.

Bu tez çalışmamın gerçekleşmesinde engin bilgi ve deneyimleriyle bana her fırsatta destek olan tez danışmanım, sevgili hocam Prof. Dr. Uğur Gündüz'e çok teşekkür ediyorum. Ayrıca tez çalışmamın tamamlanmasında katkıları olan İstanbul Kent Üniversitesinden Prof. Dr. Hasret Çomak hocama ve Doç. Dr. Ozan Örmeci hocama, İstanbul Üniversitesinden Prof. Dr. Aslı Gönenç hocama, Kocaeli

Üniversitesinden Doç. Dr. Betül Pazarbaşı hocama ve Dr. Öğr. Üyesi Yusuf Budak hocama, İstanbul Bilgi Üniversitesinden Prof. Dr. Erkan Saka hocama, derinlemesine görüşme yaptığım çok değerli katılımcılara ve jüri üyelerine de teşekkür etmeyi borç bilirim.

Sehavet Neciyev

İstanbul- 2024

## İÇİNDEKİLER

**ÖZ** ... ii

**ABSTRACT** ... iii

**ÖNSÖZ** ... iv

**TABLOLAR LİSTESİ** ... ix

**ŞEKİLLER LİSTESİ** ... x

**KISALTMALAR LİSTESİ** ... xi

**GİRİŞ** ... 1

**BİRİNCİ BÖLÜM**

**DİJİTAL DÜNYA DÜZENİNDE VATANDAŞLARIN HAKLARI VE SORUMLULUKLARI**

**1.1.Vatandaşlık Mekanizmasının Temel Mantığı** ... 5

**1.2. Vatandaşlığın Dijital Dönüşümü** ... 11

**1.3. Dijital Topluma Dair Kuramsal Tartışmalar ve Tanımlamalar** ... 13

**1.4. Dijital Dünya Düzeninde Vatandaşların Hakları ve Sorumlulukları** ... 24

**1.4.1. İnteraktifliğin Artırılması Amacıyla Erişim ve Katılım** ... 29

**1.4.2. Dijital Dünyada Öğrenme ve Yaratıcılık** ... 32

**1.4.3. Bilgi ve Medya Okuryazarlığı** ... 33

**1.4.4. Dijital Dünyada Etik** ... 37

**1.4.5. Dijital Dünyada Empatinin Gücü** ... 40

**1.4.6. Dijital Dünyada Sağlık ve Esenlik** ... 43

**1.4.7. Dijital Dünyada E-mevcudiyet, Dijital Kimlik ve Benlik Sunumu** ... 46

**1.4.8. Dijital Dünyada Aktif Katılımın Önemi** ... 48

**1.4.9. Dijital Haklara ve Sorumluluklara Odaklanmak** ... 50

**1.4.10. Dijital Dünyada Tüketici Farkındalığının Önemi** ... 54

**1.5. E-yönetişim Ekosisteminin Önemi** ... 57

**1.6. Dijital Dünyada Merkeziyetsiz Yapıların Yükselişi** ... 62

**1.7. Şeffaf Yönetim için Açık Veri Erişiminin Önemi** ..... 65

## İKİNCİ BÖLÜM

## DİJİTAL DÜNYA DÜZENİNDE HAK İHLALLERİ, HAK İHLALLERİNİN ETKİLERİ VE SONUÇLARI

**2.1. Dijital Dünyada Çözüm Bekleyen Sorunlar** ..... 70

**2.1.1. Dijital Dünyada Gözetim ve İfade Özgürlüğü** ..... 70
**2.1.2. Dijital Uçurum ve Toplumsal Tabakalaşma Sorunu** ..... 74
**2.1.3. Dijital Dünyada Düşünce Özgürlüğü ve Sansür Sorunu** ..... 77
**2.1.4. Yanlış Bilgi ve Dezenformasyon Sorunu** ..... 81
**2.1.5. Siyasi Propaganda İçin Dijital Olanakların Kullanılması** ..... 85
**2.1.6. Dijital Dünya Düzeninde İtaat, Direniş ve Dalkavukluk** ..... 87
**2.1.7. Troller, Botlar ve Algoritmalarla Algı Yönetimi** ..... 90
**2.1.8. Dijital Dünyada Ötekileştirme ve Yankı Odaları** ..... 94
**2.1.9. Dijital Bağımlılık ve Temel Nedenleri** ..... 97
**2.1.10. Dijital Çağda Mahremiyet Algısının Dönüşümü** ..... 99
**2.1.11. Dijital Dünyada Ekonomik ve Siyasi Güç Paylaşımı Sorunu** ..... 100
**2.1.12. Dijital Dünyada Nefret ve Ayrımcılık Sorunu** ..... 103
**2.1.13. Kişisel Verilerin Toplanması ve Korunmasına İlişkin Sorunlar** .... 106
**2.1.14. Evrensel Siber Güvenlik Ekosisteminin Geliştirilmesi** ..... 114
**2.2. Ulusal ve Uluslararası Düzeyde Dijital Hegemonya** ..... 120

**2.2.1. Egemenlik Mücadelesi Bağlamında Yapay Zekânın Geleceği** ..... 124
**2.2.2. Dijital Diktatörlüğün Çin Modeli ve Büyük Güvenlik Duvarı** ..... 127

## ÜÇÜNCÜ BÖLÜM

## DİJİTAL DÜNYA DÜZENİNDE HAK İHLALLERİ İLE İLGİLİ ÇÖZÜM ÖNERİLERİNE YÖNELİK NİTEL BİR ARAŞTIRMA

**3.1. Çalışmanın Amacı** ..... 134

**3.2. Çalışmanın Önemi** ..... 134

**3.3. Çalışmanın Sınırlılıkları** ..... 138

**3.4. Araştırma Soruları**..... 140

**3.5. Çalışmanın Yöntemi** ..... 144

**3.6. Çalışmanın Örneklemi**..... 146

**3.7. Çalışmanın Bulguları ve Yorumları**..... 147

**TARTIŞMA** ..... 189

**SONUÇ**..... 192

**KAYNAKÇA** ..... 207

**EKLER**..... 257

**ÖZGEÇMİŞ**..... 258

# TABLOLAR LİSTESİ

**Tablo 1.** Görüşme yapılan kişilerin demografik özellikleri..... 147
**Tablo 2.** Katılımcıların dijital dünyada veri tekelciliğinden kaynaklanan sorunların çözümüne yönelik düşünceleri (**TEMA 1**). ..... 148
**Tablo 3.** Katılımcıların dijital dünyada siber suçların ve savaşların önlenmesine yönelik alınabilecek tedbirler ve siber saldırılarla ilgili ülkeler arasında yapılan anlaşmaların güvenirliliğine ilişkin düşünceleri (**TEMA 2**)..... 157
**Tablo 4.** Katılımcıların egemen sınıfın dijital dünyada toplumsa ilişkileri manipüle etmek amacıyla dijital eşitsizlikleri görmezden gelmesine ve aktif katılımı çeşitli yöntemlerle engellemesine yönelik düşünceleri (**TEMA 3**)..... 166
**Tablo 5.** Katılımcıların dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların çözümüne yönelik düşünceleri (**TEMA 4**)..... 173
**Tablo 6.** Katılımcıların gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketlerin veya sosyal medya platformların serbest piyasada ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet edebilmesini zorlaştıran faktörlere ilişkin görüşleri (**TEMA 5**). ..... 179

# ŞEKİLLER LİSTESİ

**Şekil 1.** Homo Deus: Yarının Kısa Bir Tarihi kitabın kapak kısmından. ..... 16
**Şekil 2.** Sistemler ..... 17

# KISALTMALAR LİSTESİ

**AB** : Avrupa Birliği
**ABD** : Amerika Birleşik Devletleri
**AİHM** : Avrupa İnsan Hakları Mahkemesi
**BİT** : Bilgi ve İletişim Teknolojileri
**BM** : Birleşmiş Milletler
**BT** : Bilgi Teknolojileri
**CEH** : Certified Ethical Hacker
**CISSP** : Certified Information Systems Security Professional
**ÇHC** : Çin Halk Cumhuriyeti
**ÇKP** : Çin Komünist Partisi
**DSÖ** : Dünya Sağlık Örgütü
**KGAÖ** : Kolektif Güvenlik Antlaşması örgütünden
**NATO** : Kuzey Atlantik Antlaşması Örgütü
**SB** : Sovyetler Birliği
**UCM** : Uluslararası Ceza Mahkemesi

# GİRİŞ

İnternet bağlantılı teknolojilerin yaygınlaşmasıyla dijital dünyada vatandaşlık kavramının etkileri ve sonuçları da önem kazanmıştır. Dijital dünyada vatandaşlık kısaca, vatandaşlık sorumluluklarının dijital ortamda yerine getirilmesi olarak tanımlanmaktadır. Dijital beceriler, günümüzde herkesin sahip olması gereken temel bir ihtiyaç olarak karşımıza çıkmaktadır.

Dijital dünyada yaşanan gelişmelere paralel olarak vatandaşların dijital dünyadaki hak ve sorumluluklarının farkında olmaları da önemli hale gelmiştir. Hak ve sorumlulukların nihai amacı dijital dünyada adil bir ortamda yaşam kalitesinin iyileştirilmesidir. Dijital dünyada vatandaşların bu kapsamda ne kadar bilgili oldukları, nasıl bir performans sergiledikleri ve hangi haklarının nasıl ihlal olunduğu gibi olgular önemli bir çalışma alanını oluşturmuştur. Bu noktadan hareketle bu tezin ana konusunu dijital dünyada hak ve sorumlulukların tanımlanması ve hak ihlallerine yönelik çözüm önerilerinin sunumu oluşturmaktadır. Dijital dünyada vatandaş olmak ve dijital haklardan faydalanabilmek için gereken disiplin ve düzenin olmaması büyük bir sorun olarak devam etmektedir. Bu çalışmada vatandaşların dijital dünyadaki hak ve sorumluluklarını tanımlamakla birlikte hak ihlallerini aza indirmek hususunda hangi adımların atılabileceği incelenmiştir. Dijital dünyada farkındalık, disiplin ve düzen oluşturmak için hükümetlerin, işletmelerin, ulusal ve uluslararası sivil toplum kuruluşlarının ortak bir şekilde üstlenmesi gereken sorumluluklar belirtilmiştir.

Araştırma kapsamında dijital dünya düzenindeki sorunların çözümüne yönelik dünyanın gelişmiş ülkelerinde nasıl bir tutum sergilendiğine yönelik vurgu yapılmıştır. Dijital dünyada toplumsal duyarlılığa ilişkin olarak dijital uçurumun nedenleri ve etkileri betimlenmiştir. Bu bağlamda veri tabanlı teknoloji üreticisi olan büyük şirketlerin, hükümetlerin ve diğer güç yapılarının topluma karşı olumsuz tavırlarını ve etkilerini azaltmak için çözüm önerileri sunulmuştur. Büyük veri madencileri, hükümetler, siyasi partiler ve diğer işletmeler, vatandaşların hayatının her alanıyla ilgili ayrıntılı bilgilere sahiptir. İnternet teknolojilerin yaygınlaşmasıyla insanların hayatının her alanı izlenmekte ve veri olarak depolanmaktadır. Bu durumda insan hakları konusuna odaklanmak oldukça önem kazanmıştır. Yeni

teknolojiler temelinde inşa edilmiş engellerin azaltılmasıyla, bireylerin yeni teknolojilere dayanan kişisel, sosyal, ekonomik, politik ve kültürel haklarına değinilmiştir.

Dijital çağda yetkililer mekândan bağımsız olarak elektron sinyaller hızında komutlar verebilmekte ve verilen komutların istedikleri gibi uygulanıp uygulanmadığını da takip edebilmektedirler. Fakat hükümetlerin ve veri tekelcileri olan şirketlerin kendi istekleri ile vatandaşların yararına adım atmaları pek olası görünmemektedir. Büyük veri trafiğinin sıvılar gibi akışkan olduğu çağımızda Bauman'ın (2017, 262) "Lanetli üçleme" adını verdiği belirsizlik, güvencesizlik ve güvensizlik hüküm sürmektedir. Böyle bir düzende az da olsa sistemin vatandaşların yararına çalışması için ilk önce dijital dünyada olup bitenlerin farkında olmak, eylemleri takip, tespit ve tanımak gerekiyor. Söz konusu davranışları gerçekleştirebilmek için dijital dünyada vatandaşlar haklarını, sorumluluklarını bilmeli ve hak ihlallerine karşı koyabilmek için gereken bilgiye ve araçlara sahip olmalıdırlar. Bu noktada durumsal farkındalığın önemine değinmek anlamlı olacaktır:

> *Durumsal farkındalığın üç temel seviyesi vardır. İlk seviye etrafınızda olan bitenin farkında olmak; eylemleri ve olayları takip ve tespit etmek ve tanımaktır. İkinci seviye tutarsız olabilecek elementleri ele alıp onları bir araya getirerek büyük resmi görerek etrafınızda olan bitenleri anlamlandırmaktır. Üçüncü seviye bu kavrayışı kullanarak bir sonraki adımda ne olacağını yorumlamak ve bu sayede en iyi kararı verebilmektir (Hermida, 2017: 173).*

Çağın ruhuna uygun olarak dijital dünyada vatandaşlık haklarından faydalanabilmek için ilk önce dijital dünyada vatandaşlığın ne olduğunu anlamak gerekiyor. Avrupa Konseyi (2021) tarafından Dijital Dünyada Vatandaşlık Eğitimi projesi kapsamında dijital dünyada vatandaşlık on (10) başlık altında ele alınmıştır. Dijital dünyada vatandaşlık kısaca, vatandaşlık sorumluluklarının dijital ortamda yerine getirilmesi demektir, daha detaylı tanımlarsak, dijital dünyaya güvenli, bilinçli, üretken ve sorumlu bir şekilde katılma yeteneğidir. Söz konusu yeteneklere sahip olabilmek için dijital topluma erişim ve katılım, öğrenme ve yaratıcılık, medya ve bilgi okuryazarlığı, etik ve empati, sağlık ve esenlik, e-varlık ve iletişim, aktif katılım, haklar ve sorumluluklar, gizlilik ve güvenlik, tüketici farkındalığı gibi hususlar temel ihtiyaç olarak nitelendirilmektedir (Aydemir, 2019). Aynı zamanda

zaman ilerledikçe dijital hakların ve sorumlulukların çerçevesinin genişlediğini veya farklı boyuta taşındığını da göz önünde bulundurmak gerekiyor. Dünyanın dijital eğilimine bakıldığında bağlantılı davranışlar cinsiyete, coğrafyaya ve demografiye göre büyük oranda farklılık göstermektedir.

İnternet ortamında tehditler ve riskler, internete erişim sorunu, gözetim, sindirme ve siber suçlar, kişisel verilerin farklı amaçlarla izinsiz kullanımı, troller, sahte haberler, dijital eşitsizlik, suskunluk sarmalı, itibar suikastı, mahremiyet, taciz, nefret söylemi, ifade özgürlüğünün kısıtlanması, ötekileştirme ve ayrımcılık gibi konular hak ihlali olarak bilinmektedir. Bu tez çalışmasında dijital dünya düzeninde her sürecin adalet, hesap verebilirlik ve tazminat gibi temel ilkelere uygun hale getirilmesi, evrensel insan haklarını savunmak için evrensel bir insani tepkinin ortaya konulması, veri odaklı şirketlerin ve devletlerin gücünü kontrol altında tutan kurumlara ihtiyaç olduğuna dair önemli bilgiler ortaya konulmuştur.

Üç bölümden oluşan bu tez çalışmasının birinci bölümünde dijital dünyada vatandaşlık hakları ile ilgili literatür taraması yapılarak mekanizmanın işleyişine, dijital dünyada vatandaşları en çok etkileyen konulara ve dijital dünyadaki karmaşıklığı açıklayan teorik tartışmalara ve tanımlara yer verilmiştir. İkinci bölümde ise dijital vatandaşlık bağlamında çözüm bekleyen önemli global sorunlar ve tehditler anlatılmıştır.

Son bölümde hak ihlallerinin asıl nedenlerini anlamak, çözümüne yönelik veriler toplamak amacıyla dijital iletişim alanında bilim insanlarıyla ve uzmanlarla derinlemesine görüşmeler yapılmış ve elde edilen bilgiler kategorilere ayrılarak değerlendirilmiştir. Derinlemesine görüşme bağlamında alanda uzman olan 15 kişiye tez çalışması kapsamında önceden belirlenen 5 temel soru sorulmuştur.

Dijital uçurumun etkileri ve sonuçları ulusal devletlerde olduğu gibi dünya genelinde de olumsuz sonuçlar doğurmaktadır. ABD ve Çin'in liderlik ettiği dijital dünyada geri kalan ülkeler büyük oranda rekabetin gerisinde kalmıştır. Altyapısı gelişmekte olan ülkeler tarafından hazırlanan dijital platformlar ve cihazlar piyasada yeterince ilgi görmemektedir. Bu çalışma kapsamında dünya genelinde veri tekelciliği ve olumsuz etkilerine yönelik çözüm önerilerinin neler olabileceği, siber suçları ve savaşları önlemek amacıyla ne tür tedbirlerin alınması gerektiği, siber suçlara yönelik ülkeler arasında yapılan anlaşmaların ne derecede güvenilir olduğu,

egemen sınıfların dijital dünyada toplumsal ilişkileri şekillendirmek amacıyla dijital eşitsizliği göz ardı etmesi, aktif katılımı çeşitli yöntemlerle engellemesi, toplumu istediği gibi manipüle etmesine dair ne tür önlemlerin alınabileceği, dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların etkili bir şekilde çözülmesine yönelik hangi adımların atılması gerektiği, gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketlerin veya dijital platformların neden serbest piyasada Apple, Microsoft, Alphabet, Amazon, Tesla, Meta ve Netflix gibi küresel ölçekte rekabet edemediğine dair sorulara derinlemesine görüşme yöntemiyle bilim insanlarının ve uzmanların görüşlerine ve önerilerine dayanarak cevap verilmiştir.

Sonuç kısmında bilim insanları ve uzmanların görüşleri ve önerileri doğrultusunda önemli ayrıntılar özetlenmiş ve yorumlanmıştır. Bu çalışma, konusu ve kapsamı itibariyle hem akademik alanda hem de pratik düzeyde dijital vatandaşlık alanına katkı sağlamayı amaçlamaktadır. Çalışma dijital dünyadaki sorunların genel sistem ve suskunluk sarmalı kuramlarıyla açıklanması, sorunların çözümüne yönelik bilim insanlarının ve uzmanların görüşlerinin alınması ve yorumlanması konularında yenilikler barındırmaktadır. Aynı zamanda bu çalışma özellikle gelişmekte olan ülkelerin mevcut durumlarını gözden geçirmeleri ve yararlanmaları, dijital vatandaşların hakları ve sorumlulukları çerçevesinde bilinçlenmesine yönelik önemli ayrıntılar içermektedir.

# BİRİNCİ BÖLÜM

# DİJİTAL DÜNYA DÜZENİNDE VATANDAŞLARIN HAKLARI VE SORUMLULUKLARI

## 1.1.Vatandaşlık Mekanizmasının Temel Mantığı

Siyasal bir örgüte katılma hakkına sahip olan bireyler vatandaş olarak tanımlanmaktadır. Vatandaşlık da bireyle siyasal bir örgüt arasında siyasi ve hukuki bağı tanımlayan bir kavramdır. Etimolojik olarak Antik Yunan'daki şehir devletlerini işaret eden "cite" ya da "city" sözcüğünden türetilerek, şehir devletine mensubiyeti belirten "citizen" ya da "citoyen" kelimesinden doğmuştur (Polat, 2010: 5). Bu kavramın ilk defa antik çağda Yunan ve Roma uygarlıklarında kullanıldığı görülmektedir. İlk zamanlarda yalnız yönetenlerin uygun gördükleri veya kurulmuş olan düzen için bir şekilde fayda sağlayabilen bireylere vatandaşlık statüsü verilmiştir. Vatandaşlık kavramı ilk kez 1605 yılında 'hak ve ayrıcalıklara sahip, bir kentin eşrafı ya da özgür kişisi' anlamında kullanılmıştır (Özlü & Kösecik, 2016: 514). Vatandaşlık mekanizmasının insan topluluklarının yaşam biçimini belirli bir çerçeveye oturtmak ve var olan düzene çeşitli yolarla fayda sağlamaları için sorumluluklar yüklemek amacıyla oluşturulduğu anlaşılmaktadır. Tarihsel süreçte her ne kadar vatandaşlık statüsüyle teorik olarak bireylere hak ve sorumluluklar tanındığı söylense de pratikte görev ve sorumlulukların ağır bastığı bilinmektedir.

Antik Yunan site devletlerinde özgür olmayanlar (köleler), kadınlar ve yabancılar vatandaşlık kategorisinin dışında tutulmuştur. Yalnız reşit ve özgür olan erkekler katılımcı vatandaşlık statüsüne sahip olmuştur (Gökçınar, 2022: 9). Vatandaşlığın katılımcı özelliği, belirli hak ve sorumluluklara sahip olmaları anlamına gelmekteydi. Vatandaşlar belirlenmiş bir çerçevede, halk meclislerinde ele alınan kanunları tartışma ve oylama, idarecileri seçme, vergi ödeme ve askerlik görevini yerine getirmek gibi hak ve yükümlülüklere sahipti (Erdem, 2012: 51). Başka bir tanıma göre bir erkeğin vatandaş olabilmesi için, köleleri ve karısı tarafından hizmet edilen bir evin reisi olması gerekiyordu. Atina vatandaşları ev ve mülk sahibi, başkalarının emeğinin efendisi, bir savaşçı ve yerli Atinalılarla kan bağı olan erkeklerdi. Antik Yunanlılar için siyasi katılım vatandaşlığın temel parçasını

oluşturmaktaydı. Tüm vatandaşlar siyasi süreçte kendi rollerini aktif bir şekilde oynamak zorundaydılar, aksi taktirde sırayla yönetme ve yönetilme yerine, basitçe yönetilirlerdi. Antik Yunanda kamu alanını ihmal ederek tamamen özel işlerine konsantre olan birini tanımlamak için "aptal" terimi kullanılmıştır. Richard Bellamy'nin (2008: 97) ifadesiyle "Ancak bugünlerde çoğumuz bu konuda aptal olma eğilimindeyiz". Özetle Antik çağda şehrin geleceği için erdemle hareket edebilme kapasitesine sahip olan bireyler vatandaş olarak kabul edilmişler. Modern demokratik dünya düzeninde bireylerin eğitim düzeyine bakılmadan herkesin vatandaş olarak oy verme hakkına sahip olmasına bakıldığında Antik çağdaki düzenin daha demokratik olduğu anlaşılmaktadır.

Atina'daki vatandaşların sayısının 30.000 ile 50.000 arasında dalgalandığı, köle sayısının ise 80.000 ile 100.000 arasında olduğu tahmin ediliyor (Bellamy, 2008: 31). Yaklaşık üç kişiden ikisi köle, biri ise vatandaşlık statüsüne sahip olmuştur. Rakamlardan da anlaşıldığı gibi sadece belirli bir tabaka vatandaş olabilenlere tanınan haklardan ve ayrıcalıklardan faydalanmıştır. Vatandaş ve köle ilişkisi günümüze kadar süre gelen azınlığın çoğunluğu sömürme düzenini çağrıştırmaktadır. Aristoteles Politika eserinde Hippodamus'un anayasasındaki en çarpıcı noktalardan biri olan vatandaşların üç kısma bölündüğünden bahseder. Zanaatçılar, çiftçiler ve savaşçılar. Zanaatçıların, çiftçilerin ve savaşçıların hepsinin siyasal örgütte payı var. Ama çiftçilerin silahı yoktur, zanaatçıların silahı ve toprağı yoktur, bu nedenle savaşçı sınıfın kölesi olurlar (Aristotle, 1999: 37-38).

Roma Hukuku'nda hak ehliyeti yalnız hür olan vatandaşlara tanınmıştır. Kölelerin hak ehliyeti olmadığı için tıpkı bir eşya gibi hakların konusu durumunda olmuşlar. Roma Hukuku'nda vatandaşların statüleri üç kategoriye ayrılmıştır. Birincisi insanın hür veya köle olmasına göre hak ehliyetinin azalması veya yok olması. İkincisi hür olan bir insanın vatandaş olması veya vatandaş olmaması bakımından hak ehliyetinin az veya çok olması. Üçüncüsü ise bir Romalı vatandaşın başkasının hâkimiyeti altında olması veya olmaması bakımından medenî haklardan istifade ehliyetinin derecesi olarak ayrıştırılmıştır (Paul & Ayiter, 1977). Ayrıca bazı durumlarda hür olan insanların da ehliyetleri kısıtlanabilmiştir. Roma hukukunda herhangi bir vatandaş başka bir Roma vatandaşının aile hâkimiyeti altına girdiği taktirde ehliyetleri kısıtlanmıştır. Bu bağlamda da güçlülerin her zaman zayıfların

üzerinde bir şekilde tahakküm kurduğunu görmek mümkündür. Antik Roma şehir devletinde de başlangıç aşamasında sadece soyluların özgürce dolaşabildiği çeşitli kaynaklarda yer almaktadır. Şehir devleti, ancak soylu sınıfların özgür dolaştığı başlangıç aşamasını geçtikten sonra, yurttaşlar ve yabancılar arasındaki fark daha çok vurgulanmıştır (Çelebican, 1993: 299-300).

Roma'daki tarihsel gelişmeler, toplumsal değişimle birlikte, bireyin statüsünü tanımlama alanına vatandaşlık statüsünü yansıtmıştır. Ayrıca vatandaşlığı bir statüye dönüştürmek sosyal organizasyonların hedefi olmuştur. Roma'da kural olarak vatandaşlık doğumla verilmiştir. Roma vatandaşlığına sahip bir anne babanın çocuğuna ve Roma'da sağlanan bir evlilikle Romalı olmayan annesiyle evlenen Romalı bir babanın çocuğuna vatandaşlık hakkı tanınmıştır. Vatandaşlık başlangıçta kesinlikle şehirle sınırlıydı. Daha sonraki aşamada ise yeni bölgelerin sakinlerini Roma İmparatorluğu olacak geniş alana dahil etme ihtiyacı ile vatandaşlık verilmesine ilişkin teknik kuralların değiştirilmesi zorunlu hale gelmiştir. Bu ihtiyacın bir sonucu olarak, vatandaşlığın doğuştan kazanılmasının yanı sıra, Roma'da yaşamayan ancak kentle imtiyazlı ilişkileri bulunan kişilerin kamu kararıyla elde edilmesi de mümkün olmuştur (Matias, 2016).

Nihal Uluocak (1986: 5-6) vatandaşlığı "devletin tek taraflı, egemenlik hakkını kullanarak, koşullarını ve hükümlerini saptadığı bir hukukî statüyü gerçekleştiren fert ile, arasında kurulan bir hukukî bağ" olarak tanımlamıştır. Vatandaşlık mekanizmasının daha iyi anlaşılması için politik gücün merkezîleşmiş hali olan devlet oluşumunun tanımına değinmek gerekiyor. Oppenheimer'a (2005: 38) göre, devlet, zafer kazanmış bir insan grubunun yendikleri üzerindeki egemenliğini bir düzene bağlamak ve onları ekonomik alanda sömürmekten başka bir şey değildir:

> *Devlet, oluşumu sırasında tümüyle, varlığının ilk aşamalarında ise özünde ve neredeyse tümüyle, zafer kazanmış bir insan grubunun, yendikleri üzerindeki egemenliğini bir düzene bağlamak ve kendini içten gelecek ayaklanmalarla dıştan gelecek saldırılara karşı güvenceye almak amacıyla, yendiği gruba zorla kabul ettirdiği bir toplumsal kurumdur. Bu egemenliğin sonul amacı, yenilenlerin yenenler tarafından ekonomik alanda sömürülmesinden başka bir şey değildir.*

Oppenheimer'in bu tanımı yönetenlerle yönetilenler arasında kurulan vatandaşlık mekanizmasının amacını en doğru şekilde yansıtmaktadır. Gelişmiş

ülkelerde durum kısmen farklı olsa da gelişmemiş ülkelerin yönetim sistemlerinin temel mantığı bu tanımda özetlendiği gibidir. Örneğin günümüzde de Çin hükümeti "çekirdek lider" Xi liderliğindeki parti üyelerinin bireysel haklarına saygı duyması gerekçesiyle partinin ana politikalarına ters düşen eleştirileri yasalarla yasaklamıştır. Çin hükümeti ülke sınırları dahilinde büyük bir topluluk üzerindeki egemenliğini zorla kabul ettirmiş ve bir düzene bağlamak amacıyla da yasal düzenlemelerle kendisine yönelik eleştirileri yasaklamıştır. Demokratik değerlerle yönetilmeyen ülkelerde hükümetlerin teorilerine, çizgilerine, amaçlarına ve ilkelerine ters düşen görüş ve önerileri açıkça ifade etmeleri kesinlikle hoş karşılanmamaktadır. Zafer kazanmış bir grup insan ülkeyi istedikleri gibi yönetir ve onlara kimse karşı çıkamaz. Günümüz dünyasında her geçen gün yenilenen sansür düzenlemeleriyle rejimlerin sivil toplum üzerindeki kontrolünün tartışmasız bir şekilde güçlenmesi ciddi sorunlar yaratmaktadır. Tüm olumsuzluklara rağmen, yöneticiler vatandaşların refahını önemsiyormuş gibi yaparak demokratik liderleri taklit ediyor. Platona göre devletin yaranma nedeni, bireylerin tek başına kendi kendine yetmemesinden dolayı başkalarına ihtiyaç duydukları için toplum halinde yaşama zorunluluğudur. Bireyler beslenme, barınma ve güvenlik gibi ihtiyaçlarını karşılamak için birbiriyle iş bölümü yapmak zorunda kalmıştır. Toplumda iş bölümü nedeniyle üretici ve koruyucu sınıflar, daha sonra ise bu sınıflar arasındaki iş bölümünün sağlıklı işleyişini belirlediği kurallara uygun olarak denetleyecek yönetici sınıf ortaya çıkmıştır. Böylece bireyler üç farklı sınıfa bölünmüştür. Ortaya çıkan mekanizmaya da devlet adı verilmiştir. Amaç devlet mekanizmasıyla toplum için mutlu ve onurlu yaşam koşullarını sağlamak olmuştur (Platon, 1999).

Engels'in, Marx'ın "Fransa'da iç savaş" adlı eserine yazdığı önsözde Marksist devlet kuramının iki temel savını ileri sürülmüştür; 1. Devlet, egemen sınıf veya sınıfların baskı aracıdır. 2. Devlet toplum çıkarlarını koruma iddiasında olan küçük bir azınlığın sömürü aracıdır (Eroğul, 1974). Gelişmiş ülkelerden farklı olarak bu tanım gelişmekte olan ülkelerde her zaman geçerlidir. Egemen sınıfın düşünceleri, her çağda egemen düşüncelerdir. Yani, toplumun maddi egemen gücü olan sınıf, aynı zamanda egemen fikri güçtür. Maddi üretim araçlarını elinde bulunduran sınıf, bu sayede aynı zamanda zihinsel üretim araçlarının da üzerinde denetim kurar; böylelikle zihinsel üretim araçlarından yoksun olanların düşüncelerini de genel

olarak, kendine tabi kılar (Engels & Marx, 2013: 52). Orta çağda şehirlerle ve vatandaşlar arasında karşılıklı olarak nitelendirilen sorumluluklar vardı. Vatandaşlar sadakat, askerlik hizmeti ve vergi ödeme sorumluluğunu üstlenir, şehirler de koruma sorumluluğunu üstlenirdi. Vatandaş olmak isteyen bireyler, on yıllık ikamet taahhüdü ve vatandaşlık yükümlülüklerini yerine getirdikten sonra vatandaşlığı hak ediyordu. O dönemde iyi olarak nitelendirilen vatandaşlar kamu hizmetine katılan, yaşadığı topluma ve hükümdarlarına hizmet eden bireylerdi. Fransız devriminden önce kişisel özgürlük, mülk sahibi olmak ve eşitlik fikri önem kazanmıştı. Devrim, 1789'da vatandaşlık (modern sözleşme) fikriyle gerçekleşmiştir. Sonuç olarak mutlak monarşi devrilip, yerine cumhuriyet kurulmuştur ve Katolik Kilisesi de ciddi reformlar yapmak zorunda kalmıştır. Devrimle Fransa'da tüm sakinlere medeni haklar tanınmış ve Fransız topraklarında aktif vatandaş olmak için yemin ve doğum ön koşullar olarak kabul edilmiştir.

Genel olarak toplumların yönetim şekline bakıldığında her zaman en güçlü olanlar yöneten pozisyonda, diğerleri ise yönetilen/köle konumunda bulunmuştur. Eski düzenin temellerini düşünceleriyle sarsan Sokrates de en güçlülerin değil, en akıllıların başa geçmesini istediği için ölüme mahkûm edilmiştir. Aslında bu ilkel mantık insanlık tarihinde hiçbir zaman değişmemiştir. Zaman ilerledikçe otoriter baskıların görünürlüğü artmaya devam etmektedir. Günümüz dünyasında da gelişmekte olan ülkelerde hükümetler devletin imkânlarını kullanarak kendisine karşı çıkan herkesi çeşitli yöntemlerle bertaraf etmektedirler. Bu durumun her alanda aynı olduğunu ve ülkelere göre farklılık gösterdiğini söylemek yanlış olmaz. Anayasal vatandaşlık düzenine geçmeden önce katı sınıfsal tabakaları kırmak ve toplumsal dokuyu birleştirici bir konsepte ihtiyaç vardı. Özellikle Fransız devriminden sonra vatandaşlık olgusunun bir bakıma çok eşitlikçi bir rol oynadığı, soyluları, din adamlarını, burjuvaları ve diğer bireyleri aynı kategori altında birleştirmeye muktedir olduğu düşünülmüştür (Matias, 2016). Fakat anayasal vatandaşlık düzenine geçtikten sonra kısmen iyi adımlar atılmış olsa da eski düzenin temel mantığı devam etmiştir. Ülkelere göre az veya çok farklılıklarla dijital kapitalist düzende her şey egemenlik aracı olan parayla satılıp alınabilir ve nesneler insanlardan daha kıymetli hale gelmiştir.

Devrimci ayaklanma ile sözleşmeci doğal haklar teorisi arasındaki bağlantının ürünü olan liberal vatandaşlığın ortaya çıkmasında Büyük Britanya önemli rol oynamıştır. Modern vatandaşlık anlayışı, 1776 yılında Amerikan Bağımsızlık Savaşı ile 1789 yılında Fransız Devrimi'nden sonra ortaya çıkan anayasacılık hareketi ile şekillenmiştir (Korkut, 2014: 7). Egemenlerin ortaya koyduğu idari prosedürlere uygun olarak sözde demokratik ilkelerle rejimlerin politik düzeni kurulmuştur. Dijital kapitalizm çağında geleneksel vatandaşlık anlayışının anlamını kaybettiğini her alanda görmek ve anlamak mümkündür. Her türlü gücün hükümetlerin ve uluslararası kuruluşların elinde olmasına rağmen dünyanın farklı bölgelerinde binlerce insanın vahşice öldürülmesi, güvencesiz çalışma, yüksek işsizlik, suikastlar, cinsel şiddet, tecavüz, yolsuzluklar, mafya kontrolü, savaşlar ve nefret söylemleri gibi sorunlarla ilgili çözüm üretilmemektedir. Bununla birlikte yargı mekanizmasının çalışmaması ve caydırıcı cezaların verilmemesi var olan politik düzenin sıradan vatandaşların yararına olmadığını net bir şekilde göstermektedir. Mevcut sistem ulusal düzeyde bile kapsayıcı değildir. Sonuç olarak günümüzde politikacılara, hükümetlere, siyasi partilere, sendikalara, uluslararası kuruluşlara ve politikalarına karşı ciddi bir güvensizlik yaratmıştır (Canclini, 2018).

En basit anlamıyla 'doğrudan' veya 'katılımcı' demokratik yönetim biçimi yöneticilerin yönetilenler tarafından seçilmesi, hesap verebilir olması ve gerektiğinde görevden alınabilmesi anlamına gelir. Ama günümüzde özellikle gelişmemiş ülkelerde bu hususların hiçbiri kesinlikle mümkün olmadığı için vatandaşlar devlet yönetiminde hiçbir şekilde söz sahibi değiller. Vatandaşlık mekanizmasının geldiği noktada ağır vergi yükü altında ezilen vatandaşlar orantısız baskılarla karşı karşıya kalmaktan korktukları için yönetenlere hesap sormaya kolay kolay cesaret edemezler. Gelişmemiş ülkelerde her zaman olduğu gibi günümüze de güçlü olanlar kendi otoriter düzenini kurmuş ve yönetmeye devam ediyorlar. Aynı zamanda dijital çağda yönetenler dijital panoptikon imkânlarla daha planlı ve organize bir şekilde hareket edebildiğine göre eskiye nazaran kat kat güçlü konumdadırlar. Yönetim şekli ve amaçları birbirine benzeyen hükümetler birbirini koruyup kollamayı da ihmal etmezler. Gelişmemiş ülkelerde devletin maddi olanaklarını istedikleri gibi harcayan hükümet yetkilileri görünürde demokratik seçimler düzenleseler de genellikle sonuç değişmez. Gerektiğinde bazı muhalif parti yetkilileriyle çıkar ittifakı kurmaktan da

hiçbir zaman çekinmezler. İnternet ortamında hükümet yetkilileriyle "muhalif" parti yetkilileri arasında veya farklı çıkar grupları arasında iş birliği yapıldığı zaman zaman haberlere yansımıştır. Sonuç olarak bazı özel durumlarda yönetenlere karşı ciddi bir güvensizlik ve büyük bir huzursuzluk hüküm sürmektedir.

### 1.2. Vatandaşlığın Dijital Dönüşümü

Vatandaşlık mekanizmasının ilk biçimi antik Yunan ve Roma şehir devletinde ortayı çıkmıştır. Daha sonra Roma imparatorluğunun kurulmasıyla, şehir devletlerindeki vatandaşlık mekanizması da değişmek zorunda kalmıştır. Orta çağda yaşanan sancılı sürecin sonucunda Fransız devrimiyle mutlak monarşinin devrilip, yerine cumhuriyetin kurulmasıyla vatandaşlık mekanizması farklı bir boyut kazanmıştır. 26 Ağustos 1789'da demokrasi ve özgürlük gerekçesiyle Fransa Ulusal Meclisi'nde 17 maddelik "İnsan ve Yurttaş Hakları Bildirgesi" kabul edilmiştir (Hammersley, 2015: 80). Daha sonraki süreçte geliştirilen yasaların büyük çoğunluğu bu 17 maddelik temel üzerine inşa edilmiş ve geliştirilmiştir.

Zaman, mekân ve insanlığın gelişimine paralel olarak toplumsal yapı da sürekli bir değişme ve gelişme içindedir (Gündüz, 2018: 231). Daha önceki çağlarda olduğu gibi dijital çağda da vatandaşlık kavramına farklı anlamlar yüklenmekte ve farklı pratikler ortaya çıkmaya devam etmektedir. Gelişmiş ülkelerde sanayi toplumundan sonra bilgi toplumunun ortaya çıkmasına paralel olarak vatandaşlığın dijital boyutu gündeme gelmiştir. 1990'lardan sonra internetin yaygınlaşmasıyla dünya düzeninde hızlı bir değişim yaşanmaya başlamıştır. Vatandaşlık kavramı da bu değişimden etkilenerek dijital dünyada vatandaşlık anlamına gelen küresel vatandaşlık, çevresel vatandaşlık ve çok kültürlü vatandaşlık olarak tanımlanmıştır.

İnternet aracılığı ile dünyanın dört bir yanından birbiri ile bağlantı kuran insanların aynı çevrimiçi ortamı aynı şehri paylaşır gibi paylaşması dünyanın aynı zamanda dijital bir yer olduğunu göstermiştir. Üreticiler ve girişimciler, pazarlamacılar ve sıradan tüketiciler dijital dünyayı sürekli olarak birlikte yaratıyor ve güncelliyorlar, yenilikler dünya çapında paylaşılmakta, benimsenmekte ve tüketicilerin davranışlarını etkilemektedir (Ratchford, 2019). İnternet bağlantılı teknolojiler sosyal, politik, kültürel ve ekonomik yapıların ve uygulamaların dönüşümünü de zorunlu hale getirmiştir (Örs & Tetik, 2010). Dijital dünyada

vatandaşlık kısaca, vatandaşlık sorumluluklarının dijital ortamda yerine getirilmesi demektir, daha detaylı tanımlarsak, dijital dünyaya güvenli, bilinçli, üretken ve sorumlu bir şekilde katılma yeteneğidir. Kullanıcılar internet bağlantılı cihazlarla alışveriş yapmaktan tutun da trafik cezası ödeme, kredi kartı borcu ödeme, dava dosyası takip etme, kan tahlil sonuçlarını öğrenme, sınav sonuçlarına bakma, dünya gündemini takip etme, dijital ortamda arkadaşlıklar kurmak gibi daha birçok faaliyeti yapabilmektedirler (Çatlı ve Keskin, 2021: 210). Bununla birlikte dünya nüfusunun yarısından fazlası söz konusu faaliyetleri az zaman ve az maliyetle yerine getirme hakkından mahrumdur. İnternet olanakları olmaksızın geniş kapsamda ölçülebilen şeffaflığın sağlanması neredeyse imkânsıza yakındı. İnternetin yaygınlaşmasıyla insanlar büyük oranda hem çevrelerinde hem de dünyada olup bitenlerden haberdar olmaya başlamıştır. Aynı zamanda toplum için gerekli olan tüm uygulamaların pratiklerin, hizmetlerin dijital ortama taşınmasıyla dijital dünyada vatandaşlık için gerekli olan bilgilerin, araçların ve dijital ortamda var olabilmek için gerekli olan yeteneklerin öğrenilmesi zorunlu hale gelmiştir. Yaşam kalitesinin yükseltilmesi için teknolojik altyapının güçlendirilmesi de hükûmetlerin yerine getirmesi gereken bir sorumluluk olarak önem arz etmektedir. Uluslararası örgütlerin dünya genelinde etkili hale gelmesiyle ulusal devletler toplum üzerinde tek yetki sahibi olmaktan çıkmıştır (Lenz, 2017). Bu bağlamda dijital dünyada vatandaşlık küresel vatandaşlık olarak da tanımlanmaktadır.

Özellikle COVID-19 pandemisi döneminde vatandaşlığın dijital dönüşümü her alanda etkisini göstermiştir. Örneğin COVID-19 pandemisi kısa bir süre içinde film setlerinin, tiyatroların, operaların, konser salonlarının kapanmasına ve küresel konser turlarının iptaline, kısacası tüm sanatsal faaliyetlerin durmasına sebep olmuştur. O dönemde sanatsal faaliyetler de çevrimiçi ortama taşınmıştır (Ünlü, 2021: 7). Dijital çağın ihtiyaçlarına uygun olarak anayasal reformların yapılması ve vatandaşlığın dijital dönüşümü için gereken altyapının sağlanması da zorunlu hale gelmiştir. Dünyadaki dijital dönüşüm tüm olanaklarıyla günlük hayatımıza yön vermektedir. Bizler bu büyük dönüşümün katılımcı ve gözlemcileriyiz; yenilikler meydana geldikçe tüketerek değişim dalgalarına katkıda bulunuyoruz (Rindfleisch & Malter, 2019).

### 1.3. Dijital Topluma Dair Kuramsal Tartışmalar ve Tanımlamalar

Karmaşık teknolojik ve sosyal yapıları anlamak ve dijital dünyadaki zararlı davranışlara karşı koya bilmek için dijital hak ve sorumlulukların farkında olmak temel bir gereksinimdir. Fuchs'un ifadesiyle (2016: 21-22) yaşadığımız çağda dünya çapındaki eşitsizlik, küresel ekonomik kriz, küresel ekolojik kriz, savaş ve terörizm, yüksek işsizlik, güvencesiz yaşama ve çalışma koşulları, artan yoksulluk seviyeleri vb. ile şekillenen çalkantılı zamanlarda yaşıyoruz. Dijitalleşme her ne kadar hayatımızı kolaylaştırsa da kapitalist bir düzenin parçası olduğu için birtakım sorunları da beraberinde getirmiştir. Bauman'a göre (2017, 70-71), "De jure bireyseniz yaşadığınız sefalet için kimseyi suçlayamaz, başarısızlığınızın suçunu kendi miskinliğiniz ve tembelliğinizden başka bir şeye yükleyemez ve hep daha çok çabalamaktan başka bir çare arayamazsınız".

"Büyük Birader"in (Orwell, 1949) ruhunun tavan aralarından ve bodrum katlarından çekildiği söylense de günümüz dünyasında internet bağlantılı cihazlarla misyonunu daha da kolay bir şekilde sürdürmektedir Yurttaşlar daha kolay gözetlenmekte, etiketlenmekte, ötekileştirilmekte ve manipüle edilmektedirler. Bilindiği üzere yaşam politikaları alternatiflerini başlatma iktidarında olanlar politik ve ekonomik güce sahip olanlardır. Alternatif bir ortak yaşam arayışını ortaya koymak güç ve kontrol yapılarının işine gelmediği için tercih edilmemektedir. Politik ve ekonomik güce sahip olanlar ellerindeki gücü muhalif olarak gördükleri hiç kimseyle paylaşmak istemiyorlar. Dünya genelinde ağırlıklı olarak devletlerin kaynaklarının savunma sanayisine harcanması yaşamı dengesiz bir şekilde olumsuz etkilemektedir.

Konfüçyüs (MÖ 551-479), bireysel refahın iyi karaktere ve bir bütün olarak toplumun düzgün işleyişine bağlı olduğu "bütüncül" bir insan doğası anlayışını savunmuştur (Donnelly, 2022: 6). Her toplum bir bütündür, yani birbiriyle ilintili unsurların oluşturduğu bir sistemdir (Ceylan, 2011: 90). Dijital dünya düzenine sistem yaklaşımı perspektifinden bakıldığında dünya toplumunu olumsuz etkileyen sorunların birbiri ile bağlantılı olduğu görünmektedir. Çok karmaşık görünen olaylara sistematik bir yaklaşımla odaklanan genel sistem kuramına göre sistem birbiriyle uyumlu ve dinamik çalışan farklı bileşenlerden oluşmaktadır. Başka bir deyişle sistem yaklaşımı nesnelerin ve canlıların birbiriyle bağlantılı olduğu dünyaya

bakmanın bir yoludur. Oxford English Dictionary'e göre sistem belli bir plan veya projeye göre sırayla düzenlenen parçaların oluşturduğu bir bütündür (Kılıç, 2011).

Genel sistem teorisinin kurucularından biri olan Spencer, astronomi, biyoloji ve psikoloji gibi çeşitli bilim dallarında aynı temel ilkenin geçerli olduğunu, varlıkların belirsiz, tutarsız bir homojenlik halinden belirli ve tutarlı bir heterojenliğe doğru evrildiğini belirtmiştir (Gönç Şavran vd., 2019: 6). Kendini organize eden evrende, kendini aşan süreçlerin nasıl fiziksel, biyolojik, sosyal ve psikolojik sistemler ürettiği Erich Jantsch tarafından açıklanmıştır (Bausch, 2001). Sistem yaklaşımı; doğadaki, toplumdaki ve bilim alanlarındaki olayları bütünsel olarak inceleyebileceğimiz bir çerçeve olarak kabul edebileceğimiz disiplinler arası bir teoridir (Akkuş & İzci, 2018: 224). Ludwig von Bertalanffy mühendislik, biyoloji, Gestalt psikolojisi ve özellikle sibernetik alanındaki entelektüel geleneklerden yararlanarak genel sistem kuramının ilkelerini toplumsal ve kültürel dünyaya da uyarlanabilecek şekilde genişletmiştir (Collins, 1988:47-48). Bertalanffy'e göre her olayı çevresiyle birlikte başka olaylarla etkileşimli veya bağlantılı olduğunu göz önünde bulundurarak incelemek genel sistemi anlamak, tahmin etmek ve kontrol etmek açısından önemlidir.

Sistemler dış çevreleriyle etkileşimde bulunduğunda açık, etkileşimde bulunmadığında ise kapalı sistemler olarak adlandırılmıştır. Çevre sistemin dışında kalan ve sistemin parçası olmayan her şeyi içerir (Akkuş & İzci, 2018: 231). Dijitalleşmenin etkisiyle sitemlerin daha geniş dış çevreyle etkileşimi kaçınılmaz hale gelmiştir. Bu durumda dijital dünya ile fiziksel dünyadaki olayların iç içe geçtiği, birbirinden aslı olduğu veya zincir halkaları gibi birbiriyle bağlantılı olduğu anlaşılmaktadır. Biyolojik bir kuram olan genel sistem kuramı dinamik parçalardan oluşan yeni dünya düzeninin işleyişini incelemek ve anlamak için önemli bir araç niteliğindedir. Toplumsal düzen canlı bir organizma olarak göz önünde bulundurulduğunda içende barındırdığı tüm varlıkların ve yönetim mekanizmasının birbirleriyle etkileşimli ve bağlantılı olduğu anlaşılmaktadır. Dolayısıyla toplumsal sistem, kendisini oluşturan unsurlardan ve onlar arasındaki ilişki ağından başka bir şey değildir ve her bir unsur belli normlara göre hareket etmekte, belli işlevleri yerine getirmektedir (Ceylan, 2011: 91). Sistemin alt grupları nasıl oluşmuş olursa olsun, hepsinin bütünün davranışı üzerinde etkisi vardır (Skyttner, 2005: 57-58). Bir

sistem olarak canlı bir organizmanın varlığını devam ettirmesi organların sağlıklı olmasına bağlı olduğu için organizmanın bir bütün olarak kendini yenileme mekanizması vardır. Toplum düzeninde ise bireyden başlayarak dünya düzenine yön veren en güçlü aktörlerin bulunduğu her aşamada sistemin devam etmesi için ya doğrudan ya da dolaylı yollarla baskı mekanizmaları vardır. Aile ortamında, ulusal devletlerde veya dünya genelinde belirlenen değerlere karşı çıkanlar bir şekilde cezalandırılır, itaat edenler bazen ödüllendirilir. Bu ceza veya ödül mekanizmaları toplumsal sistemin yenilenmesini ve dengede kalmasın sağlar. Alt sistemler çevreleriyle etkileşime açık oldukları için büyük bir kesimin sürekli huzursuz olması kaçınılmazdır. Sonuç olarak dinamik dengenin sağlanması kolay değildir.

Dünya toplumunu etkileyen tüm sorunların aslında bireylerin bencilliğinden veya karaktersizliğinden kaynaklandığını söylemek yanlış olmaz. Harari (2014) Homo Deus: Yarının Kısa Bir Tarihi adlı kitabında "Kapitalist düzende anlamdan vazgeçmek pahasına kabul edilen sözleşmelere göre ahlak, güzellik, hatta merhamet; tanrıların, cennetin ve cehennemin olmadığı" bir dünyada insanların nasıl baş edebildiğine değinmiştir. Kitabın ön kapağı üzerinde dört adet, soldan sağa doğru; taştan yontulmuş bir ok ucu, metalden yapılmış bir ok ucu, bir mermi ve parmak izine benzeyen çip simgesine yer verilmiştir. Bu simgelerle insanların her çağda imkânları yettiği kadar savunma veya saldırı amacıyla geliştirdikleri silahların tarihsel evrimi özetlenmiştir. İnsanların birbirini çeşitli yöntemlerle öldürmeye veya sömürmeye çalışmasının sadece vahşi kapitalist düzene özgü olmadığı, insanoğlunun var olduğu günden günümüze kadar bencil, agresif ve saldırgan tavırlar sergilediği simgelerden de anlaşılmaktadır. Dijital dünya düzeninde söz konusu saldırganlığın ve sömürgeciliğin dijital olanakların kullanılarak sürdürüldüğü de yaygın olarak bilinmektedir. İnsanlık tarihine bakıldığında kullanılan silahların ve yöntemlerin daha etkili ve daha isabetli olması yönünde geliştirilmesi dikkat çeken önemli bir husustur. Gelecekte de savaşlarda mümkün olduğu kadar çip temelli otonom silahların kullanılması ve bunun yanı sıra veri sömürgeciliğinin yaygınlaşması kaçınılmazdır. Gelişmeler ışığında insanların bencil, merhametsiz, agresif ve saldırgan olduğunu söylemek yanlış olmaz. Bu yaklaşım mikro düzeyde bireyler için geçerli olduğu gibi makro düzeyde de agresif tavırlar sergileyen devletler veya hükümetler için de geçerlidir.



**Şekil 1.** Homo Deus: Yarının Kısa Bir Tarihi kitabın kapak kısmından

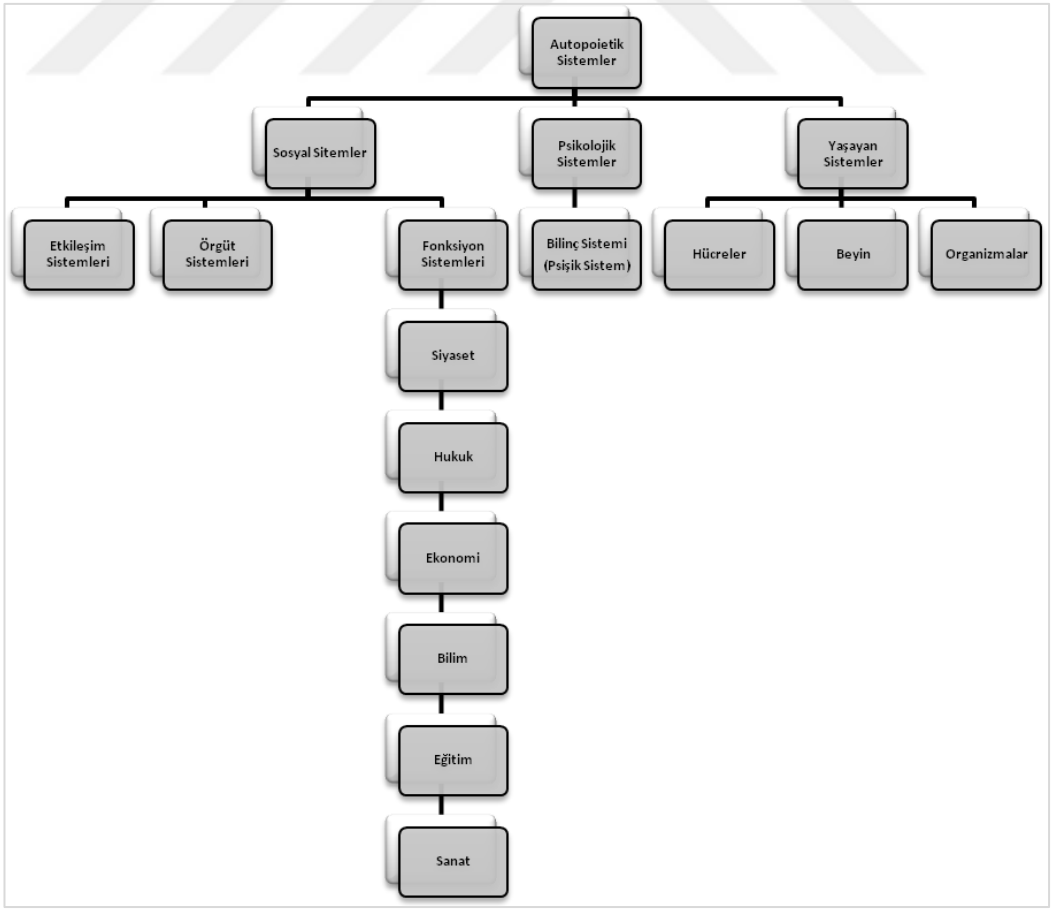
Dünya düzeninde sorunların sebep ve sonuç ilişkileri döngüseldir (Akkuş & İzci 2018). Sistem yaklaşımı sorunların tüm yönlerini ele alarak parçalar arasındaki dinamik etkileşime odaklanmaktadır (Tecim, 2004: 78-81). Dijital dünyada veri tekelciliği veya sömürgeciliği ve siber saldırılar veya savaşlar, gözetim sorunu gibi çeşitli kişisel hakların ihlali birbiriyle bağlantılı çıkar çatışmalarıdır. Bu çıkar çatışmalarının temel nedeni doğal madenlerin toprak altından çıkarılıp işlenmesi ve kullanıma sunulması gibi insanların davranışlarıyla ilgili verilerin bilinçaltlarından toplanarak işlenmesi (Doyle, 2023: 17-18) ve elde edilen muazzam finansal gücün tek elde toplanmasıdır.

Veri madenciliğinden ve dijital teknoloji üretiminden elde edilen finansal gücün ABD merkezli şirketlerin tekelinde toplandığı bilinmektedir (Yıldız, 2021: 456-459). Çin kendine özgü dijital ekosistemini yaratarak ABD merkezli teknoloji şirketleriyle rekabet edebilecek düzeye ulaşsa da şimdilik ABD lider ülke konumundadır. Siber suçlarla ilgili yapılan uluslararası yasal düzenlemeler ve anlaşmalar tehlikeleri önlemek için yeterli değildir. Uluslararası medyada Rusya tarafından ABD'nin petrol boru hatları, havaalanları ve enerji santralleri gibi kritik altyapılarını hedef alan siber saldırıların gerçekleştirildiği zaman zaman haberlere yansımaktadır. Pek çok fidye yazılımı çetesinin Rusya'da bulunduğuna dair birçok gösterge vardır (Tidy, 2021). Dünya genelinde tüm hükümetler çıkarları uğruna çeşitli sorunlar yaratmakta veya kirli pazarlıklar yapmaktadırlar. Bu sorunlar bir canlının organizmasındaki organlar gibi birbiriyle bağlantılıdır. Otonom silahların yaygınlaşmasıyla dünyadaki çatışmaların daha da artacağı öngörülmektedir (Leveringhaus, 2016: 14-15; The World Economic Forum, 2024).

Toplumsal sistem, parçaların bütün için etkileşimli ve bağımlı çalıştığı, kendini yenileyen ve sürekli hareket halinde olan bir yapıdır. Luhmann'ın savunduğu sistem yaklaşımında en çok üzerinde durduğu kavram kendi kendini yeniden üretme anlamına gelen "autopoiesis" kavramıdır. Autopoietik sistemlerin beş özelliği vardır (Ertong, 2011: 10);

- Sistem, sistemi oluşturan temel elementleri üretir.
- Kendilerini düzenlerler.
- Kendi sınırlarını çizerler.
- Sistem ve çevreyi ayrıştırırlar.
- Kendi içyapılarını düzenlerler.

Sistem, belirli bir amaca göre belirli bir çevrede yer alan, birbirleriyle ilişkileri olan, belirli kurallara göre işleyen bir mekanizmadır (Luhmann, 1995: 29-31). Sistem yaklaşımına göre asıl önemli olan bütündür, parçalar ise bütünü etkilediği ölçüde önemlidir.




**Şekil 2.** Sistemler (Luhmann, 1995; Moeller, 2006; Yoldaş, 2007; **akt.** Ertong, 2011: 10)

Ertong'un (2011: 10) derleyerek oluşturduğu şekil 2'de görüldüğü gibi autopoietik sistemler Luhmann tarafından üç temel başlık altında sınıflandırılmıştır; sosyal sistemler, psikolojik sistemler ve yaşayan sistemler. Luhmann (1995) genel toplumsal sistemin çeşitli alt sistemlerden oluştuğunu ve birbiriyle dinamik bir şekilde bağlantılı olduklarını vurgulamıştır. Sosyal sistemlerin kendilerini yenilemesi ve varlığını sürdürebilmesi için fonksiyon sistemler başat rol oynamaktadır. Modern kapitalizmin ekonomik kompleksi ve onun teşvik ettiği toplumsal hareketlerin bütünü sisteme özgü iletişim kodlarıyla dünya düzenini şekillendirmektedir. Öğelerin, süreçlerin, duyguların, düşüncelerin ve davranışların da sistemin bir parçası olduğu mevcut dünya düzeni ağırlıklı olarak dijital ortamda şekillenmektedir.

Herkesin gözetlene bildiği yeni dünya düzeninde, sorunların kimler tarafından, neden ve nasıl yaratıldığı dijital platformlarda yaygın olarak bilinir hale gelmesine rağmen dijital ortamlarda yeterince müzakere edilmemesinin temel nedeni 1974 yılında Noelle Neumann'ın kitle iletişim araçları bağlamında geliştirdiği suskunluk sarmalı kuramıyla açıklanabilir. 20 yüzyılda geliştiren bu kuramın temelleri fikirleri toplum veya çevresi tarafından desteklenmeyen bireylerin konuşmaktan çekinmesine veya korkmasına dayamaktadır. Bireyin görüşünün çoğunluk tarafından onaylanmaması, bireyin aksi bir görüş dile getirmesi veya kamuoyu önünde çoğunluğun onayladığı davranışların aksine hareket etmesi tecrit tehlikesi doğurur (Noelle-Neumann, 1974). Ama tam tersi olarak fikirlerinin onaylanacağını hisseden bireylerin, fikirlerini korkusuzca ve bazen de yüksek sesle dile getirmeye meyilli oldukları gözlemlenmiştir. Düşüncelerinin kamuoyu tarafından kabul gördüğünü ve çoğunlukta olduklarını hisseden gruplar düşüncelerini çekinmeden ifade ederken, azınlıkta olduğunu düşünenler ise dışlanma korkusuyla düşüncelerini çoğunluk yönünde değiştirir ya da ifade etmek yerine suskunluk sarmalına girerler (Kutlu, 2019: 45-46).

21. yüzyılda internet bağlantılı teknolojilerin yaygınlaşması ve gözetim olanaklarının artmasıyla suskunluk sarmalının çerçevesi genişlemiş ve farklı bir boyuta taşınmıştır. Otoriter/totaliter yönetimler tarafından yönetilen ülkelerde bireylerin korktukları için düzene uyum sağlamak zorunda kaldıkları bilinmektedir (Kamil, 2020: 290; Moreland-Capuia, 2021). Avcı ve toplayıcı topluluklarda bireylerin fiziksel özelliklerine göre kendilerinden daha güçlü olan türünden, vahşi

hayvanlardan ve yıldırım gibi doğal afetlerden korktukları gibi modern dünyada bireyler egemen güç ve kontrol yapılarından korkarlar. Korku toplumsal bir uyum aracı olarak işlevselleştirilmiş ve korku kültürü olarak yaygınlaştırılmıştır (Eren, 2005).

Baskı ve korku kültürünün içinde dünyaya gözlerini açan bireyler yaşamlarının ilk yıllarından itibaren nelerden ve kimlerden korkmaları gerektiğini öğrenmeye başlar ve öğretilmiş çaresizlikleri kabullenmek zorunda kalırlar. Ailede başlayan korku kültürü eğitim kurumlarında pekiştirilmektedir (Cüceloğlu, 2018; Mullahi & Dhimitri, 2015; Robin, 2004). Sistemlerin işleyişine uygun davranışlar sergilemeyen bireyleri veya grupları dışlamak, kısa yoldan saf dışı bırakmak için bir dizi kalıplaştırılmış yakıştırmalar ve etiketler her zaman hazır beklemektedir (Asch, 2016; Oğuz, 2023: 119-120). Aynı zamanda baskıcı hükümetler devletin ekonomik imkânlarını ve yetkilerini kullanarak bireylerin gelir kaynaklarını kısıtlayıp toplumu susmaya veya itaat etmeye mecbur ederler. Daha sonraki aşamada ise gerekirse hükümetin kontrolündeki diğer enstrümanlar (alt sistemler) baskı yapmak amacıyla kullanılır. Bu tür sistemlerde hükümetler mevcut düzene karşı tehdit olarak görülen kişileri veya grupları susturmak veya baskı altında tutmak için devletin itibarı dahil tüm imkânlarını kullanmaktan çekinmezler.

Baskı ve kontrol amaçlı dijital gözetim egemen güçler veya hükümetler tarafından yüksek seviyede gerçekleştirilmektedir (Dolgun, 2004). Korku kültürünün yaygınlaşmasında kitle iletişim araçlarının büyük rolü vardır (Yılmaz, 2013). Parlamenter düzenin ve demokrasinin rafa kaldırıldığı devletlerde serbest piyasa koşulları oluşmadığına göre insanların gelir kaynakları ya kamu kurum ve kuruluşlarıdır ya da hükümetlerin kontrolündeki özel şirketlerdir (Harrijvan, & Weerdesteijn, 2020). Durum böyle olunca baskıcı rejimler için insanların gelir kaynaklarını kısıtlamak çok kolaydır (Arıkan, 2001: 238-242). Özellikle devlet kurumlarında çalışanlar işlerini kaybetmemek korkusuyla tüm emir ve talimatları sorgulamadan uygulamak, sadakatlerini göstermek amacıyla sistemin lehine konuşmak veya içerikler paylaşmak ya da susmak zorunda kalmaktadırlar. Hiç kimse çok zor durumda kalmadığı sürece sahip olduklarını kaybetmek (Debs, 2010) veya suçsuz yere hapse atılma ihtimalini göze almak istemez.

Baskıcı rejimlerde sivil oluşumların ortaya çıkması ve yönetilenlerin hükümetin yolsuzluklarına ve başarısız politikalarına karşı çıkmaları neredeyse imkânsızdır. Dayanışma içinde olan grupların arasına trollerin sızması (Rone, 2022) bireyleri güvensizliğe sürüklemektedir. Ayrıca bireylerin bulundukları pozisyonlarda yükselmesine dair vaatler ve beklentiler de otoriter sistemlerin kendini yenilemesine hizmet etmektedir (Aktaş, 2023: 152-153). Hukuk sisteminin en tepeden verilen talimatlarla işlemesi, işlevsiz ve hantal olması otoriter sistemlerin önemli özeliklerinden biridir (Solomon, 2007). Cezaların gerçek anlamda caydırıcı olmaması ve yargı mekanizmasındaki yetkililerin para veya şantaj karşılığında yetkilerini kötüye kullanması toplumsal refahın yükselişini engelleyen ciddi sorunlardır. Mahkemeler ve polis dahil olmak üzere her şey satılığa çıktığında güven uçar gider, krediler çarçur olur, işletmeler batar (Harari, 2016: 347; De Mesquita, & Smith, 2010). Vatandaşların büyük çoğunluğunun eğitimsiz, vizyonsuz, sosyal yardıma muhtaç olması ve açlık sınırının altında yaşaması baskıcı rejimlerin ömrünü uzatmaktadır (Lipset, 1959). Dünya genelinde ve ülkelerinde baş veren olayları gözlemleme ve analiz etme olanaklarından mahrum olan kitlelerin oy kullanarak ülkelerinin kaderini belirlemeleri pek mümkün değildir (Williamson, 2021). Daha kötü durumda olan ülkelerde düzenin seçimle değişme ihtimali olmadığı için oy kullanma işlevi anlamsızdır ve seçim tiyatroları devlet için ekstra masraftan başka bir anlam ifade etmez (Bedford, 2017).

15 ve 16. yüzyıllarda modern devlet anlayışının ortaya çıkmasıyla bölgesel güç olmak isteyen devletlerin çevrelerindeki ülkeleri sömürmek amacıyla baskı altında tutmak istemesi dünya genelinde ciddi bir sorun olarak devam edegelmiştir. ABD diğer dünya devletlerinden farklı olarak bencil davranışlarını daha üst boyuta taşıyarak yalnız kendine komşu olan ülkelerin tabii kaynaklarına göz dikmekle kalmamış Ortadoğu ülkelerine kadar uzanmıştır (Beck, 2020). ABD'nin dünyayı kutuplaştırması, çatıştırması, silah sanayisinden gelen gelirlerini artırması, dünya ülkelerinin her türlü kaynaklarını sömürmeye çalışması sonucunda milyonlarca insan vahşice katledilmiştir. Gelinen aşamada da ABD petrol madenleri kadar değerli olan veri sömürgeciliğiyle de tanınmaktadır (Couldry & Mejias, 2023: 791). Sergilenen bencil ve saldırgan politikalar sonucunda gelişmemiş ülkelerde totaliter yöneticiler yönettikleri halkın temel haklarını bile kısıtlamak pahasına koltuklarını korumak

derdine düşmüştür. Dünya düzeni üzerinde oynanan bin türlü ABD merkezli oyuna karşın gelişmişlik düzeyine göre birbirine benzeyen hükümetler koltuklarını korumak için birbiriyle dayanışma içinde olmak zorunda kalmıştır.

Dış faktörlere bakıldığında dünya genelinde bölgesel güç olma iddiasında olan devletlerin saldırgan ve bencil tavırlarından dolay dünya toplumunun büyük bir kısmı esaret altında yaşamaktadır (MacQueen, 2014). ABD ve Rusya gibi devletlerin güç ve çıkar çatışması nedeniyle Ukrayna'da (Fekete, 2023) ve Gazze'de binlerce insanın ölümüne neden olması son zamanlarda yaşanan örneklerdir. Ukrayna'da savaş suçu işlediğinden dolayı Uluslararası Ceza Mahkemesiyle (UCM) iş birliği yaparak Rusya Devlet Başkanı Vladimir Putin için tutuklama emri çıkaran Biden Yönetimi (CRS Report, 2023) İsrail'in Gazze'de yaptığı katliama her türlü destek vermektedir. Bu tür tezatlar ABD ve Rusya gibi sömürgeci ülkelerin gerçek yüzünü ortaya koymaktadır.

Rusya'nın ve ABD'nin izlediği bencil politikalar Sovyetler Birliği'ne (SB) dahil olan ülkelerin yöneticilerini adeta konsey üyeleri gibi birlikte hareket etmeye mecbur bırakmıştır. Aksi taktirde Rusya'nın çevresindeki ülkeleri Ukrayna gibi savaş alanına çevirme tehdidi bölgedeki insanların köle gibi yaşamasına neden olmaktadır (Mardan, 2020). Rusya'nın esareti altındaki bölgelerde yaşayan insanlar yönetimi altında bulundukları hükümetlerin Rusya tarafından desteklendiğini bildikleri için yolsuzluklara ve başarısız politikalara karşı çıkamazlar. 2022'nin ilk günlerinde Kazakistan'da akaryakıt zammına karşı meydana gelen ayaklanmaları kontrol altına almakta zorlanan hükümetin Kolektif Güvenlik Antlaşması Örgütünden (KGAÖ) yardım istemesi üzerine Rus askerleri krize müdahale ederek (Özsoy, 2022:120) bölgede etkili olduklarına dair gövde gösterisi yapmıştı. SB dağıldıktan sonra Vladimir Putin Rusya'nın çevresindeki ülkelerin yöneticileriyle gizli ve açık çıkar ilişkisi kurarak bölgesel güç olma iddiasıyla egemenliğini sürdürmektedir. Putin'in kurduğu birliklerden KGAÖ, Bağımsız Devletler Topluluğu (BDT), GUAM Demokrasi ve Ekonomik Kalkınma Örgütü örnek olarak gösterilebilir. Bunun yanı sıra sözde bağımsız olan çevresindeki ülkelerde Rus kültürünün izleri eğitim alanı ilk sırada olmakla yaşamın her alanında kendisini göstermektedir.

Uluslararası konsorsiyum oluşturulmadığı taktirde dünyadaki kaynakların büyük bir kısmının savunma sanayisinin geliştirilmesi için harcanacağı

kaçınılmazdır. Kuzey Kore Lideri Kim Jong-Un'un roket adam olarak anılması, Rusya devlet başkanı Vladimir Putin'in ABD'ni ve AB ülkelerini sürekli nükleer silah kullanmakla tehdit etmesi dünya genelinde güvenlikle ilgili kaygıların düzeyine işaret etmektedir. Dünyayı yönetmek iddiasında olan liderlerin kirli ilişkileri ve politikaları dijital dünyada da siber güvenlik, siber saldırılar ve veri sömürgeciliği alanında devam etmektedir. Başka bir ifadeyle dijital dünyadaki sorunlar "dünya liderlerinin" gerçek dünyada yarattığı sorunların devamıdır.

Dijital vatandaşlık alanı, eğitim, psikoloji, siyaset bilimi, kamu yönetimi, sosyoloji, hukuk, medya ve teknoloji gibi farklı disiplin alanlarına dayanan çok yönlü bir yapıdır (Chen vd., 2021). Aşağıdaki paragraflarda kamu yönetimi ve sosyoloji disiplinlerinde dijital vatandaşlığın önemine, etkilerine ve sonuçlarına değinilmiştir.

Dijital gelişmelerin etkisiyle kamu yönetimi disiplininde vatandaşların yönetim sürecine katılım pratikleri doğal olarak dijital ortama evrilmiştir. Hem devleti hem de vatandaşları konu edinen bir alan olarak kamu yönetimi, dijital çağ olarak adlandırılan bu dönemde önemli bir alanı oluşturmaktadır (Oğuzhan, 2023: 115). Geleneksel kamu yönetimi anlayışında vatandaşların yönetim sürecine dahil olmadığı ve hem hizmet üretimi hem de hizmet sunumu konusunda merkezi kurumlar baskın konumda bulunmuştur. Yeni düzende kamu hizmetlerinin dijital ortamda sunulmaya başlamasıyla birlikte çok merkezliliğin, katılımcılığın, sorgulayan aktif vatandaşlığın ön planda olduğu bir düşünce yapısı ortaya çıkmıştır (Bincan, 2022: 108). 20. yüzyılda egemen paradigma olan Weberyan bürokrasi anlayışına bir tepki olarak ortaya çıkan yeni kamu yönetimi anlayışına karşın geleneksel kamu yönetimi anlayışı yöneticilere geniş yetkiler veren, kaynak israfına yol açan, verimsiz, hantal bir yapı olarak tanımlamıştır (Oğuzhan, 2023: 119-120).

İnternetin yükselişiyle birlikte sivil, sosyal ve politik hayata katılma fırsatları da artmıştır (Pangrazio & Sefton-Green, 2021: 18). Dijital olanakların yaygınlaşmasıyla vatandaşların da sürece dahil olma fırsatı yaranmıştır. Kamu yönetimi sürecine dahil olma durumu kişiye göre ve dünya ülkelerinin gelişmişlik düzeyine göre farklılık göstermektedir. Kamu yönetimi disiplininde dijital vatandaşlıkla ilgili en temel odak noktalarından biri vatandaşın yönetim sürecine katılımı olan yönetişimin sosyal medya aracılığıyla sağlanması ve vatandaşın sosyal medya üzerinden yönetim ve hukuk politikalarına etkileridir (Nohutçu & Yörükoğlu,

2023). Nesnelerin interneti, sensör tabanlı akıllı sistemler, büyük veri, akıllı şehir, akıllı yönetim sistemleri gibi Endüstri 4.0'ın çıktıları olan gelişmelerin kamu yönetimi alanına girmesi ve bir dönüşüm başlatmasıyla halen de bir gelişim içerisindedir (Oğuzhan, 2023: 120-121; Göçoğlu, 2020). Alan yazında pek çok çalışmanın dijital iletişim uygulamalarının kamu yönetiminde şeffaflığı ve vatandaş katılımını güçlendirdiğine vurgu yaptığı dikkat çekmektedir (Boztepe Taşkıran, 2019). Bu konuyla alakalı tartışmalara "Dijital Dünyada Aktif Katılımın Önemi", "Dijital Haklara ve Sorumluluklara Odaklanmak", "Dijital Dünyada Tüketici Farkındalığının Önemi" ve "E-yönetişim Ekosisteminin Önemi" adlı başlıkların altında detaylı yer verilmiştir. Bunun yanı sıra güvenlik ve veri gizliliği sorunları, dijital eşitsizlik ve altyapı sorunlarıyla ilgili tartışmalara da yer verilmiştir.

Günlük yaşamın önemli gereksinimlerinden olan dijital araç ve ortamlar toplumsal ilişkileri etkilemeye ve dönüştürmeye devam etmektedir. Dijital ortamda gerçekleştirilen yaşam pratiklerini toplumsal etkileriyle birlikte analiz etmek için dijital sosyoloji devreye girmektedir. Özellikle yeni dönemin tanımlanması, dijital dönüşüm çağındaki gelişmelerin tartışılması süreci sosyal bilimler ve sosyoloji açısından yeni, hızlı ve yoğun tartışmaların da kapısını aralamaktadır (Zinderen, 2021). Sosyoloji, ortaya çıkan gelişmeleri anlamayı hedefleyerek toplum hayatı hakkında yeni fikirler üretir, eski fikirleri eleştirir ve güncelliğini sorgulayarak toplum yaşamına yeni bakış açıları kazandırır (Bahar, 2009). Dijital sosyoloji toplumsal değişimi dijital bir perspektiften ele alarak toplumsal yapıyı analiz etmektedir (Dede, 2024: 357). Davranış ve ahlak anlayışının dönüştüğü, bilim ve kültürde çığır açıcı yeniliklerin yaşandığı bir çağda (Kara & Atasoy, 2019) dijital dünyada vatandaşlığın sosyolojik açıdan incelenmesi oldukça dikkat çekicidir.

Sosyolojik açıdan dijital vatandaşlık, onun tanımından farklı olarak dijital araçları kullanma becerisine, sosyal sorunları anlamaya ve dijital bir toplumda aktif vatandaşların önemli bir özelliği olan sosyal adaletsizliğe karşı mücadele için bir seferberlik ağı oluşturmayı içeren çevrimiçi siyasi katılım sürecidir (Pholmat, 2023). Teknolojik gelişmelere paralel olarak "yeni" toplumsal ilişkiler ve onların çıktıları tartışılmaya devam etmektedir. Bu bağlamda dijital sosyoloji, dijital eşitsizlik, dijital gözetim, sanal kimlik, dijital aktivizm, kuşaklar, ebeveynlik, dijital sağlık, dijital diplomasi ve eğitimde dijitalleşme gibi toplumu şekillendiren konuların etkilerini ve

sonuçlarını anlamak önem taşımaktadır (Zinderen, 2021). Bununla birlikte sosyoekonomik koşullar, sosyokültürel altyapı, bölgesel farklılıklar, eğitim düzeyi, eğitime erişim imkânı, yaş ve cinsiyet gibi faktörler de dijital dünyada vatandaşlık bağlamında sosyolojik açıdan dikkatle incelenen konulardır.

### 1.4. Dijital Dünya Düzeninde Vatandaşların Hakları ve Sorumlulukları

Vatandaşların hak ve sorumluluklarıyla ilgili gereken düzeyde bilgi ve beceri elde etmeleri ve sorumluluklarını kolay bir şekilde yerine getirebilmeleri için internet bağlantılı teknolojik cihazlara sahip olmaları temel hak ve zorunluluktur. Farklı disiplinler ile ilişkilendirme bağlamında incelenen dijital dünyada vatandaşlığın eğitim, psikoloji, siyaset bilimi, ekonomi, sosyoloji, hukuk, medya ve teknoloji gibi çeşitli disiplin alanlarına dayanan çok yönlü bir yapı olduğu bilinmektedir. Bu yapının toplumsal yaşamın her alanındaki etkisi şüphesiz ki, bu alana zenginlik ve karmaşıklık katmaktadır. Toplumun yaşam biçimini şekillendiren dijital hakları ve sorumlulukları öğrenmek, yararlanmak ve aynı zamanda dijital ortamdaki zararlı davranışlara karşı vatandaşların kendilerini savunabilmeleri de temel zorunluluk olarak nitelendirilmektedir. AB'nin dijital dönüşüm yaklaşımına yön veren etik ilkelerin oluşturulmasının yanı sıra veri koruma, cinsiyet eşitliği, mahremiyet hakkı, ayrımcılık yapmama, tüketicinin korunması, teknoloji ağı tarafsızlığı, güvenilirlik ve kapsayıcılık gibi temel haklara ve ilkelere tam uyumun sağlanması gerekmektedir.

Dijital vatandaşlık, eleştirel incelemeye hazır, oldukça tartışmalı bir kavramdır (McCosker vd., 2016: 1). Mossberger ve arkadaşları (2007) dijital dünyada vatandaşlığı çevrimiçi olarak topluma katılma yeteneği olarak tanımlamıştır. Dijital dünyada vatandaşların haklarını bilmeleri ve sorumluluklarını yerine getirmeleri için internet bağlantılı modern teknolojilere ve onları kullanma yeteneğine sahip olmaları temel bir gereksinimdir. Dijital vatandaşlık haklarının sağlanması ve korunması çevrimiçi platformların daha fazla hesap verebilirliğine ve dijital ekonominin güçlendirilmesine yönelik bir girişim olarak değerlendirilebilir. Dijital yetenek bazen dijital okuryazarlık, medya okuryazarlığı veya bilgi okuryazarlığı olarak anılır, genellikle bilgiyi çevrimiçi olarak bulmak, değerlendirmek, oluşturmak, düzenlemek ve iletmek için modern teknolojileri kullanma yeterliliği olarak anlaşılır (Taylor, 2019). Ribble (2015) göre dijital

vatandaşlığın dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, dijital etik, dijital hukuk, dijital haklar ve sorumluluklar, dijital sağlık ve dijital güvenlik olmak üzere dokuz bileşeni bulunmaktadır. Bu bileşenler telif haklarından siber saldırılara kadar dijital vatandaşlığın farklı boyutlarını anlamak için temel bir çerçeve sunmaktadır. Bu haklardan vatandaşların yararlanabilmesi için erişim hakkının tanınması ve ayrımcılığın yasaklanması, ifade ve bilgi edinme özgürlüğünün sağlanması, toplanma, örgütlenme ve katılım özgürlüğünün sağlanması, gizlilik haklarının ve verilerin korunması, eğitim ve okuryazarlık becerilerinin geliştirilmesi için uygun şartların sağlanması, çocuk ve gençlerin korunması, insan hakları ihlallerine karşı etkili çözümlerin bulunması ve uygulanması seçim dönemlerinde ön koşul olarak ileri sürülmelidir.

Zaman ilerledikçe teknolojik gelişmelere paralel olarak yaklaşımların da sürekli güncellenmesi gerekmektedir. Custers (2022) mevcut dijital hakların uzantıları olan ve literatürde az tartışılan aşağıdaki haklara da dikkat çekmiştir;

- Çevrimdışı olma hakkı, internet erişim hakkı.
- Bilmeme hakkı, fikrini değiştirme hakkı.
- Temiz dijital bir sayfayla yeniden başlama hakkı.
- Verilerin son kullanma tarihi hakkı.
- Verilerin değerini bilme hakkı.
- Temiz bir dijital ortam hakkı.
- Güvenli bir dijital ortam hakkı.

Çevrimdışı olma hakkı vatandaşların çalıştıkları şirketler tarafından çalışma saatleri dışında telefon veya e-posta gibi iletişim araçlarıyla rahatsız edilmemesi anlamına gelmektedir.

İnternet erişimi hakkı vatandaşların dijital ortamda hizmet veya ürün satın almak için, bilgi edinmek için, haberleşmek için dezavantajlı durumda kalmaması konusunda önemli olduğu bilinmektedir. Diğer hakların dengelenmesi, rekabet koşullarının iyileştirilmesi, ifade özgürlüğünün sağlanması ve dijital uçurumun kapatılmasına katkı sağlaması amacıyla BM internet erişiminin temel bir hak olması gerektiğini öne sürmüştür.

Bilmeme hakkı yaklaşımına göre özelikle veri analiziyle tahmine dayalı bilgilerin bilinmemesi insanların refahını olumlu etkilemektedir. Bilme hakkı veri koruma yönetmeliğine uygun olarak veri sahiplerinin kendileri hakkında hangi bilgilerin toplandığı ve işlendiği, hangi amaçlarla kullanıldığı konusunda bilgilendirme yükümlülüğünü gerektiriyor. Ama tam tersi olan bilmeme hakkı veri sahiplerinin kendileriyle ilgili belirli bilgileri bilmemek veya dikkate almak konusunda tıp alanı hariç çok az tartışılmaktadır. Tahmine dayalı analitiklere göre insanların kategorize edilmesi, kredi alımının engellenmesi ve hayatlarını etkileyebilecek kısıtlamaların bilinmemesi daha faydalı olacaktır.

Fikrini değiştirme hakkı vatandaşların fikirlerini değiştirdikten sonra algoritmalar aracılığıyla eskiden sahip olduğu düşüncelere uygun kategorideki içeriklere maruz kalması anlamına gelmektedir.

Temiz dijital bir sayfayla yeniden başlama hakkı belirli koşullar yerine getirildiği takdirde eski bilgilerin tamamen silinmesi ve yeniden temiz bir sayfayla dijital topluma katıla bilmek anlamına gelmektedir. Temiz dijital bir sayfayla yeniden başlama hakkı AB Genel Veri Koruma Yönetmeliği'nin 17. maddesinde silme hakkına ve literatürde tartışılan unutulma hakkına benzemektedir.

Verilerin son kullanma tarihi hakkı yaklaşımına göre hizmet koşullarına yönelik sözleşmelere ve çerezlere sonsuza kadar onay vermek yerine, bir ayla beş yıl arasında isteğe bağlı bir süre seçilmelidir. Kullanıcılar dijital ortamda hizmet koşullarına yönelik sözleşmeleri ve çerezleri kabul ederken belirli bir süre için onay verme seçeneğine sahip olmalıdırlar. Bu süre dolduktan sonra, doğrulukları yeniden teyit edilmediği sürece verilerin hatalı olduğu varsayılmalıdır.

Verilerin değerini bilme hakkı büyük teknoloji şirketlerinin platformlarını ve lisanssız ürünlerini kullanan kullanıcılar karşılığında paylaştıkları kişisel verilerinin maddi değerinin ne kadar olduğunu bilmeleri gerektiği anlamına gelmektedir. Görünürde herhangi bir abonelik ücreti alınmasa da aslında kullanıcılar verileriyle ödeme yapmaktadırlar. Ürün ve hizmetler sunan şirketler karşılığında topladıkları verileri diğer verilerle de birleştirerek istedikleri gibi büyük miktarda maddi servete dönüştürmektedir. Özelikle büyük teknoloji şirketleri kullanıcılara ait kişisel verilerin ifşa edilmesi, üçüncü taraflarla paylaşılması, verilerin çeşitli amaçlarla işlenmesi gibi işlemlerden ne kadar kâr elde ettiklerini kullanıcılarla da paylaşmalıdırlar.

Temiz bir ortam hakkı gezegende olduğu gibi dijital dünyada da kullanıcıların temiz bir ortama olan ihtiyacının karşılanması anlamına gelmektedir. Çevrimiçi ortamda olduğu gibi çevrimdışı ortamda da dijital kirliliğin etkileri vatandaşların yaşamını olumsuz etkilemektedir. Örneğin blockchain teknolojisinin kullanımı çok büyük miktarda enerji tüketiyor, atık pillerin kritik bileşeni olan lityum ve diğer nadir toprak elementleri sağlık sorunlarına ve çevre kirliliğine neden olmaktadır. Bilgi çağının kirlilik sorununu çözmek hükümetlerle birlikte birçok ülkede bireysel bir çaba gerektiren konu haline gelmiştir. Her geçen gün dijital egzozun çevrimiçi ekosistemde ciddi kirliliğe neden olduğu apaçık ortadadır. Topluma hiçbir yararı olmayan anlamsız paylaşımlar, istenmeyen reklamlar gibi içerikler dijital ekosistemi ciddi anlamda kirletmektedir.

Güvenli bir dijital ortam hakkı özelikle yeterli bilgi ve beceriye sahip olmayan kullanıcıların kötü amaçlı saldırılardan korunması için gereken kapsamlı siber güvenlik önlemlerinin alınmasıyla da örtüşmektedir. Gerçek dünyada hükümetlerin ve özel aktörlerin emniyet ve güvenlik için çaba gösterdiği gibi dijital dünyada da kullanıcıların güvenliğini sağlamak için çaba göstermeleri gerekmektedir. Çünkü kullanıcıların dijital dünyada bireysel güvenlik tedbirleri alması bilgi, beceri, zaman ve maliyet açısından çok zahmetli bir süreçtir. Bu hakların yanı sıra dijital eşitliğin sağlanması, fikri mülkiyet haklarının korunması, adalete ve çözüme erişim gibi haklar da sağlanmalı ve korunmalıdır.

15 Aralık 2022 tarihinde AB Konseyi, Avrupa Parlamentosu ve Komisyon Başkanları tarafından imzalanan dijital haklar ve ilkelere ilişkin bildiride insanı merkeze alan kapsayıcı, adil, güvenli ve sürdürülebilir bir dijital dönüşümün yol haritası hazırlanmıştır (Cocito & De Hert, 2023). Dijital haklar ve ilkelere ilişkin bildiri AB'nin dijital çağda korumak istediği haklar ve değerler olarak görülse de aslında bu bildiri dijital anayasacılığın manifestosudur. Dijital anayasacılık, temel anayasal değerleri dijital ekosistemin ihtiyaçlarına uyarlayan çağdaş anayasacılığın teorik olarak evrimidir. Asırlık değerler, yeni toplumsal gerçekliğe hitap edebilecek normatif ilkelere dönüştürülüyor (Celeste, 2021). Çünkü küresel sorunların çözümü ulusal devletlerin tekelinden çıkarak çokuluslu özel kuruluşlar gibi çok sayıda ulusötesi aktörle iş birliği biçimlerini gerektirmektedir. Çevrimdışı erişilebilen haklar dijital vatandaşlık hakları kapsamında çevrimiçi olarak da erişilebilir olmalıdır.

Dijital dünyada demokratik yaşam ve temel kamu hizmetlerine kolay erişim büyük ölçüde bağlantılı dijital teknolojilere bağlıdır. Bu nedenle gelişmiş ülkelerde güncel teknolojilerin, dijital alanla sınırlı olmayan kullanımının vatandaşların günlük yaşamlarını ve refahını olumlu etkilemesi için planlar hazırlanmakta ve uygulanmaktadır (Avrupa Birliği'nin resmî gazetesi, 2022). Avrupa Birliği (AB) ülkeleri için Avrupa Komisyonu tarafından hazırlanan dijital hedeflere göre veri ekonomisi, sürdürülebilirlik ve siber güvenlik alanlarındaki teknik, ekonomik ve toplumsal gelişmelere yönelik ilerlemelerin takip edilmesi, tüm sürecin performansının puanlanması ve raporlanması talep edilmektedir. Eğer AB üye devletleri insan merkezli dijital ekosistemin yaratılmasında başarılı olursa muhtemelen diğer ülkeler tarafından da örnek alınacaklardır.

BM'nin birçok farklı sektördeki sürdürülebilir kalkınma hedeflerine göre iklim değişikliği çerçeve sözleşmesi kapsamında kabul edilen Avrupa Yeşil Anlaşması ve Paris Anlaşması'nın hedeflerini kolaylaştıran dijital dönüşümün teşvik edilmesi için yatırım yapılması kritik öneme sahiptir.

Gelişmekte olan ülkelerin dijital hedeflerinde dijital becerilerin geliştirilmesi, dijital altyapıların sağlanması, işletmelerin dijitalleşmesi ve kamu hizmetlerinin dijitalleştirilmesi adeta dijital bir pusula niteliğindedir. Bu dört önemli girişimin etkili olabilmesi için herkesin varlığını, önemini bilmesi ve üzerine düşen sorumluluğu üstlenmesi gerekmektedir. Sürdürülebilir yaşam döngülerini desteklemek, iklim değişikliğiyle mücadele etmek ve çevreyi koruma konusundaki politikaların etkisini en üst düzeye çıkarmak için yapay zekâ, 5G, 6G, blockchain, bulut ve uç bilgi işlem ve nesnelerin interneti, yapay zekâ gibi dijital teknolojilerin kullanımına büyük ihtiyaç vardır.

15 Aralık 2022 tarihinde AB Konseyi, Avrupa Parlamentosu ve Avrupa Komisyonu Başkanları tarafından imzalanan bildiri insanların dijital dönüşümün merkezine koyulması, dayanışma ve katılımın önemi, seçim özgürlüğünün sağlanması, dijital kamusal alana katılım için gereken şartların sağlanması, emniyet, güvenlik ve yetkilendirmenin önemi ve sürdürülebilirlikle ilgili konulara yer verilerek önemli bir referans çerçevesi oluşturulmuştur. Bu ilkelerin sadece AB ülkeleri için değil dünya genelinde dijital dönüşüm için kabullenilmesi ve uygulanması gerekmektedir. Bu amaçla özellikle gelişmekte olan ülkelerde dijital

uçurumu azaltmak için uluslararası iş birliği, uygulama ve takip mekanizması oluşturmak etkili bir çözüm olabilir. 2030 Dijital Pusulasında kullanılan dijital teknolojilerin ve hizmetlerin geçerli yasal çerçeveye uygun olması, insan odaklı, güvenli ve açık dijital ortam yasalarına uygun olması, aynı zamanda insanların mahremiyet ve veri koruma hakları, ifade özgürlüğü, çocuk hakları ve tüketici hakları gibi haklarını kullanmalarına da olanak sağlanması gerektiği belirtilmiştir (European Commission, 2021). Çünkü teknolojik gelişmeler küresel ekonomilerin odak noktası olarak bir nirengi taşıdır ve dijitalleşme süreci teknolojik gelişmelerle birlikte gelişen bir olgudur (Kalaycı, 2023: 43). İnsanların dijital haklarından yararlanabilmeleri için öncelikle uygun maliyetli, güvenli ve yüksek kaliteli bağlantıya erişebilmeleri, temel dijital becerileri öğrenebilmeleri ve modern teknolojik cihazları alabilme imkânına sahip olmaları temel gereksinimlerdir. Dijital toplumun ve ekonominin demokratik işleyişi, hukukun üstünlüğüne, etkili hukuk yollarına ve kanunların uygulanmasına tam saygı gösterilerek daha da güçlendirilmelidir (European Commission, 2021).

### 1.4.1. İnteraktifliğin Artırılması Amacıyla Erişim ve Katılım

Erişim ve katılımın yaygınlaşması bilinçli kullanıcılar için çok büyük avantajlar sağlamaktadır. Avantajlar açısından incelendiğinde durum her alanda olduğu gibi ülkelerin gelişmişlik düzeyine ve vatandaşların bilgi düzeyine göre değişmektedir (UNCTAD, 2021). Erişim ve katılım dijital dünyada vatandaşların dijital ortamda bilgiye erişme, içerik oluşturma ve o içeriği yayma haklarına sahip olmaları anlamına gelmektedir. Dijital dünyaya erişmek, dijital dünyada vatandaş olmanın ilk adımıdır. Bu alan, dijital bölünmenin farklı biçimlerinin üstesinden gelmek, dijital alanları azınlıklara ve farklı görüşlere açmak için gerekli bir dizi yetkinlikleri içerir. Dijital eşitsizlik, sadece internet erişimine ve araçlara sahip olmakla ilgili sorunları değil, aynı zamanda onların nasıl kullanılacağını bilmek açısından sorunları da içeren geniş kapsamlı bir kavramdır.

Dijital eşitsizliği, dijital dünyaya erişimleri, becerileri, kullanımları ve dijital dünyaya katılımlarından elde edilen sonuçlarla ilgili olarak farklı sosyoekonomik geçmişlere sahip bireyler arasındaki sistematik farklılıklar olarak tanımlıyoruz (Buchi & Hargittai, 2022). İnternet bağlantılı teknolojilerin daha yeni yaygınlaşmaya

başladığı yıllardan itibaren kişisel başarı ve ilerlemenin lokomotifi olarak görülmesi günümüze kadar geçerliliğini korumaktadır.

Kültürel sermaye sosyal statü ve güç verir, dolayısıyla yüksek statülü istihdama doğru sosyal seçilim için harekete geçirilebilecek sosyal yatkınlıkları ve ayırt edici kültürel zevki içerir (Isopahkala-Bouret vd., 2023: 53). Dijital dünya düzeninde maddi sermayenin yanında kültürel ve sosyal sermaye birikimi de büyük önem arz etmektedir. Bireyler kültürel veya sosyal sermayelerini artırabilmeleri için de dijital dünyaya erişim ve katılım sağlamaya ihtiyaç duyarlar. Kültürel sermaye, seçim yapma ve karar verme sürecine rehberlik eden bilgi birikimi ve becerilerdir (Bourdieu, 1996). Dolayısıyla kültürel sermaye birikimine sahip olmayan bireylerin yeni dünya düzeninde varlığını sürdürebilmesi kolay değildir. Her zaman kültürel çevrenin sunduğu fırsatlardan kültürel sermayesi en yüksek olanlar yararlanır ve böylece şehirlilerle taşralılar arasındaki uçurum, yüksek eğitim seviyelerinde daha belirgin hale gelmektedir. Bu noktada dijital çağın olanaklarına erişebilmekle kültürel sermayeyi artırmak adına aradaki boşluğu azaltmak mümkündür. Sosyal, ekonomik, kişisel, politik ve kültürel sermayeler kullanıcıları eşit olmayan başlangıç noktalarına yerleştirir, kullanıcıların dijital sermayesinin oluşmasına yardımcı olur ve bu yeni sermayeyle etkileşime girerek dijital kaynakları sosyal kaynaklara dönüştürür (Ragnedda, 2018).

En riskli pozisyonların gerektirdiği kişisel risk, toplumsal ilişkileri belirleyen değişik sermaye biçimleri arttıkça hem öznel hem de nesnel olarak azalır. Gelecekteki fırsatları değerlendirmek için önemli olan sermaye her türlü biçimde arttıkça kâr şansı da artar. Bu bağlamda ekonomik sermayenin yanı sıra kültürel sermaye yeni ürünler yaratmak ve satmak için gerekli olan sembolik şiddetle o geleceği oluşturmaya yardımcı olur, sosyal sermaye gayri resmi olarak örgütlenmiş sektörlerde bireyin yarışa girmesini ve içinde kalmasını sağlar (Bourdieu,1996). Bireylerin toplum içinde edinmiş olduğu her türlü beceri, yetenek, bilgi, eğitim ve kariyer gibi durumların genel adı olarak tanımlanan kültürel sermaye eşit erişime açık olmadığından dolayı ayrıcalıklı kazançlar veya avantajlar sağlamaktadır. Özetle kültürel sermaye toplumsal eşitsizlikleri tetikleyen bir faktördür.

Özelikle ekonomik sorunlar nedeniyle erişim ve katılım imkânlarına sahip olmayan vatandaşlar dijital dünyadaki olanaklardan mahrum kalama riskiyle karşı

karşıyadırlar (UNCTAD, 2021). Gelişmekte olan ülkelerde sivil toplum kuruluşları veya eğitim bakanlığı tarafından en azından öğrenciler için adil erişim ve katılım imkânları yaratılmalıdır. Örneğin İngiltere'de Adil Erişim Ofisi tarafından 2006'dan 2018'e kadar belirlenen gereklilikler ve düzenlemeler uyarınca bu tür girişimleri yürütmüştür (Moores vd., 2023). 1 Nisan 2018'den itibaren Öğrenci Ofisi'ne devredilmiştir. Gelişmemiş ülkelerde de yönetimlerin üstlenmediği önemli faaliyetler sivil toplum kuruluşları tarafından üstelenerek yürütülebilir. Belirli bir güce ulaştıktan sonra hükümetlerden de destek alınabilir veya demokratik yollarla hükümetlerin bu tür girişimleri desteklemesi talep edilebilir.

Bilgi ve İletişim Teknolojisi (BİT) günümüz toplumunda günlük yaşamın ayrılmaz bir parçası olduğu için, onsuz dijital olmayan demokratik vatandaşlık bile zorlaştı (Richardson & Milovidov, 2022: 18). İnternete erişim temel insan haklarından biri olduğu için, hükümetlerin, işletmelerin ve sivil toplum kuruluşlarının dijital altyapıyı ve erişilebilirliği iyileştirmek için çalışmaya devam etmesi ve vatandaşların dijital ortama dâhil olabilmesi için gerekli şartların sağlanması gerekiyor. Aynı zamanda kapsayıcılık, dijital dünyada vatandaşların uyması gereken yol gösterici bir ilke ve önemli bir değerdir. Dijital dünyada kapsayıcı bir yaklaşıma sahip olmak, azınlıklara, bizden farklı olanlara veya farklı düşünen herkese karşı belirli bir "duyarlılığa" sahip olmak demektir.

Development Initiatives'in verilerine göre 2022 yılında dünya nüfusunun yaklaşık yarısının (4,2 milyar insan) günde 6,85 doların altında gelirle yoksulluk sınırının altında yaşadığı bilinmektedir (Christensen, 2023: 8). Yoksulluk sınırının altında yaşayan insanların internet bağlantılı teknolojilere erişim sağlaya bilmeyeceği aşikardır. Gelişmemiş ülkelerdeki sefaletin, huzursuzluğun asıl nedeni olan antidemokratik rejimleri değiştirmek için mutlaka AB gibi uluslarüstü yapıların devreye girmesi gerekiyor. AB gibi uluslarüstü bir örgütün tüm dünya toplumunun yaşam standartlarını iyileştirmek için kriterler belirleyip ve belirlediği kriterleri uygulamaya çalışması günümüz dünyasının en zorunlu ihtiyaçlarından biridir. AB zaman zaman aday ülkelerde de yaşam standartlarını iyileştirmek için hibeler sunsa da hedeflenen projenin uygulanması ve takibi konusunda başarılı olamamıştır. Örneğin ayrılan hibelerin despot rejimlerin kontrolünde çalışan şirketlere aktarılması hiçbir pozitif sonuç doğurmamıştır. Çünkü gelişmemiş ülkelerdeki sorunları yaratan,

sorunların yaranmasına neden olan veya göz yuman zaten bu tür despot rejimlerdir. Ama ne yazık ki, AB'ye üye olabilmek için standartların yerine getirilmesi kargaşadan beslenen, toplumu kutuplaştırmak için uğraşan ve kurdukları diktatoryal düzenle gelir dengesizliğini had safhaya çıkaran hükümetlerin insafına terk edilmiştir. Maddi kaynakları elinde bulunduran antidemokratik hükümetler toplumun tüm bileşenlerini istedikleri gibi yönetmektedirler. Tüm kararları zaten halka sormadan istedikleri gibi kabul edip uygulamaya koydukları için, devletin kolluk güçlerini de halkı susturmak için sopa niyetine kullanmaktadırlar. Söz konusu düzende toplumun devlet zırhına bürünmüş ve her türlü imkânlara sahip olan hükümetlere karşı kendisini savuna bilmesi imkânsızdır.

### 1.4.2. Dijital Dünyada Öğrenme ve Yaratıcılık

Öğrenme ve yaratıcılık yaşam boyunca dijital ortamlarda öğrenmeye yönelik farklı bağlamlarda, farklı araçlarla, farklı yaratıcılık biçimleri geliştirme kapasitesidir. Gelecekte, öğrenme bilimleri araştırmasına dayalı yeni okullarda, yaratıcılık tüm müfredata yayılacaktır (Sawyer, 2010: 176). İnternet bağlantılı teknolojiler, her yaştan vatandaşa hayatlarının her aşamasında öğrenmeleri için geniş fırsatlar sunmaktadır. Bu fırsatlardan yararlanmak için yaşam boyu öğrenmeye yönelik temel yeterliliklere sahip olmak gerekiyor. Dijital olarak yetkin olmak doğuştan gelen bir şey olmadığından, eğitim insanların öğrenme süreçlerini geliştirmek için gerekli olan dijital yeterliklerini şekillendirmede çok önemli bir rol oynamaktadır (Hatlevik vd., 2015: 228). Dijital yetenek ve dijital açıklık dijital yaratıcılığı önemli ölçüde artırır (Nguyen vd., 2023). Sürekli olarak yeni cihazların, yeni uygulamaların ve yeni aktivitelerin geliştirilmesinden dolayı dijital yeterlilik sürekli yenilenmeli ve kavramsal olarak akışkan dijital yeterlilik olarak algılanmalıdır.

COVID-19 krizi, eğitimin sürekliliğini sağlamak için televizyon kursları, çevrimiçi öğrenme yönetim sistemleri ve sanal simülasyon eğitimi dahil olmak üzere dünya çapında eğitim sisteminde dijital öğretme ve öğrenme yöntemlerinin yaygın olarak kullanılmasına yol açmıştır (Yanli & Danni, 2021: 165). Bilgilendirici web siteleri, e-posta alışverişleri, sohbet odaları, video konferanslar, web seminerleri ve

kitlesel çevrimiçi açık kurslar aracılığıyla uzaktan eğitim, vatandaşların sosyal ve fiziksel engelleri aşmasını ve seslerini daha kolay duyurmasını sağlamaktadır.

Dijital dünyada en büyük zorluklardan biri, eğlence ve kültürün yalnızca bir tıklamayla veya bir ekranı kaydırmayla 7/24 erişilebilir olduğu bir dünyada yaratıcılığı teşvik etmektir. En yaygın kabul gören tanımına göre yaratıcılık, yeni veya orijinal ve faydalı veya etkili fikir ve ürünlerin üretilmesidir (Mumford vd., 2002; Runco & Jaeger, 2012; Weisberg, 2020). Yaratıcılık, estetik ve ekonomik faydalarının yanı sıra insanların sorunlarla yüzleşmek için yenilikçi çözümler geliştirmelerine de yardımcı olur ve refahlarını artırır (Conner vd., 2018; Tan vd., 2019). Yaratıcılık ve anlamlı sanatsal anlatım, her zaman öğrenme ve sosyal ilerlemenin önemli itici güçleri olmuştur. Ancak günümüzde dünya nüfusunun yüzde 99'nun tüketici, yalnızca yüzde 1'nin yaratıcı olduğu tahmin edilmektedir (Ledford, 2022). Bilgi kirliliğinin aşırı derecede attığı dijital çağda artık öğrenme ve yaratıcılık tekniklerini öğreten derslerin müfredata entegre edilmesi de büyük önem arz etmektedir.

Bilgi ve iletişim teknolojilerinin (BİT) etkin kullanımı, giderek dijitalleşen dünyaya başarılı katılım için bir zorunluluktur (Fraillon vd., 2020). Öğrenme ve yaratıcılık, farklı bağlamlarda, farklı araçlarla farklı yaratıcılık biçimlerini hem geliştirmek hem de ifade etmek için vatandaşların yaşamları boyunca dijital ortamlarda öğrenmeye yönelik istek ve tutumlarını ifade eder (Richardson & Milovidov, 2022: 13). Öğrenme ve yaratıcılık BİT ile bütünleştirildiğinde, toplumun her kesiminden insanlar daha derin bir anlayışa ulaşır, içerik bilgisini kullanmayı öğrenmekle daha esnek düşünme yeteneği kazanır, eleştirel düşünme ve yaratıcılık becerileri doğal olarak gelişecektir.

### 1.4.3. Bilgi ve Medya Okuryazarlığı

Buckman Labs'ın eski CEO'su Robert Buckman'ın (2004) ifadesiyle bilgi her zaman yaşamak için güç, uyum sağlamak için güç, zor bir çevrede başarılı olmak için güç anlamına gelmiştir. Bilgi günümüzde dünyada egemen olmak için kullanılan bir araçtır. Refah düzeyi yüksek olan ülkelerin bilgi ürettiğini ve amaçları doğrultusunda kullandıklarını, vatandaşların refah düzeyi aşağı seviyelerde olan ülkelerde ise tam tersine bilgi üretilmediği ve kullanılmadığı görülmektedir. Bu

açıdan bakıldığında bilgi her alanda olduğu gibi ekonomik alanda da temel belirleyicilerden biri olarak karşımıza çıkmaktadır.

Genel olarak okuryazarlık, süreklilik olarak belirli bir sosyokültürel bağlamda okuma ve yazma yeteneği, temel aritmetik yetkinlik ve ayrıca belirli bir alanda yeterlilik olarak tanımlanır. Okuryazarlık ideolojik yetenek ve beceri değildir, ideolojik ve politik olarak yüklüdür. Sosyal kontrol veya düzenleme aracı olarak ve aynı zamanda özgürlük mücadelesinde ilerici bir silah olarak kullanılabilir.

Bilgi okuryazarlığı terimi ilk defa Zurkowski (1974) tarafından "Bilgi Hizmeti Ortamı, İlişkiler ve Öncelikler" raporunda kullanılmıştır. Bu raporda bilgi okuryazarlığı, bireyin sorunları çözmek için bilgi kaynaklarını kullanabilme kapasitesi olarak öne sürülmüştür. Bruce Christine'ye göre (2003: 1) bilgi okuryazarlığı, bilgi toplumunda okuryazarlık kavramının doğal bir uzantısıdır ve bilgi okuryazarlığı eğitimi, bugünün bilgi toplumunu yarının öğrenen toplumuna dönüştürmek için gerekli katalizördür. Öte yandan, "bilgisayar okuryazarlığı", "medya okuryazarlığı", "ağ okuryazarlığı", "dijital okuryazarlık", "veri okuryazarlığı", "mobil okuryazarlık" ve diğer kavramlar bilgi okuryazarlığı kavramının uzantıları olarak ortaya çıkmış ve yaygın olarak tartışılmıştır (Bruce, 2000; Pinto vd., 2010; Pinto vd., 2019).

Amerikan Kütüphane Derneği Bilgi Okuryazarlığı Başkanlık Komitesinin nihai raporunda (American Library Association, 1989) bilgi okuryazarı olan kişiler aşağıdaki gibi tanımlanmıştır:

> *"Nihayetinde bilgi okuryazarı insanlar, öğrenmeyi öğrenmiş kişilerdir. Nasıl öğreneceklerini biliyorlar çünkü bilginin nasıl organize edildiğini ve bilgiyi nasıl bulacaklarını ve bilgiyi başkalarının onlardan öğrenebileceği şekilde nasıl kullanacaklarını biliyorlar. Herhangi bir görev veya karar için gerekli bilgiyi her zaman bulabildikleri için yaşam boyu öğrenmeye hazır insanlardır".*

Ekonomik Kalkınma ve İş Birliği Örgütü'nün tanımına göre, BİT okuryazarlığı, bireylerin bilgiye erişmek, yönetmek, bütünleştirmek ve değerlendirmek, yeni bilgiler oluşturmak, topluma etkin bir şekilde katılmak ve başkalarıyla iletişim kurmak için dijital teknoloji ve iletişim araçlarını uygun şekilde kullanmaya yönelik ilgi, tutum ve yeteneğidir (Lennon vd., 2003: 8). Son yıllarda bilgi okuryazarlığı araştırmaları ve bursları, öğrenme sürecinde bilgi ile etkileşime odaklanmıştır. Her bir birey yaşam boyu sahip olduğu kapasiteye uygun olarak

bilgiyi başara bildiği düzeyde kullanır. Geleneksel olarak okullarda, bireylerin "nasıl öğreneceklerini öğrendikleri" bir ortam sağlansa da tam olarak yeterli değildir. Potansiyel bilgi kaynaklarına erişme, bilgilerin doğruluk ve uygunluk açısından değerlendirilmesi, bilgileri organize etme ve son olarak, süreçteki en değerli adım bilgiyi uygulamayı içerir (Doyle, 1994). En büyük motivasyon sadece bilgiyi bulmak değil, bilgiyi doğru zamanda ve doğru yerde kullanmaktır. Bu bağlamda ekonomik faaliyet hala değerli bir sonuç olsa da öne çıkan faydalardan eşitlik ve sosyal adaletin sağlanması da ilk sıralarda yer almaktadır.

Okuma kültürü sırasıyla dikkatle dinleme alışkanlığı, okuma ve yazma becerisi, evrensel olarak eleştirel okuma, algılama ve analiz etme becerisi gerektiren döngüsel bir süreçtir (Sever, 2007). Dijital teknolojilerin yaygınlaştığı çağda bireylerin toplumdaki yaşamın karmaşıklığı nedeniyle dijital okuryazarlık alanındaki becerilerini sürekli geliştirmeleri ve geniş bir bilgi yelpazesine güvenli erişim sağlamaları çok önemlidir. Daha önceki araştırmalar, okuryazarlığı daha yüksek olanların cinsel davranışlar, alkol tüketimi ve siyasi katılım konusunda daha sağlıklı kararlar verme eğiliminde olduğunu göstermektedir (Austin vd., 2015).

Vatandaşların dijital ortamlarda yayımlanan bilgileri sürekli eleştirel yaklaşımla okumaları, paylaşmak istedikleri bilgilerin doğru olup olmadığını güvenli kaynaklardan teyit edebilecek kadar bilgi ve becerilere sahip olmaları önem arz etmektedir. Başka bir ifadeyle "dijital okuryazarlık" sorgulamaya dayalı becerilerin geliştirilmesini ve etkileşim kurma yeteneğini sürekli geliştirmeyi zorunlu hale getirmiştir. Dijital okuryazarlık, dijital medya, bilgisayar ve BİT'in kullanımını çevreleyen geniş bir yetkinlikler kümesini ifade eder (Leaning, 2019: 4). Dijital teknoloji, insanların çeşitli günlük aktiviteleri gerçekleştirmesini kolaylaştırmakla (Madakam vd., 2019) birlikte vatandaşların söz konusu kolaylıklardan faydalanabilmeleri için gereken yeteneklerini de geliştirmelerini zorunlu kılmaktadır. Canlı ve gelişen enformasyon sisteminde, bilgi okuryazarlığı ve mobil öğrenmenin yakınsamasında, yeni başlayan bir alt alan olan "Mobil Bilgi Okuryazarlığı" ortaya çıkmıştır (Pinto vd., 2020). Bu alan her şeyden önce bilgi okuryazarlığı ve mobil öğrenmenin sürekli gelişimine dayanmaktadır. Dijital okuryazarlık ile ilgili yapılan araştırmaların evrenine bakıldığı zaman çoğunlukla öğrenci odaklı çalışmaların yapıldığı görülmektedir. Fakat dijital çağda dijital okuryazarlığın öğrenci olmayan

bireyler için de kritik bir yetkinlik olduğu yaygın olarak kabul edilmektedir (List vd., 2020).

Medya okuryazarlığı, vatandaşların erişebildiği medya mesajlarının (grafik, imgeler, ses, video, yazılı metin vb..) içeriğini eleştirel yaklaşımla okuma ve anlama, bu içerikleri doğru analiz edebilme, değerlendirebilme ve gerektiğinde yeni içerikler üretmek gibi beceri temelli kültürel bir süreci kapsar (Karaduman, 2019). Bu yetkinlikler dijital dünyada vatandaşlık için ön koşul veya kilit beceriler olarak kabul edilmektedir. Dijital içeriklerin bilişsel, duygusal, siyasal ve sosyal yönlerini anlama, eleştirel olarak değerlendirme ve çeşitli bağlamlarda iletişim kurma yeteneği gerektirir (Karaoğlu, 2022). Küreselleşme eğilimlerine rağmen, hâlâ ulusal devlet ve onun siyasi kurumları, gazetecilerin çalıştığı koşulları şekillendiren baskın bir faktördür (Rao, 2019). Mevcut koşullarda hükümetler ve politikacılar toplumun çıkarına değil, yalnızca kendi özel çıkarlarına veya muhtemelen seçim kampanyalarını finanse eden lobilerin çıkarlarına göre hareket ederse, yalnızca kendi güçlerini sürdürmeyi amaçlarlar (Celot, 2012).

Bilgi okuryazarlığı ve medya okuryazarlığı terimlerinin tanımlarında benzerlik olduğu görülse de bazı önemli farklılıklar da vardır. Genel olarak bilgi okuryazarlığı geleneği, bilgi malzemelerinin belirlenmesi, konumu, değerlendirilmesi ve kullanımını vurgularken, medya okuryazarlığı geleneği ise, medya içeriklerinin anlaşılmasını, eleştirilmesini ve oluşturulmasını vurgular. Mecazi anlamda, medya okuryazarlığının medyayı dünyaya bakmak ve kendini ifade etmek için bir mercek veya pencere olarak görüldüğünü, bilgi okuryazarlığının ise bilgiyi dünya üzerinde hareket etmek için bir araç olarak görüldüğünü söyleyebiliriz (Livingstone vd., 2008: 107). Medya okuryazarlığının amacı, insanların günlük yaşamlarında karşılaştıkları birçok medya mesajının biçimine ilişkin farkındalıklarını artırarak, yaşadıkları toplumların bilinçli ve aktif vatandaşları haline gelmelerini sağlamaktır (EAVI). Yapılan araştırma sonuçları dijital okuryazarlık becerisinin dijital dünyada vatandaşlık sorumluluğunu yerine getirmek için önemli bir kaynak olduğunu ortaya koymaktadır. Toplumun finansal açıdan en dezavantajlı üyelerinin de erişebileceği temel medya ve bilgi okuryazarlığı eğitimini içeren eğitim 3.0 politikalarına ihtiyaç olduğu genel kabul görmüş bir konudur. Eğitim 3.0, eğitim teorisyenleri tarafından

teknolojiyi öğrenmeye entegre etmenin çeşitli yollarını tanımlamak için kullanılan bir şemsiye terimdir.

Medya ve bilgi okuryazarı olmak, eğitim yoluyla ve çevremizle sürekli bir değiş tokuş yoluyla geliştirilmesi gereken bir kabiliyet gerektirir. Örneğin, şu veya bu medyayı basitçe "kullanabilmenin" ya da bir şey hakkında basitçe "bilgilendirilmenin" ötesine geçmek esas teşkil etmektedir. Dijital dünyada vatandaşlar topluluğuna anlamlı ve etkili katılımın temeli olarak eleştirel düşünmeye dayanan bir tutum sürdürmek zorundadır (Richardson & Milovidov, 2022: 13). Gelişmiş ülkelerde araştırmacılar ve uygulayıcılar bilgi teknolojisinin etkisine odaklanarak araştırma alanının genişliğini ve derinliğini artırmaya çalışmakta ve dijital okuryazarlık alanında kapsamlı, sürdürülebilir ve etkili gelişmeyi teşvik etmek için verilere dayalı yenilikçi değerlendirme yöntemleri geliştirmeye devam ederken, BM tarafından hazırlanan raporlarda İnsani Gelişme Endeksi (İGE) üst sıralarda olan ülkelerde dahi dijital okuryazarlık orta okullarda seçmeli ders olarak bile öğretilmemektedir (UNDP). Dijital okuryazarlık alanında da ülkeler arasında büyük bir fırsat eşitsizliğinin varlığı sorun olarak devam etmektedir.

### 1.4.4. Dijital Dünyada Etik

Etik Antik Yunan'da, ideal bir toplumun barış ve düzeni korumak veya elde etmek için "iyi" veya "olumlu" olarak kabul edilen davranışlar dizisine atıfta bulunurdu. Yunanca "yaşam tarzı" anlamına gelen "ethos" sözcüğünden türetilmiş etik, insanların toplumdaki davranışlarıyla ilgilenen bir felsefe dalıdır. İnsanların, diğer insanlara ve doğaya karşı davranış tarzı etik kurallar çerçevesinde nitelendirilmiştir. Etik kurallara uymak, doğru davranışlar sergilemek ve Baden Powell'ın ifadesiyle, bir yeri bulduğumuzdan daha iyi bırakmak için elimizden geleni yapmaktır. Her toplumun kültürüne uygun olarak etik kriterler karar alma sürecinde ahlaki yargıya rehberlik eder. Temel olarak etik, ahlaki açıdan neyin doğru, neyin yanlış, neyin adil veya neyin adaletsiz olduğunu temsil eder. Etik yalnızca neyin doğru ya da yanlış olduğuna ilişkin insan kararlarını etkilemekle kalmaz, aynı zamanda gelecekteki eylemlerin temelini oluşturur (Gwagwa vd., 2022: 4). Etik kurallara uygun davranışlar sergileyen insanlar diğer insanlarla birlikte yaşarken empati kurarak ahlaki değerlere uygun kararları kendi başına verebilmektedirler.

Zygmunt Bauman (2011: 33) etiği, tek ahlak kuralı, her ahlaklı kişinin itaat etmek zorunda olduğu, birbiriyle tutarlı ilkelerden oluşan tek buyruklar grubu olarak tanımlamıştır. Sosyal kontrolu sağlamak amacıyla toplum insanlardan etik kurallara uymayı talep eder, uyulmadığı taktirde ayıplayarak veya dışlayarak toplumsal baskı uygular.

Son yıllarda dijital dünyada sosyal etkileşim yaygın olarak arttığına göre dijital dünyanın dinamikleri ile gerçek dünyanın dinamikleri farklılaşmıştır. Gelişen dijital dünya için yeni dijital etik kavramlarının tartışılması, farklı çözümler sunabilecek etik uygulamaların evrensel boyuta ulaşma imkânının sorgulanması gerekmektedir. Dijital dünyada etik konusu internet etiği, dijital etik, robot etiği, yapay zekâ etiği, siber etik gibi farklı başlıklar altında tartışılmaktadır. Dijital dünyada etik, internet bağlantılı teknolojiler aracılığıyla etkileşimde bulunurken doğru ve ahlaki olan davranışlar bütününe atıfta bulunan bir ifadedir. Dijital etik, dijital araçların ve internetin kullanımında etik ilkelerin dikkate alınmasının gerekliliğini ifade eden kavramdır (Öteleş & Merey, 2022: 1306). Dijital etik, dijital araç ve gereçlerin amacına uygun olarak kullanılması, dijital ortamlarda uyulması gereken kurallar, kişi hak ve özgürlüklerinin korunması ve telif haklarının korunması anlamını taşımaktadır.

Uyulması gereken etik ilkeler zarar vermemek duygusuyla hareket etmeyi, başkalarının emeğine, mahremiyetine, düşüncelerine ve duygularına saygılı olmayı gerektirir. Yapay zekâ, nesnelerin interneti, robotlar, biyometri teknolojisi, sanal gerçeklik, "deepfake", sanal evren (metaverse) ve farklı etkileşim imkânları sunan sosyal medya ve dijital platformlar yaygınlaştıkça dijital dünyada etik sorunlar da artmaya devam etmektedir. Gerçek dünyada olduğu gibi dijital dünyada da hukuka aykırı olan davranışlar aynı zamanda etik dışı davranışlar olarak nitelendirilmektedir. Gerçek dünyada olduğu gibi dijital dünyada da tüm paydaşlar çoğu zaman etik dışı davranışlar sergileyerek insan haklarını ihlal etmektedirler. Başka bir ifadeyle dijital dünyada insanlar etik kuralları ihlal ettiği gibi hükümetler ve teknoloji şirketleri de ihlal eder ve caydırıcı yaptırımlardan kaçınırlar. Dijital dünyada etik yalnızca "netiket" bilmekle ilgili değildir, aynı zamanda çevrimiçi ortamları daha olumlu, üretken ve anlamlı yerler haline getirmek için özen göstermek ve aktif olarak hareket etmekle ilgilidir. Bu aynı zamanda empati kurmayı da gerektirir. Etikle empati

arasında pozitif bir ilişki bulunmaktadır. Etik ve empati, başkalarının duygularını ve bakış açılarını tanıma ve anlama yeteneği gibi becerilere dayalı olarak çevrimiçi etik davranış biçimleri ve başkalarıyla etkileşim ile ilgilidir (Richardson, & Milovidov, 2022: 13).

Yaşamın her alanını etkileyen dijitalleşme sürecinde etik kodların belirlenmesi amacıyla dijital iletişim, siber uzay ve yapay zekâ sistemleri en çok üzerinde durulması gereken konular olmalıdır (Aslan, 2022). Çünkü etik dışı davranışların en çok bu üç alanda gerçekleştiği çok tartışılan bir sorundur. Etik kodların belirlenmesi ve uygulanması için gereken regülasyonların yeterli olmayacağını göz önünde bulundurmanın yanı sıra caydırıcı yasal düzenlemeler tekrar gözden geçirilmeli veya güncellenmelidir. Etik kuralların yaygın olarak bilinmesi ve uygulanması için farkındalık yaratmak, yasal düzenlemelerin uygulanması için de bağımsız bir yargı sistemi olmalıdır. Yapay zekâ teknolojilerinin gizlilik ihlalleri, "deepfake", algoritmik ayrımcılık, güvenlik ve güvenilirlik sorunları, şeffaflık ve diğer istenmeyen etik sorunlara neden olması tartışılması gereken sorunlardır. Dünya çapında yapay zekâ etiği ile ilgili beş farklı dilde 200 belgenin analizi sonucunda belirlenen 11 etik ilkeden (beş tanesi) şeffaflık (%86), adalet (%81), zarar vermeme (%71), sorumluluk (%71) ve mahremiyet (%56) en çok tekrarlanan ilkeler olmuştur (Corrêa vd., 2023).

Bilgi ve iletişim teknolojileri (BİT), insanların birbirleriyle etkileşime girme, yaşama ve çalışma şekillerini önemli ölçüde değiştirmiştir (Gebhardt vd., 2019: 1). Dijital enformasyon sistemleri, yoğun bir sosyal değişim için fırsatlar yaratarak gücün, paranın, hakların ve sorumluluğun mevcut dağılımını etkilemektedir (Laudon & Laudon, 2012:124). Etik sorunların siyasi, ekonomik ve kültürel olmak üzere üç temel nedeni vardır. Dijital dünyada etik ihlallerinin önüne geçmek amacıyla maddi cezaların artırılması caydırıcı bir çözüm olabilir (Katyal, 2001). Bu cezalar dijital araçları ve ortamı amacı dışında kullanan hükümetler için ayrı, kullanıcıların haklarını ihlal eden teknoloji şirketleri için ayrı, saldırganlar (hackerler) için ayrı, sıradan bireyler için ayrı ayrı düzenlenerek uygulanmalıdır.

Gracia Calandín'ya göre (2018), eğitim sisteminde etik-yurttaşlık boyutu göz ardı edilse, toplumun demokratik yaşamı toplumsal moral bozukluğunun kötülüğünden ciddi bir şekilde etkilenecektir. Mbinjama-Gamatham ve Olivier

(2020: 109) dijital etik konusunun geliştirilmesi için eğitim ve mevzuatın önemine dikkat çekmiştir; birincisi her yerde, tüm kültürlerde, özellikle çocuklarda ve gençlerde etik veya ahlaki sorumluluk duygusu aşılamayı hedefleyen eğitim sistemi geliştirmek, ikincisi ise etik çerçevede suç teşkil eden davranışları belirleyen mevzuat geliştirmektir. Öğrencilerin dijital etik bilincine sahip olabilmesi için ilkokuldan itibaren eğitimin çeşitli kademelerinde dijital etik dersi verilebilir, yetişkinler için ise farkındalık yaratmak amacıyla seminerler ve çeşitli etkinlikler düzenlenebilir (Öteleş & Merey, 2022).

Hem dijital hem de gerçek dünyada etik davranış kurallarının tüm boyutları bütüncül bir şekilde öğretilmek için okul müfredatına entegre edilmeli ve uygulanması için de gereken şartlar sağlanmalıdır. Sadece yasaları formüle etmek değil, aynı zamanda insanları, eğitim sürecinin ilk yıllarından itibaren evrensel etik ve ahlaki kurallarla eğitmek, gelecekte kararlarını verirken derinlemesine düşünmeyi teşvik etmek için süreci aile eğitimi ile tamamlamak önemlidir (Taylor 1992). Hans Jonas (1995) insan sorumluluğu ilkesine ilişkin açıklamalarında yerine getirilmesi gereken sorumluluklara atıfta bulunarak ahlaki değerler ve ilkeler çerçevesinde kişisel beklentilerin, eylemlerin ve kararların sonuçlarının her zaman tahmin edilmesi ve öngörülmesi gerektiğini belirtmiştir. Adil bir düzende yaşamak amacıyla hem gerçek hem de dijital dünyada şeffaflık, adalet, zarar vermeme, kişisel verilerin kötüye kullanılmaması, sorumluluk almak ve mahremiyetin korunması gibi ilkeler karar verme süreçlerinde temel kılavuz olarak kullanılmalıdır. BT'ler her boyutuyla insana saygıyı garanti eden etik bir çerçevede geliştirilip kullanıldıkları sürece büyük sosyal ve kişisel faydalar sağlayabilirler (Novella-García & Cloquell-Lozano, 2021: 3532).

### 1.4.5. Dijital Dünyada Empatinin Gücü

Empati kurmak diğer insanların deneyimlerini, duygularını ve bakış açılarını anlama ve hissetme kapasitesidir (Collins vd., 2023; Wondra & Ellsworth, 2015; Davis, 1996). Bu yetenek, özellikle ekranın diğer tarafında bizim gibi insanlar olduğunu düşünerek şiddet içeren veya zararlı davranışlardan kaçınmak ve olumlu etkileşimleri teşvik etmek için çok önemlidir. Literatürde sosyal varoluşun temel kategorilerinden biri olan empati kavramının çok sayıda tanımı mevcuttur. Alfred

Adler empatiyi "başkasının gözüyle görmek, başkasının kulağıyla dinlemek, başkasının kalbiyle hissetmek" olarak tanımlamıştır (Ansbacher & Ansbacher, 1956). Hem fiziksel dünyada hem de dijital dünyada empatik davranışlar insanların farklı kültürlerin temsilcileriyle etkileşimi sürecinde başkalarına yardım etmek ve başkaları için adalet arzu etmesi olarak nitelendirilir (Hoffman, 2001). Empati kurma anlayışı genişledikçe başkalarına karşı yapılan adaletsizlikler, sınıflar arası çatışmalar, ön yargılı davranışlar, zorbalıklar ve egoist tavırlar azalma eğilimi göstermektedir. Empati, pozitif çevrimiçi etkileşim ve dijital dünyanın sunduğu olanaklardan faydalanabilmek için temel bir gerekliliktir. İnsanlar okuryazarlık, deneyim, seyahat ve sosyalleşme yoluyla başkalarına dair anlayışlarını genişlettiklerinde, başkalarının kendilerine davranmasını istedikleri gibi başkalarına davranmak isteyebilirler (Segal vd., 2017).

Anlık mesajlaşmanın yaygınlaşması göz önüne alındığında, internet bağlantılı cihazlar üzerinden başarılı iletişim kurabilmek için, sempatik iletişim kurma yeteneğinin geliştirilmesi kadar mesajlaşma araçlarının arkasındaki kişiyi anlama becerisi de gereklidir. Sempati duygusu empatik ilginin şefkat duygusuyla birlikte başka bir kişinin acısının değerlendirilmesi, acı çeken kişinin iyiliğiyle ilgili endişe duyulması ve yardım etme isteği anlamına gelmektedir.

Bir dizi bilişsel ve pratik beceriye bağlı olan katılım bilgisi, eleştirel düşünme, sözlü ve yazılı ifade becerilerini tam olarak kavramak için ne zaman ve nasıl konuşulacağını bilme, empati ve kültürel anlayışı birleştirir (Richardson & Milovidov, 2022: 18). İnsanların duygu ve düşüncelerinin anlaşılmasında fizyolojik tepkilerin ve mimiklerin önemli olduğu gerçeğine göre empati deneyimi yüz yüze iletişim ile dijital iletişim arasında farklılık göstermektedir. Hawk ve arkadaşlarının (2011) araştırmalarına göre yüz ifadesi, ses tonu ve beden dili gibi ipuçları insanlarda empatik durumların oluşmasına neden olmaktadır. Dijital dünyada iletişim kurarken, fizyolojik tepkilerin ve mimiklerin eksikliği azaltılmış empati perspektifini tartışmaya açık hale getirmiştir. Azaltılmış empati perspektifi, yüz yüze iletişimde ses tonu, jestler ve beden dili gibi önemli belirtilerin dijital iletişimde görünmediği konusuna odaklanmaktadır (Preece, 2000). Sözsüz ipuçları, insanlar arasında empati ve bağlantı kurmak için kritik öneme sahip olduğuna göre dijital dünyada iletişim kurarken genellikle anlayış duygusunun azalması empati kurmak açısından bir sorun

olarak görülmektedir. Empati, stereotipleri yıkmaya, önyargıları ortadan kaldırmaya ve kapsayıcılığı teşvik ederek dijital dünyada birlik duygusunu güçlendirmeye yardımcı olmaktadır. Dijital dünyada duyguları ifade etmek amacıyla emojiler kullanılsa da etkileşimlerin çoğu, yüz yüze konuşmalar zamanı doğal olarak ortaya çıkan incelik ve derinlikten yoksundur. Yanlış anlamaların ve yanlış yorumlamaların kolay olduğu dijital dünyadaki etkileşimlerde nazik bir söz, sanal bir kucaklaşma veya içten bir yorum moral yükseltebilir, duyguları hissettirebilir ve insanlara yalnız olmadıklarını hatırlatabilir.

Dijital olanakların önemli avantalardan bir de fiziksel uzaklıktan dolayı yüz yüze iletişim kurma şansı olmayan insanların birbirini dijital ortamda tanıma veya etkileşimde bulunma imkânı bulabilmesidir. Dijital dünyada nefret söylemi ve çevrimiçi taciz gibi zararlı davranışları azaltmak için empati, derin anlayışı, anlamlı ilişkileri ve daha şefkatli bir dijital topluluğu teşvik edebilir. Sonuç olarak empati çatışmaları azaltarak, olumlu değişimi teşvik ederek dijital dünyayı daha şefkatli ve kapsayıcı bir alana dönüştürebilir (Khan, 25 Mayıs 2023). Dijital dünyadaki etkileşim bazı durumlarda yanlış anlaşılmaya müsait olsa da yenilikçi teknolojiler sayesinde yanlış anlaşılmanın etkilerini azaltmak mümkündür. Örneğin holografik mesajlar dijital iletişimde duygusal empati fırsatı yaratabilir. Dijital dünyada empati kurabilmek için karşı tarafın mesajları farklı bakış açılarıyla değerlendirilmeli, aktif bir şekilde dinlenilmeli veya izlenmelidir, mesajların cevaplandırılması için acele edilmemeli ve gerektiğinde açıklama istenmelidir.

Aynı zamanda kültürlerin çeşitliliğini anlamak için sosyal ve tarihsel araştırmalar ve analizler yaparak empatik becerileri daha geniş ölçekte geliştirmek mümkündür. Eğer empatik davranışlar okuryazarlık, deneyim, sanal oyun, seyahat ve sosyalleşme gibi etkili stratejilerle öğretilirse toplumda huzur ve barışın sağlanması için faydalı olacaktır. Uygulama yoluyla insanlar zamanla empatilerini de geliştirebilirler (Zaki, 2017). Gerçek dünyada ve dijital dünyada empatinin temel ilkeleri aynı olduğundan hem medya okuryazarlığı eğitimi hem de öz yansıtma faaliyetleri teorik olarak insanları dijital dünyadaki etkileşimlerini sorgulamaya ve incelemeye teşvik edebilir. Bu kendi kendini inceleme süreci, potansiyel olarak çevrimiçi farkındalığın artmasını sağlayabilir ve dijital empatinin artmasını teşvik edebilir (Terry & Cain, 2016).

Dijital dünyada empati türlerini (Batson, 2009) öğrenmek, öğretmek, incelemek ve savunmak, insanların sosyal, duygusal ve bilişsel becerilerini geliştirmek için yardımcı olabilir. Empati demokratik süreçlere, küresel anlayışın artmasına ve toplumsal değişime katılım konusunda daha fazla yetkinliğe katkıda bulunabilir (Segal vd., 2017). Yapılan araştırmalara göre empati duygusunun geliştirilmesine odaklanmış eğitimsel müdahalelerin başarılı olduğu bulgulanmıştır (Friesem, 2016; Stepien & Baernstein, 2006).

### 1.4.6. Dijital Dünyada Sağlık ve Esenlik

Esenlik, sağlık ve iyi oluşun tüm yönlerini kapsayan bir terim olup, bunun yanında hem vücut hem de zihin için olumlu bir iyilik duygusunu ifade etmektedir (Erkmen 2013: 26). Esenlik, kişinin mutlu ve keyifli hissetmesinin yanı sıra yaşam sürecinde sahip olduğu potansiyelin ve planlarının farkında olmasıdır. Adams ve arkadaşları (1997) esenliği kişinin fiziksel, manevi, psikolojik, sosyal, duygusal ve entelektüel boyutlarının tutarlı ve dengeli gelişimini içeren bir yaşam biçimi olarak tanımlamıştır. Sağlık ve esenliğin toplumla, kültürle ve doğal dünyayla bağlantılı olduğu düşünülmektedir. Sağlık ve esenlik konusu, dijital teknolojilerin uygun ve zamanında kullanımından güvenilmez veya çarpıtılmış bilgilerin etkisine, aileler içindeki ve vatandaşlar arasındaki günlük yaşamdaki etkileşimleri değiştirme biçimine kadar geniş kapsamlı konuları ve zorlukları kapsamaktadır (Richardson & Milovidov, 2022).

Dünya Sağlık Örgütü (DSÖ) esenliği fiziksel, zihinsel ve sosyal açıdan tam bir iyilik hali olarak tanımlamaktadır. Bu tanım yaşam tarzını, zihinsel ve ruhsal refahı, aileyi, çevreyi, sosyal ortamları, uykuyu ve fiziksel sağlığı kapsayan çok boyutlu ve bütünsel bir sağlığı kapsamaktadır. Avrupa Konseyi'nin dijital vatandaşlık yeterlilik çerçevesi birçok açıdan Maslow'un ihtiyaçlar hiyerarşisiyle uyumludur (McLeod, 2007). Sağlık ve esenlik, dijital dünyada vatandaşların hem çevrimiçi hem de gerçek alanlarda yaşadığı gerçeğiyle ilgilidir. Bu nedenle dijital yeterliliğin temel becerileri tek başına yeterli değildir. Bireyler ayrıca sağlık ve esenlikle ilgili konularda kendilerini daha bilinçli kılan bir dizi tutum, beceri, değer ve bilgiye ihtiyaç duyarlar (Richardson & Milovidov, 2022: 13). Bu alan, kişinin dijital olarak zengin bir dünyada sağlık durumunu etkileyebilecek sorunlar ve

fırsatlar hakkındaki farkındalığını kapsamaktadır. Dijital dönüşüm sağlık ve esenliğe yönelik hem fırsatlar hem de riskler yaratmaktadır. Dijital teknolojiler insan faaliyetlerini daha verimli hale getirerek yaşamı kolaylaştırmanın yanı sıra dezenformasyon, nefret söylemi, yalan haber, kontrol edilemeyen yapay zekâ ve siber tehditler kullanıcıların ruh sağlığını olumsuz etkilemektedir. Örneğin siyasi, ideolojik, ulusal ya da kişisel sebeplerden dolayı karşı tarafa zarar vermek amacıyla dijital saldırılar yapılabilmektedir (Küçükbezirci, 2023: 5).

Sağlık ve esenlik, kişinin dinleme, gözlemleme, empati kurma ve iş birliği yapma kapasitesine bağlıdır. Bu yeterlilikler, problem çözme ve çatışma çözümü gibi daha yüksek bilişsel becerilerin yapı taşlarıdır (Richardson & Milovidov, 2022: 68). DSÖ'nün tanımına göre ruh sağlığı, bireyin kendi yeteneklerinin farkına vardığı, yaşamın günlük stresleriyle baş edebildiği, verimli ve yararlı çalışabildiği, yaşadığı topluma katkıda bulunabildiği bir iyilik halidir. Sağlık ve esenlik, bireyler tarafından günlük yaşamlarında, çevrimiçi ve çevrimdışı topluluklarla etkileşimlerinde teknolojinin dengeli ve uygun kullanımına odaklanır. Tam esenlik oluşturan fiziksel, zihinsel, duygusal, ruhsal, çevresel, sosyal, finansal ve mesleki esenlik biçimleri genellikle birbiriyle yakından bağlantılıdır. Bu anlamda, dijital dünyada sağlık ve esenlik sağlıklı yaşam alanını etkileyebilecek sorunların ve fırsatların farkında olmak ilk sıralarda yer almaktadır. İnternet bağımlılığıyla mücadele etmek, doğru ergonomik duruşu korumak, mobil cihaz kullanmanın riskleri ile ilgili bilgi edinmek sadece birkaç örnektir. DSÖ'nün tanımına göre esenlik, ekonomik ve çevresel koşullar tarafından günlük yaşam için belirlenen bir kaynaktır. Ekonomik İş birliği ve Kalkınma Örgütü'nün raporuna göre gelir ve zenginlik, işler ve kazançlar, barınma, sağlık durumu, eğitim ve beceriler, iş ve yaşam dengesi, sivil katılım ve yönetişim, sosyal bağlantılar, çevresel kalite, kişisel güvenlik ve öznel refah gibi faktörler insanların sağlık ve esenliğini etkilemektedir (OECD Publishing, 2019). Bu faktörler göz önünde bulundurularak dijital dünyada insanların refah düzeyini artırmayı amaçlayan projelere yatırım yapılmalıdır.

Kavramsal olarak esenlik dünya genelinde psikoloji, sosyoloji, felsefe, ekonomi gibi birçok farklı alt disiplinlerde araştırmalara konu olmaktadır. Esenlik, başka bir ifadeyle iyi olma hali yaşam kalitesini artırmanın yanı sıra pek çok olumlu sonuca yol açmaktadır. Esenliğin önemsenmediği toplumlarda yaşam kaygısından

dolayı tükenmişlik, düşük verimlilik, yaşam tatminsizliği, iş tatminsizliği, fiziksel sağlığın bozulması, örgütsel bağların zayıflaması, düşük performans ve nefret duygusunun artması gibi olumsuz sonuçların ortaya çıkması kaçınılmazdır (Rahimnia vd., 2013; Clercq vd., 2021; Pyc vd., 2017; Kanten, vd., 2022). Tüm dünya nüfusu için her türlü güvenliğin sağlanması, insanların esenlik içinde yaşaması ve isteklerini gerçekleştirmesi için küresel bir dayanışma içinde olmak faydalı olacağı gibi, her bir bireyin hem gerçek hem de sanal dünyada hak ihlallerine karşı çıkması etik bir sorumluluk olarak kabul edilmelidir (Özdemir ve Sinan, 2022).

Küreselleşmenin de etkisiyle dünya ülkelerinde toplumun kutuplaştırıldığı bir dünyada hükümetler iktidarlarını korumak için hem yönettiklerine hem de bazı devletlere karşı devletin kaynaklarını ve enerjilerini harcadıkları için insanların özgürlüğünü, güvenliğini ve esenliğini sağlamak konusunda son derece başarısızdırlar. Özellikle gelişmemiş ülkelerde hükümetler fahiş vergi oranlarıyla, yolsuzluklarla, ekonomik sorunlarla insanların esenliğini olumsuz etkilemektedirler. Gelişmiş ülkelerde politika yapıcılar ve anayasal düzenleri insani iyi olma halinin gelişmesine hizmet ederken, gelişmemiş ülkelerde ise durum tersine cereyan etmektedir. Fiziksel sınırların kalktığı dijital dünyada, küresel sağlıklı yaşam ekonomisi 2022 yılında 5,6 trilyon dolara ulaşmıştır (GWI, 2023).

Toplumların esenlik düzeyinin yükseltilmesi için bilim insanları araştırmalar yapmalı ve politikacılar da esenlik için gereken koşulların sağlanması ve korunması için çalışmalıdırlar. Olumlu zihinsel sağlığı destekleyecek bir ekosistem oluşturmak, fırsatlar, riskler ve dayanıklılık konusunda farkındalık yaratmak, dijital teknolojileri daha etkili, bilinçli ve sağlıklı bir şekilde kullanmayı öğrenmek olumlu sonuçlara yol açacaktır. Dijital teknolojilerin olumlu ve kapsayıcı kullanımı bireysel refah üzerinde önemli etkilere sahip olabilir. Refah eksikliğinden kaynaklanan olumsuz veya sınırlı bir dünya görüşüne sahip vatandaşların topluma aktif olarak katkıda bulunma olasılıkları daha düşüktür (Richardson & Milovidov, 2022: 68). Hükümetler ve büyük teknoloji şirketleri belirli müdahalelerle dijital teknolojileri kendi çıkarlarını korumak için kullanabildiği gibi toplumun da dijital teknolojilerden faydalanması için imkân sağlayabilirler. Fakat yetersiz politikalar veya uygun düzenlemelerin eksikliği, insanları dijital dönüşümün tüm faydalarından yararlanmasından çok risklerine maruz bırakmaktadır.

### 1.4.7. Dijital Dünyada E-mevcudiyet, Dijital Kimlik ve Benlik Sunumu

Bilgi çağında e-mevcudiyet dijital dünyada vatandaşların, olumlu, uyumlu ve tutarlı çevrimiçi etkileşimler kurmak için kişisel ve kişilerarası niteliklerinin gelişimini içerir. Kullanıcılar, hesaplarına ekledikleri bilgiler, profil fotoğrafları, katıldıkları gruplar, var olan veya yeni edindikleri arkadaşlarla kurdukları etkileşim ağı ve bunları yönetme biçimleriyle kimliklerini aktarmaktadırlar (Sertaç, 2021: 1408). Dijital ortamda sosyal alanlar aracılığıyla başkalarıyla olumlu iletişim kurmak ve iş birliği yapmak, kendi e-kimliğini yönetmek bu alana ait yetkinlikler arasındadır. Gerçek toplulukların, ilişkilerin, duyguların hatta aşkların yerini sanalları alırken, benlik sunumu, kimlik inşası ve onun korunması da dijital dünyadaki trendlere göre şekillenmektedir (Kıran, 2021). Bireyler dijital dünyada kendilerini maksimum beğeni alacak şekilde tasvir ederek gerçek hayatları popüler ideallere ve trendlere göre şekillenirken çeşitlilik azalıyor ve dijital dünyayı şekillendirmek yerine toplum dijital dünyanın trendlerinin etkisiyle şekillenmiş oluyor (Richardson & Milovidov, 2022: 70-71).

Toplumsal etkileşim üzerine yaptığı bilimsel çalışmalarla sosyoloji dünyasına önemli katkılarda bulunan Erving Goffman, günlük yaşamı bir tiyatro oyununda olduğu gibi yapmacık olmasına rağmen gerçek ve genel olarak prova edilmeden sunulan performanslara benzetmektedir. Dijital dünyada da bireyler tıpkı seyirci ile hem etkileşim içerisinde olan hem de seyircileri etkilemeye çalışan tiyatro sanatçısı gibidir. Sosyal medya platformları da oyuncusunu bekleyen hazır sahnelere benzetilmektedir. Goffman'a (2009) göre kişi benlik sunumunu, içinde bulunduğu sosyal ortama en uygun şekilde ortaya koymaktadır. Dijital dünyada toplumda kabul görme kaygıları, yaşam kaygıları, maddi kaygılar, çeşitli korkular, kolay yoldan para kazanma isteği insanların benlik sunumunu etkileyen ve şekillendiren faktörlerdir. Dijitalleşmenin insanları kendi kimliklerinden uzaklaştırdığı zaman zaman dile getirilse de aslında insanlar doğası gereği özgür oldukları ölçüde benliklerini sunarak idealize edilmiş bir kimlik inşa etmeğe çalışırlar. İdealize edilmiş dijital kimliklerin insanların gerçek benliklerinden tamamen bağımsız olmadığı, benliklerinin uzantıları olduğu bilinmektedir.

Paylaşılan ve bazen de paylaşılmayan tüm içerikler, yorumlar, arkadaşlıklar, beğeniler, takip edilenler ve takipçiler, kullanıcının dijital kimliğindeki ilgi alanları,

zevkleri, başkalarının onunla ilgili paylaştıkları karakterini ve sosyal yönünü gösteren ipuçlarını barındırmaktadır. Dijital dünyada da her bir bireyin ve toplumun kendine özgü kavramları, tutumları ve dijital bir kültürü vardır. Siyasi, sosyal ve ekonomik şartların ortaya çıkardığı fenomenler diğer dijital kimliklere öncülük etse de aslında her iki taraf birbirinden etkilenmektedir. Dijital kimlik, insanların dijital alanda kendileriyle ilgili sunduğu, paylaştığı ve tanıtımını yaptığı bilgilerin bütünüdür (Dalton & Crosby, 2013: 1). Dijital kimliklerini istedikleri biçimde kurgulayabildikleri için bireylerin genel olarak sosyal yönleri ile ilgili gösterdikleri ipuçlarının bazen de gerçek olmadığını da unutmamak gerekiyor. Bireyin yaşadığı koşullara uygun olarak inşa ettiği dijital kimlik daha tatmin edici olduğuna göre, gerçek sosyal kimlik üzerinde de etkili olabilmektedir.

Windley (2005) insanların dijital ortamlarda inşa ettikleri dijital kimlikleri psikolojik kimlik olarak tanımlamıştır. İnsanlar bazen bilinçli olarak, bazen de bilinçsiz olarak psikolojik durumlarını yansıtmaktadırlar. Psiko-pedagojik bir perspektiften bakıldığında, dijital kimliğin gelişimi, benliğin, diğer dijital kimliklerin ve dijital kültür müzakerelerinin toplumsal ve bireysel yansıması anlamına da gelir (Muñoz-Rodríguez vd., 2020: 3). Bazı kullanıcılar dijital ortamlarda beğeni toplama tutkusuyla vatanseverlik, vefat, milli değerler gibi toplumda kabul gören konularda zaman zaman içerikler paylaşıp beğeni toplamaya çalışırken, bazı kullanıcılar ise dijital ayak izlerinin olumsuz etkilerini göz önünde bulundurarak daha dikkatli davranırlar. İnternetin, mobil cihazların ve yapay zekâ teknolojilerinin yaygınlaşmasıyla, "geleneksel" yüz yüze etkileşimlerin ötesine geçen etkileşimde bulunma giderek daha kolay hale gelmiştir. Başka bir deyişle, dijital teknolojiler iletişim olanaklarını güçlendirerek mevcudiyet, zaman ve yer sınırlarını genişletmiştir.

İnternet olanaklarının her geçen gün geliştirilerek ileri aşamaya taşındığı ve etkileşimlerin de daha gelişmiş evreye yükselişi devam etmektedir. Benlik sunumunun da avatarlar ve NFT'ler aracılığıyla daha ileri bir boyuta taşınarak fiziksel yaşamın Metaverse'de tekrar yaratılması planlanmıştır. İnsanlar adeta fiziksel dünyada yaşanıyormuşçasına her tür duyguyu deneyimlemek adına benliklerini vitrin performansları ile Metaverse'de sunmaktadırlar (Türk vd., 2022: 316). İnsanlar Metaverse'de değerli hissetmek, onaylanmak, ait olmak gibi

duyguların yanı sıra kendi statülerini, sosyoekonomik sınıflarını, kimliklerini, imajlarını kurgulayıp tekrar yaratmak imkânına sahiptirler. Kullanıcıların dijital dünyada imajlarını oluşturmak ve muhafaza edebilmek için niteliklerini geliştirmeleri konusunda eğitim almaları veya en azından faydalı kaynakları okumaları yararlı olacaktır. İnsanların sürdürülebilir gelişimini ve bilinçli dijital katılımını sağlamak için sosyal ve motivasyonel özellikleri de dikkate alınarak eğitilmeleri anlamlı olacaktır.

### 1.4.8. Dijital Dünyada Aktif Katılımın Önemi

Aktif katılım vatandaşların içinde yaşadıkları demokratik kültürlere aktif ve olumlu bir şekilde katılırken, sorumlu kararlar alabilmeleri için gereken yeterlilikleri kapsar. Dijital dünyada aktif katılım başka bir ifadeyle e-katılım olarak da bilinmektedir. E-demokraside katılımcıların aktif ve yapıcı katılım sağlamaları hesap verme sorumluluğu ve şeffaf yönetim için başarının kilit noktasıdır (Wirtz vd., 2018: 9). Göz önünde bulundurulması gereken temel hususlar, hedeflenen grupların tercihleri, teknik erişimi ve becerileridir. Vatandaşlar dijital katılım paradigmasıyla toplumda sosyal değişimi destekleyen ve ayrıştıran unsurlar konusunda kapsayıcı ve toplumun etik değerlerine uygun bağlantısal katılım davranışı sergileme fırsatına sahiptirler (Atalay, 2022). Aktif katılım ister çevrimiçi ister çevrimdışı olsun, çevreyi şekillendirme ve kişinin kendisini etkileyen kuralları belirlemesi için gerçek bir olasılık olarak anlaşılmalıdır. Çevrimiçi aktif katılım, kullanıcılar arasında güç ve etkinin eşit dağılımına dayanır. Dijital vatandaşlık anlayışıyla birlikte yöneticilerin geleneksel hesap vermeme eğilimleri, güçlü merkez düşüncesi, gerçek olmayan şeffaflık ilkesi, sınırlandırılmış ifade özgürlüğü araçları, merkezi devletle derin ilişkiler kuran geleneksel medya gibi sorunlar farklı bir şekle evrilmiştir (Işıklı, 2015). Fakat dijital olanaklar yönetenleri geleneksel demokrasi anlayışını terk etmek zorunda bıraksa da manipülasyona açık olmaları da en büyük dezavantajlardan biridir.

Müzakereci karar verme süreçleri gibi demokratik değerlere sahip, merkezi olmayan çevrimiçi hizmetlerin geliştirilmesi, çevrimiçi aktif katılımın teşvik edilmesine de katkıda bulunacaktır. Sürdürülebilir kalkınma hedeflerine ulaşmak için vatandaşların bilinçli katılımı öncelikli meselelerden biri olarak görülmektedir.

BM'nin 2030 gündemi ve sürdürülebilir kalkınma hedefleri arasında bilgiye erişimin ve vatandaş katılımının sağlanması, bölgesel ve ulusal veri ekosistemlerinin güçlendirilmesi, özel sektör ve sivil toplumun katılımıyla inovasyon ve teknoloji ağlarının güçlendirilmesi, veri açıklığının teşvik edilmesi, idari kayıtlar, büyük veriler ve sivil toplumdan gelen geleneksel olmayan verilerin dahil edilmesi, coğrafi bilgilerin toplanması ve görselleştirmelerin yapılması, teknolojik yenilikleri, dijital ekonomiyi, bilgi ve bilgi toplumunu takip etmek gibi sorumlulukların önemi özelikle vurgulanmıştır. E-katılımın, kapsayıcı kalkınmayı teşvik etmek için halkın katılımını ve planlama yapan yetkilileriyle iş birliğini kolaylaştıracağına dair büyük umutlar vardır (Bouregh vd., 2023). Gelişmiş ülkelerin planlama sistemlerinde e-katılımın kullanımı giderek artmasına rağmen, gelişmekte olan ülkelerde uygulaması oldukça sınırlı kalmıştır (Shahab vd., 2021: 1).

Gerçekleşme olasılığı çok düşük olsa da sürdürülebilir kalkınma hedeflerinin gerçekleştirilmesi için özellikle en yoksul ve en savunmasız durumdakilerin ihtiyaçlarına odaklanan ve tüm ülkelerin katılımıyla güçlendirilmiş bir küresel dayanışma ruhu yaratılmalıdır. Söz konusu ihtiyaçlar arasında yeni nesil teknolojilerin satın alınma gücü ve kullanma yeteneğine sahip olmak kalkınma hedeflerin gerçekleştirilmesinde mühim rol oynamaktadır. E-katılımı gerçekleştirmenin önünde sosyoekonomik koşulları, eğitimi ve demografik özellikleri yansıtan en büyük engellerden biri dijital uçurumdur (Setthasuravich & Kato, 2020). E-demokrasinin temel konsepti olan e-katılımın nihai amacı yolsuzlukların azaltılması, kurumların şeffaflığının ve hesap verebilirliğinin artırılması, kapsayıcı ve katılımcı süreç ve politikaların teşvik edilmesi ve iyi yönetişim ilkelerinin güçlendirilmesine yardımcı olmaktır (Tavares vd., 2020). E-katılım, düşük maliyetli olması, garantili anonimlik özelliği, uzak bölgelere ve dışlanmış gruplara küresel erişimi nedeniyle, geleneksel halk katılımı tarzının bazı sınırlamalarının aşılması için en iyi fırsatlar sunmaktadır (Bouregh vd., 2023). Her ne kadar iktidar ve muhalif görünümlü siyasetçiler çıkar ittifakları kursalar da bireyler dijital imkânları dijital avantajlara çevirmek için direnmelidir. World Wide Web Vakfı tarafından yürütülen birçok araştırma sonucunda, kadınlar, azınlıklar ve engelliler gibi aktörlerin dışlandığı, çevrimiçi aktif katılımda beyaz eğitimli erkeklerin egemen olduğu ortaya çıkmıştır.

Dijital becerilerin geliştirilmesi, gençlik girişimciliği, bağlantılı öğrenme, dijital hikâye anlatımı, topluluk liderliğindeki dijital girişimler ve politika geliştirme vatandaşların dijital güvenlerini ve becerilerini hem evde hem de yerel toplulukta geliştirmelerine olanak sağlayacak yeni yollar önermektedir (Dezuanni vd., 2017). Halkın e-katılımı benimsemesi ve memnuniyeti ile yerel yönetimdeki şeffaflık ve güven arasında pozitif bir ilişki olduğu tespit edilmiştir (Kim & Lee, 2012). Birçok sektörde yetkililer e-katılımcıların öfkesini dindirmek ve bazen de haklı eleştirileri dikkate almak amacıyla sosyal medya platformlarında kendilerine karşı muhalif görünümlü sayfalar veya gruplar oluşturarak kitleleri kontrol altında tutmaya çalışıyorlar. Sorun yaşayan katılımcılar ilgili kurum veya kuruluşa karşı olduğuna inandığı sosyal medya grubuna veya sayfasına mesaj göndererek veya yorum yazarak kısmen de olsa psikolojik olarak tatmin olmuş olur. Böylelikle kurum ve kuruluşların oluşturdukları muhalif görünümlü sosyal medya grupları bir nevi koruyucu kalkan rolünü oynamaktadır.

BT'nin demokratik katılımda devrim yaratacağı yönündeki umutlara rağmen, e-katılım sistemlerinin genellikle beklenen hedeflere ve uygulama düzeylerine ulaşmada başarısız olduğu da zaman zaman tartışılmaktadır (Toots, 2019). Ama bu durum tüm dünya ülkeleri için kesinlikle aynı değildir. Dünya ülkelerinin toplumları hükümetleri arasında istişare ve diyalog konularında gerçek dünyada ne kadar katılım sağlayabiliyorlarsa dijital dünyada da o kadar katılım sağlayabilmektedir. Sonuç olarak dijital teknolojiler vatandaşların iradelerine, kültürüne, inançlarına, sosyoekonomik (Girish vd., 2014) faktörlere ve becerilerine bağlı olarak kullandıkları araçlardır. E-Katılım biçimlerinin hükümet ve vatandaşlar arasında karşılıklı yarar sağlayacak şekilde nasıl düzenlenebileceği ve güncel teknolojilerin kullanımıyla alışıla gelmiş durumun nasıl dönüştürebileceği konusunda ayrıntılı araştırmaların yapılması yararlı olacaktır.

### 1.4.9. Dijital Haklara ve Sorumluluklara Odaklanmak

Modern vatandaşlık yaklaşımına göre haklar medeni, siyasal ve sosyal haklar olarak üç kategoride ele alınmaktadır. Haklar ve sorumluluklarla ilgili bilgi sahibi olmak, dijital vatandaş olarak aktif katılım sağlamanın anahtarıdır (Richardson & Milovidov, 2022: 18). Yeni teknolojilere uyum ve adaptasyon uluslararası insan

haklarının doğasını değiştirmiş (Shany, 2023), yeni dijital insan hakları ortaya çıkmış ve mevcut evrensel insan hakları normlarının kapsamlı bir şekilde yeniden yorumlanması zarureti doğmuştur. Dijital dünyada vatandaşın çevrimiçi dünyadaki farkındalığı, hak ve sorumluluklarını anlamasıyla ilgilidir. Dijital haklar, bireylerin dijital içeriğe erişmesine, içerikleri kullanmasına, içerikleri oluşturmasına ve yayınlamasına veya elektronik cihazlara ve telekomünikasyon ağlarına erişmesine izin veren insan haklarını ifade eder. Dijital dönüşüm öğrenmekten, çalışmaktan, iletişim kurmaktan, iş yapmaktan yönetimlerle etkileşime, alışverişten kültürden keyif almaya kadar hayatımızın her alanında hepimizi ilgilendirmektedir (Polona, 2022). Otomasyon, yapay zekâ, nesnelerin interneti ve makine öğrenmesi gibi teknolojik tabanlı gelişmelerin hem işletmelere hem de toplumlara faydaları günlük yaşamda giderek daha da belirgin hale gelmektedir (Akman, 2023: 1).

Dijitalleşme, bireylerin belirli bölgelerin ve sosyal konumların ötesine ulaşmasını sağlayarak, bireylerin öğrenmesi, eğlenmesi, çalışması, keşfetmesi ve hedeflerini gerçekleştirmesi için yeni ve çeşitli imkânlar sunmaktadır. Vatandaşlar dijital dünyada mahremiyet, güvenlik, yanlış bilgiye karşı koruma hakkı, kişisel verilerin korunması hakkı, erişim, katılım, ifade özgürlüğü, bilgi edinme özgürlüğü, dijital eğitim, beceriler edinme, adil çalışma koşulları, miras hakları, telif hakları ve dijital kamu hizmetleri gibi daha pek çok haktan yararlanma konusuna iyi odaklanmalıdırlar (Polona, 2022). Bununla birlikte, dijital dünyadaki avantajların ve yasal faaliyetlerin yanı sıra, telif haklarının ihlali, nefret söylemi, sanal bahis, uyuşturucu ticareti, pornografi, siber güvenlik sorunları gibi kötü niyetli çevrimiçi davranışlara karşı da hazırlıklı olmak için efor sarf etmek gerekmektedir.

Gelişmiş ülkelerde yönetenler yarının dünyasında, kendi kaderlerinin efendisi olmak amacıyla dijital olarak yetkilendirilmiş ve yetenekli vatandaşlara, dijital olarak yetenekli bir iş gücüne ve bugün olduğundan çok daha fazla dijital uzmana güvenmeleri gerektiğinin farkındadırlar. Vizyonlu yöneticiler amaçları doğrultusunda, yüksek performanslı dijital eğitim ekosisteminin geliştirilmesinin yanı sıra, dünyanın dört bir yanından yeteneklerle bağlantıları teşvik eden ve onları cezbeden politikalar yürütmektedirler. Bu politikaların yanı sıra dijital ürünleri ve çevrimiçi hizmetleri kullanabilen, dezenformasyon ve dolandırıcılık girişimlerinin

farkında olan, kendisini siber saldırılara karşı koruyabilen toplum oluşturmak için projeler de desteklenmektedir.

Dijital dünyada sorumlu davranmayan veya başkalarının haklarını ihlal eden bireylerin diğer bireyler, topluluklar ve yetkililer tarafından tespit edilip cezalandırılmasının mümkün olduğu gibi, bireylerin dijital haklarını ihlal eden ve sorumluluklarını yerine getirmeyen hükümetlerin ve teknoloji şirketlerinin de uygun yöntemlerle cezalandırılması önem arz etmektedir. Dijital dünyada ülke sınırları olmadığı için, bireyler ulusal düzenlemelerin yanı sıra uluslararası bazı düzenlemeleri, uyulması gereken etik kuralları da bilmek zorundadırlar.

Avrupa Komisyonu dijital dönüşümün herkese fayda sağlamasını hedefleyen altı ilke belirlemiştir; insanları ve haklarını dijital dönüşümün merkezine koymak, dayanışma ve katılımın desteklenmesi, çevrimiçi seçim özgürlüğünün sağlanması, dijital kamusal alana katılımın teşvik edilmesi, bireylerin güvenliğini, emniyetini ve yetkilendirilmesini artırmak, dijital geleceğin sürdürülebilirliğini teşvik etmek (European Commission, 2023). Dijital haklardan kimsenin mahrum kalmaması amacıyla kırsal kesimdekiler dahil herkesin bağlantı kurabilme olanaklarına sahip olması, dijital eğitim alma, gereken becerilerin geliştirilmesi, adil çalışma koşullarının sağlanması, şeffaflığın artırılması ve dijital ortamda kamu hizmetlerinin ulaşılabilir olması için yetkililerin ekstra çaba göstermesi gerekmektedir.

İnovasyonu artırmakla küresel çevre sorunlarına ve toplumsal engellere yönelik çözümler arasında etkili bağlantılar kurmak için bireylerin bilgi teknolojilerini proaktif bir şekilde kullanmaları büyük önem taşımaktadır (Özbay & Genç, 2023: 615). AB yatırım akışına ve inovasyona dayalı açık bir dijital ekonominin refahın motoru olduğunu belirterek birliğe dahil olan ülkelerin çıkarlarını ve değerlerini güçlü bir şekilde desteklemek amacıyla üç kapsayıcı ilke belirlemiştir; dijital pazarlarda eşit şartların sağlanması, güvenli bir siber alanın ve çevrimiçi temel hakların desteklenmesi (European Commission, 2021). AB sadece kendi sınırları içerisinde dijital hakların korunmasına yönelik kapsamlı bildiriler yayınlamakta ve uygulanmasını teşvik etmektedir. Dijital hakların korunması dünyanın belirli bir kesimi için değil, dünya genelinde uygulanması gereken evrensel bir proje olmalıdır. Dijital dünyanın ulusal devletler gibi sınırları olmadığını unutmamak gerekiyor. Gelişmemiş ülkelerde ve dünya genelinde kırsal alanlarda da

en azından temel dijital haklardan faydalanmak için gereken koşullar oluşturulmalıdır. Dünya genelinde ekonomik refahın güçlendirilmesi için becerilerin geliştirilmesi, altyapıların, iş dönüşümü ve kamu hizmetlerinin iyileştirilmesi temel hedefler olarak belirlenmelidir.

Kendisinin fiziksel sınırları dahilinde dijital ortamda insan haklarının korunmasına nispeten özen gösteren Batı toplumu ve Avrupa ülkeleri diğer ülkelerin vatandaşları tarafından bir dönem rol model olarak görülmüştür. Fakat Batı ve Avrupa ülkelerinin 2022 yılında başlayan Ukrayna savaşı ve 2023 yılında başlayan Gazze katliamına yönelik bencil politikaları hayal kırıklığına neden olmuştur. Yıllarca demokrasi ve insan hakları savunucusu gibi görünen ABD'nin İsrail'i desteklemesi ve Gazze için gönderilen temel insani yardımlara bile karşı çıkması haberlere yansımıştır. Ortaya çıkan manzara uluslararası kuruluşları araka plana itmiş, otoriter baskıların artmasına veya devam etmesine zemin hazırlamıştır. Otoriter yönetimler devletin temel pozitif yükümlülüklerini yerine getirmek yerine dijital teknolojileri gözetim ve sansür amacıyla kullanarak yönettikleri toplumların inkişafına engel olmaya devam etmektedirler. Güç ve kontrol yapılarından insan hakları ihlallerine yönelik çözüm beklemek yerine bireysel olarak yasal sorumluluk yüklenme zarureti her geçen gün artmaya devam etmektedir. Bireyler dijital dünyada insan haklarıyla ilgili evrimin dayandığı gelişmelerin siyasi sürdürülebilirliğini sorgulamak zorundadırlar.

Çeşitli olumsuz gelişmeler teknoloji alanında lider olan ülkelerin dijital olanakları dünya genelinde insanların yararına kullanmaktan ziyade çıkarlarını savunmak ve korumak için kullanmaya üstünlük vereceklerini göstermiştir. Uluslararası kuruluşlar, sivil toplum kuruluşları ve hükümetler ortak çalışmalarla dijital ortamda temel hakların korunmasına yönelik zorluklara ve hak ihlallerine karşı çözüm üretmeli, yeterliliklerin pekiştirilmesi amacıyla projeler hazırlanmalı ve desteklenmelidir. Dijital dünyada tüm insanların medeni, siyasi, ekonomik, sosyal ve kültürel bağlamlarda çeşitli haklarının hiçbir fark gözetilmeden korunması amacıyla kimseyi geride bırakmayan güçlü bir toplumsal sözleşme hazırlanmalıdır. İnsanların dijital tüketim üzerine eleştirel bir yaklaşımla düşünmeleri, sorgulamaları, birbirinin haklarına saygılı davranmaları için gereken imkânlar sağlanmalıdır. Bunun yanında dijital ortamda gözetim, sansür ve manipülasyona karşı çıkarak mahremiyet, veri

koruma ve ifade özgürlüğü haklarını desteklemek için kapsamlı yasal düzenlemeler yapılmalı ve bağımsız kurumlar tarafından takip edilmelidir.

Dijital teknolojiler dünya genelinde tüm insanlara hizmet etmeli ve insanlara fayda sağlamalı, insanların hedeflerine ulaşmalarını ve günlük yaşamlarını kolaylaştırmalı, güvenliklerini veya temel haklarını ihlal etmemelidir. Günümüz dünyasında büyük veri, blockchain, robotlar ve yapay zekâ bağlamında şekillenen sosyal ilişkiler ilerleyen süreçte otonom silahların yaygınlaşmasıyla (Harari, 2016) daha karmaşık hale gelecektir. Dijital gelişmelere paralel olarak insanların başkalarıyla etkileşimde bulunurken uygun dil kullanmaları, başkalarının inançlarına ve fikirlerine saygı göstermeleri, telif haklarıyla ilgili kurallara uymaları, dijital ortamdaki sözleşmelere dikkat etmeleri gerekmekte, siber güvenlikle ilgili sorumlulukları da artmaktadır. Dijital sorumluluklar, vatandaşların dijital ortamlarda ve topluluklarda başkalarıyla etkileşimde bulunurken gerçekleştirmesi gereken eylem ve davranışlardan ibarettir. Dijital haklarının ve sorumlulukların farkındalığına yönelik en büyük engeller gelir dengesizliği, dijital bölünme, erişim sorunu ve dijital okuryazarlık eksikliğidir. Vatandaşların dijital ortama hazırlanması için dijital haklar ve dijital okuryazarlığın paralel olarak geliştirilmesi gerekmektedir (Pangrazio & Sefton-Green, 2021). Dijital hakların korunması ülkelere göre farklılık gösterse de dijital hukuki ilişkilerin alanı sınır ötesi ve dijital dünya olduğuna göre gelişmekte olan ülkelerin de sürece dahil edilmesi zaruridir. Gelişen dijital evrim aşamasında bilgi toplumunda insan varlığının hukuki dayanağı olan faydalara, koşullara, ilkelere, prensiplere ve fırsatlara odaklanmak olumlu değişimlere yol açacaktır.

### 1.4.10. Dijital Dünyada Tüketici Farkındalığının Önemi

Dijital dünyada, vatandaş olmak aynı zamanda kullanıcı, tüketici ve üretici olmak anlamına gelmektedir. Bu konuyla bağlantılı boyutları anlamak, bireylerin dijital ortamlarda bilinçli hareket edebilmeleri için gereklidir. Bilinçli tüketici, ihtiyaç ve isteklerini doğru analiz edebilen, mal veya hizmet satın aldığında ise kalite, fiyat ve sağlamlık konularını iyi değerlendirebilen ve satın alacağı ürünün doğa ve toplum ile ilişkisini de irdeleyerek tüketimden fayda sağlanmasına önem veren kişidir (Karaboğa, 2022). Dijital çağda bilinçli tüketiciler işletmelerin kaliteli ürün ve hizmet sunmaları konusunda gerekli standartların oluşturulmasında etkili rol

oynamaktadır. Tüketici bilincinin birçok boyutu vardır; organize boykotlar, köleliği sona erdirmek veya adil ticareti teşvik etmek vb. Bu bağlamda birçok siyasi hedefe ulaşmak için gerekli adımlar atılabilmektedir. Micheletti ve Boström'te (2014) göre boykot, belirli bir ürün veya markayı satın almamaya yönelik kasıtlı ve bilinçli tüketici seçimidir. Bilinçli tüketici davranışlarında boykot eyleminin yanı sıra teşvik edici satın alma süreci veya politik davranışlar da zaman zaman sergilenmektedir. Yapılan araştırmalara göre tüketicilerin etik tüketimini ve çevre yanlısı davranışlarını dindarlık, farkındalık, çevresel tutumlar, güven ve bilgi, değerler, ahlaki inanç ve öznel normlar gibi birçok faktör etkilemektedir (Khan & Abbas, 2023).

Tüketimin değişen yapısı ve internet bağlantılı teknolojiler vatandaşların maddi ve manevi konulardaki siyasi ve ekonomik tepkilerini tüketim üzerinden sergileyebilme olanağı sunmuştur. Eskiden bilinçli tüketiciler sadece satın alma öncesi ve sonrası rasyonel davranışlar sergileyen tüketici konumundayken artık değişen koşullar ve insanoğlunun doğaya karşı bilinçlenmesiyle birlikte etik bilinci, sosyal ve siyasi sorumluluk bilinci, çevre sorumluluğu bilinci gibi rasyonel boyutlara da sahiptirler (Buğday, 2015). Tüketici odaklı bir ekonomide, mal ve hizmetleri tüketme eyleminin kendisi bir demokratik katılım biçimidir. Garrett (1987) boykot kavramını, bir grup aktörün (temsilcilerin), belirli politikalara ilişkin hoşnutsuzluğunu iletmek ve bu politikaları değiştirmek amacıyla hedef aktörlere baskı yapmak için pazarlama işlemlerini yürütmeyi planlı ve zorunlu olmayan bir şekilde reddetmesi olarak tanımlamaktadır.

Belirli bir ürün veya hizmeti satın almak sadece bireysel bir karar değil, aynı zamanda bir şirket için resmi bir destek, iş modeli, iş uygulamaları ve üretim stratejisidir. Özel sektörün ekonomik ve politik hayatımızda artan rolü göz önüne alındığında, demokrasi sadece sandıkla uygulanamaz. Dijital teknolojiler yaygınlaşmadan önce ekonomik yapının temeli olan üretim süreci tüm toplumsal süreçleri etkiliyordu, dijital çağda ise tüketim eğilimleri üretim yapısı da dahil tüm toplumsal süreçleri şekillendirmektedir. Tüketici eylemleri başta büyük çokuluslu şirketler olmak üzere, uluslararası kuruluşları, hükümetleri ve diğer güç sahiplerini hedef alabilmektedir. Sosyal platformlarda kullanıcılar sadece tüketici değildir, ayrıca bir çeşit kullanım ya da değişim değeri ihtiva eden profiller, içerikler, bağlantılar, toplumsal ilişkiler, ağlar ve topluluklar yaratan üretken tüketicilerdir

(Gümüş, 2023). Dijital platformlarda kullanıcıların ücretsiz emek konusunda bilinçli davranışlar sergilemesi büyük teknoloji şirketlerini dijital emek sömürüsünü sona erdirmeye de mecbur edebilir.

Yönetenler her ne kadar bireyleri özel hayatlarıyla meşgul olmaları için belirledikleri çerçevede tutmaya çalışsalar da yerel ve küresel ölçekte toplumsal sorunlar herkesi yakından etkilemektedir. Tüketiciler hem bireysel hem de toplu şekilde boykot eylemiyle kurumsal davranışları etkileyebilme veya değiştirebilme potansiyeline sahiptirler. Yapılan araştırmalarda Almanya'da nüfusun yaklaşık yüzde 60'ı, Birleşik Krallık'ta ise nüfusun yüzde 50'sinden fazlasının tüketime yönelik aldığı kararlarda siyasi ve etik faktörlerin belirleyici rol oynadığı saptanmıştır (Zorell, 2018). Ayrıca yaşam tarzı politikalarının amacı diğer insanlara mesaj göndermek, genel olarak toplumsal değerleri şekillendirmek, gıda ve tüketim mallarının tedarikini dolaylı olarak etkilemektir (Stolle & Micheletti, 2013). Nitelikli boykot eylemleriyle devletin rolünde siyasal ve ekonomik açılardan değişimlerin yapıldığı tecrübe edinilmiştir. Teknolojik imkânların yaygınlaşmasıyla daha da sofistike hale gelmiş boykot eylemleriyle hedefler üzerinde daha fazla baskı oluşturmak mümkündür. Aynı zamanda, tüketicilerin tüketici gücünün sınırlarını anlamaları ve onları yanıltma veya manipüle etme girişimlerinin farkına varmaları, tekellerle veya tüketicileri belirli koşullara kilitleyen baskın piyasa oyuncuları ile ilgili konularda bilgi sahibi olmaları kolaylaşmıştır. Dijital dünyadaki faaliyetlerin izlenmesi ve işlenmesi sonucunda hedefli reklam, yeşil yıkama, yalan haber, algoritmalarla manipülasyon gibi temel konuların farkında olmak tüketici davranışları açısından belirleyici hususlardır. Klasik anlamda politika oluşturma sürecine dahil olamayan ve karar alma süreçlerinden dışlanan yurttaşlar, tüketim edimini ve pazarı bir siyasal ifade ve eylem aracı olarak kullanabilirler (Kiçir & Cengiz, 2022: 103).

Öte yandan ürün veya hizmet üretenler ve satanlar, kurum ve kuruluşların yetkilileri güncel dijital olanaklardan planlı bir şekilde faydalanabildikleri için tüketicilere nazaran daha avantajlı konumdadırlar. Hizmet veya ürün üretip satanların yapay zekâ teknolojilerini de kullanarak tüketici davranışlarına yönelik topladıkları somut bilgiler ışığında hareket edebilmelerine karşın tüketiciler sınırlı imkânlara sahiptirler. Fakat esas güç tüketicilerin veya yönetilenlerin tarafındadır. Üretim ve

tüketimin siyasi arka planı ve sonuçları küresel ölçekte bireyler tarafından anlaşılırsa ve bir politik katılım eylemine dönüşürse kamuoyu yararına anlamlı sonuçlar ortaya çıkacaktır.

### 1.5. E-yönetişim Ekosisteminin Önemi

Dijital olanaklar, vatandaşların istedikleri yerden, istedikleri zamanda, en uygun yollarla ve en uygun şeklide hizmet beklemesine yol açmıştır. BİT toplumsal yaşamın her alanını etkilediği gibi klasik kamu yönetimi anlayışını da derinden etkilemiştir. Dijital çağa uygun olarak yönetişim anlaşışı e-yönetişim modeline evrilmiştir. BT'lerin kamu sektörünün çeşitli düzeylerinde ve ötesinde, geliştirme amacıyla kullanılması anlamına gelen e-yönetişim, elektronik yönetişim (Saylam, 2022), akıllı yönetişim, e-katılım, e-devlet uygulaması olarak da bilinmektedir. E-yönetişim, bilgi ve iletişim teknolojilerinin bilgi alışverişi ve işlemlerin verimliliğini, etkililiğini, şeffaflığını ve hesap verebilirliğini artırmak amacıyla faydalı bir şekilde kullanılmasıdır (Yılmaz vd., 2022). E-yönetişim sürecinde bilgi alışverişi ve işlemlerin gerçekleştiği dört temel alan vardır; hükümetler arasında, devlet kurumları arasında, hükümet ile vatandaşlar arasında ve hükümet ve işletmeler arasında olan alanlardır. Bu bağlamda hem özel hem de devlet sektöründe süreçleri basitleştirmek, birleştirmek ve daha verimli hale getirmek için e-yönetişim ekosisteminin yaratılmasına büyük ihtiyaç vardır. Daha bütünsel bir bakış açısıyla şu anda e-devlet uygulamasında eksik olan vatandaş merkezli yaklaşımı e-devlet ekosisteminde tamamlamak mümkündür. E-devlet ekosistemi, vatandaşları, kuruluşları, şirketleri ve devlet kurumlarını kapsayan, katılımcılarına değer yaratmak ve dağıtmak için elektronik platformları kullanan karmaşık bir sosyoteknik bir sistem olarak tanımlanmaktadır (Rantanen vd., 2019).

E-yönetişim yeni bir trend olmasa da hala gelişmiş ülkelerde bile vatandaşların dijital ortamda kapsamlı bir şekilde karar alma süreçlerine katılımı gerçekleştirilmemiştir. Gelişmekte olan ülkelerdeki üniversitelerde bile henüz basit imzalama işlemlerini dijital ortama taşıyabilecek kadar mesafe kat edilmemiştir. Bu uygulamanın kapsamlı bir şekilde gerçekleştirilmesi için uygun kapasiteli topluma, hukukun ve ahlakın üstünlüğünü ilke edinmiş yönetimlere ve dijital devrim için uygun siyasi, kültürel ve ekonomik bir düzene ihtiyaç vardır. E-yönetişim girişimleri

karmaşık bir süreç olduğu için kolektif bir vizyona ve ortak bir amaca odaklanmayı gerektirir. Kamu hizmetlerini vatandaşlar için dijital ortamda daha ulaşılabilir hale getirmek amacıyla uygun altyapının sağlanması en temel ihtiyaçlardan biridir. Şeffaflığın ve güvenilirliğin artırılması amacıyla devlet hizmetlerinden toplumun her ferdinin eşit bir şekilde ve uygun maliyetlerle faydalanabilmesi temel hedef olmalıdır. Nitekim AB'nin 2030 Dijital Pusulası'nda 2030 yılına kadar Avrupa vatandaşları ve işletmeleri için temel kamu hizmetlerinin yüksek güvenlik ve gizlilik standartlarına uygun olarak yüzde yüz çevrimiçi olarak sağlanması, demokratik yaşamın ve çevrimiçi kamu hizmetlerinin engelli kişiler de dahil olmak üzere herkes için tamamen erişilebilir olması hedef olarak belirlenmiştir (European Commission, 2021). Dijital çağda temel ihtiyaçların dijital ortamda kolay bir şekilde karşılanması temel insan haklarından biridir. Dijital teknolojiler halkın yönetime katılabilmesi, şeffaf ve hesap verebilir bir yönetim modelini uygulanması açısından büyük kolaylık sağlamaktadır.

Vatandaşlar için daha rahat ve kolay hizmet alma imkânı sunan e-yönetişim modeli hükümetlerin iş yükünü de hafifletmektedir. Ayrıca ülke sınırlarında yaşayanların kişisel verilerinin tek merkezde toplanması ve ihtiyaç olduğu taktirde kullanılabilir olması hükümetlerin de işine yaramaktadır. Dijital çağın günümüz toplumlarında yarattığı en önemli etki, eskiye kıyasla daha fazla denetlenebilen bir yaşam biçiminin içine girilmesidir (Kaypak vd., 2017: 913).

Postkolonyal ulusal devletlerin bir tür varoluşsal kriz içinde olduğu konusunda teorisyenlerin hemfikir olduğu açıktır (Rao, 2019). Ulusal devletler yalnızca ekonomik değil, aynı zamanda sosyal, kültürel, politik, çevresel, medya, teknolojik olarak küresel güçlere karşı giderek savunmasız ve bağımlı hale gelmektedirler. Ulusal ve uluslararası organizasyonların, hükümetlerin sürdürülebilir rekabet avantajı yakalamasında yenilikçilik zorunlu bir gerekliliktir. BİT alanında, son yıllarda yaşanan büyük gelişmeler neticesinde emek, sermaye ve doğal kaynakların yanı sıra yeni bir üretim faktörü olarak yerini alan bilgi, organizasyonların rekabet avantajı sağlamasında en önemli kaynak unsuru hâline gelmiştir (Aktan, 2018). Dijital teknoloji, insanların çeşitli günlük aktiviteleri gerçekleştirmesini kolaylaştırdığı için dijital hak ve sorumluluklar da zorunlu hale gelmiştir. Yolsuzlukların dijital platformalar aracılığıyla yaygın olarak bilinmesi ve

hükümetlerdeki gücün kötüye kullanılması, yönetimle ilgili şeffaflık talebinin artmasına yol açmıştır. Başta X (Twitter) olmak üzere sosyal ağlarda yer alan gündem ve tartışmalar, siyasiler üzerinde de kamuoyu baskısı yaratmaktadır (Demirel, Kahraman & Gündüz 2022: 24).

Ulusal devlet kavramı bölgesel olarak siyasi arenada kendi kaderini tayin etme hakkına sahip olan devlet şekli olarak tanımlanmıştır. Ulusal devlet kültürel, dilsel veya dini yakınlık ve ekonomik bağımsızlığı olan devlet şeklidir. Özellikle internet teknolojilerinin yaygınlaşmasıyla küreselleşme, ulusal devletleri sermayeye, uluslararası şirketlere ve daha güçlü devletlere karşı giderek daha savunmasız ve bağımlı hale getirmektedir. Son yıllarda yapılan seçimlere katılım oranları incelendiğinde ciddi düşüşler olduğu gözlemlenmektedir. Bu davranışlar çoğu kişinin mevcut yönetim şeklinden memnun olmadığı veya yönetenlere güvenmediği anlamına gelmektedir. Dünya nüfusunun yarısı ulusal devlet yönetimi yerine teknokrasiyi tercih ediyorsa, seçimlere katılım oranı genellikle %40'ın altındaysa, eğer dünya ekonomisinin %60'ı kayıt dışı ise ve dolayısıyla vergiye tabi değilse, o zaman en azından dünyanın bazı yerlerinde ulusal devlet mekanizması artık boş bir kabuğa dönüşmüştür (Mihr, 2022; 129-130).

Küreselleşme süreci kapitalizm ile ulusal devlet arasındaki ilişkiyi geçmişten farklı bir boyuta taşımış ve ulusal devletin ekonomik alan başta olmak üzere siyasal, sosyal ve kültürel alanda yürüttüğü faaliyetlerinin tüm boyutlarıyla sorgulandığı bir durumu ortaya çıkartmıştır (Bakan & Tuncel, 2012: 51). Zorunlu olarak değişen koşullardan dolayı ulusal devletleri yeniden yapılandırılırken kritik zorluklarla karşı karşıya kalan hükümetler vatandaşları baskı altında tutmak için devletin ekonomik gücünü, kolluk güçlerini ve dijital olanakları kullanmaktadırlar. Fakat yapılan baskıların uzun dönemde işe yaramayacağı ve dijital olanakların eski politik düzenin çöküşünde önemli rol oynadığı anlaşılmaktadır. İnsan haklarının kolluk güçleriyle kısıtlandığı ülkelerde vatandaşlar korktukları için sussalar da huzursuz oldukları bilinen bir gerçektir. Siyasi liderliğin küresel zorluklara yanıt verme konusundaki beceriksizliği ve isteksizliği nedeniyle öfkeli ve hayal kırıklığına uğramış bir kalabalığı temsil ediyorlar ve bu da onlara büyük bir sosyal hareketlilik eksikliği yaşatıyor (Mihr, 2022; 133). Otoriter hükümetlerin direnişine rağmen dijital

olanaklar eski politik düzenin çöküşüne yol açan ekonomik, kültürel ve çevresel bozulmaların lokomotif gücü olarak nitelendirilmektedir.

Bilgi sistemleri verimliliği artırmakta ve zamandan tasarruf sağlamakta, işletme yönetimi, karar verme, rekabet, gelişme için önemli bir araç haline gelmekte ve özellikle yeni öğrenme ve eğitim yöntemlerinde öne çıkmaktadır (Szymkowiak vd., 2021: 2). Dijital teknolojilerin itici gücü tek taraflı bilgi akışından bireylerin çevrimiçi ortama taşınan veriye ve hizmetlere doğrudan erişimini sağlamanın ötesine geçerek, örgütsel yapıyı ve devlet-vatandaş etkileşimini şeffaflık, hesap verebilirlik, eşitlik, iş birliği, katılım ve demokrasi ilkeleri çerçevesinde güçlendirmeye evirilmiştir (Çiftçi, 2023). Kısa zamanda yaygınlaşmasına rağmen dijital ortamda yönetişim ve hükümetler arası güvenli bilgi alışverişinin önemi her geçen gün artmaktadır. E-yönetişim uygulamaları az maliyetli ve pratik olması nedeniyle hem hükümet hem de vatandaşlar için büyük kolaylık sağlamaktadır. Bu hizmetler dünyanın birçok ülkelerinde farklı düzeylerde verilmektedir. Hem dijital hem de fiziksel dünyada vatandaşların her türlü ihtiyaçları hükümet denetimi altındaki kişi veya kurumlar tarafından karşılanmaktadır. Fakat hükümetler tarafından gelir kaynağı olarak görülen bazı işlemler bilinçli olarak dijital dünyaya entegre edilmemiştir. Kurum ve kuruluşların bazılarında da masraflardan kaçınmak için eski düzen devam etmektedir.

Ulusal ve uluslararası yasal düzenlemelere göre insan haklarının güvence altına alındığı belirtilse de uygulama aşamasında ciddi sıkıntıların olduğu ve hatta birçok ülkede insanların neredeyse tüm haklarının ellerinden alındığı bilinen bir gerçektir. Yapılan araştırmalara göre, birçok vatandaşın politikacılar yerine bağımsız uzmanlar, teknokratlar ve üniversite profesörleri tarafından yönetilmeyi tercih ettiği bulgulanmıştır (Sebastián vd., 2021; Bertsou & Caramani, 2022; Chiru & Enyedi, 2022; Rojon vd., 2023). Siyasi güvensizlik, güvencesizlik, ekonomik istikrarsızlık, yolsuzluklar ve genel olarak toplumdaki huzursuzluk mevcut ulusal devlet yönetimi modelinin istenmediğini ve insanların farklı arayışlar içinde olduğunu ortaya koymaktadır. Gelişmiş ülkelerde yönetenler insan odaklı e-yönetişim modeliyle bilgi ve hizmet sunumunu kolaylaştırmak için çaba harcamalarına rağmen dünya genelinde yönetenlerle yönetilenler arasında gerilimin ve huzursuzluğun olduğu sık sık haberlere yansımaktadır. Günümüze kadar süregelmiş yönetim biçimleri mantık

ve ahlaki açıdan tatmin sağlayacak düzeye ulaşamamıştır. Acımasız vergi politikaları ve ülkelerin doğal zenginliklerinin yönetenler tarafından kanun kılıfına uydurularak özelleştirilmesi yıllarca süre gelmiş uygulamalardır.

Yeni dünya düzeninde Uluslararası Para Fonu (IMF), Dünya Bankası, Birleşmiş Milletler (BM), Kuzey Atlantik Antlaşması Örgütü (NATO) ve AB gibi kurumların sermayenin uluslararası çıkarlarını koruduğunu savunan (Civelek, 2005) yazarlar ulusal devletlerde yaşanan ciddi sorunları, huzursuzlukları, hukuk sisteminin rafa kaldırıldığını göz ardı etmektedirler. Her çağda toplumun davranışlarını sermaye ilişkileri şekillendirmiştir. Günümüz dünyasında da gelir dengesizliği, toplumsal kutuplaşma, savaşlar ve hem fiziksel hem de dijital dünyadaki ekonomik dengesizlik ve güvenlik gibi sorunlardan kaynaklanan huzursuzluk ulusal devletlerden kopuşu hızlandırmaktadır.

Gelinen noktada ulusal devlet temelli yönetimler ve büyük boyutlu parlamentolar artık gençlerin ve tepkili kitlelerin referans noktası olmaktan çıkmıştır. Dünyanın dört bir yanındaki toplumsal hareketler, en otokratik yönetimlerin ve silah tröstlerinin yönettiği devletlerde bile uluslararası normlara, ulusötesi anlaşmalara ve yerel uygulamalara atıfta bulunmaktadır (Mihr, 2022: 131-132). Teknolojik gelişmelerin ışığında dünya toplumunun ulusal devlet yönetiminden kurtulmak için fırsat kolladığı aşikardır. Küreselleşmenin veya başka yönetim şekillerinin daha iyi olmayacağını savunanlar ulusal devlet temelli yönetimin de iyi bir seçenek olmadığını anlamak için çaba harcamalıdırlar. Merkezi olmayan bir dijital ekosistemde güvenli bir kimlik doğrulama sistemiyle tüm kamu hizmetlerini tek bir platformda kullanıcının hizmetine sunmak hükümetle toplum arasında güven oluşturmanın anahtarı olabilir. Dijital olanaklar sayesinde hizmet kalitesinin iyileştirilmesi, zaman ve maliyet kaybının azaltılması, bilgi ve hizmet sunumu sürecinde şeffaflığın artırılması, kamu politikasının oluşumu ve uygulanması safhasında çoklu aktörlerin katılımına olan ihtiyaç e-yönetişim ekosistemini zaruri hale getirmektedir. Fakat tüm gelişmelere rağmen dünya genelinde e-yönetişim politikalarının ve uygulamalarının istenilen düzeyde olmadığı tartışılmaktadır. Özellikle internet hizmetleri sağlayan ve yapay zekâ ürünleri geliştiren teknoloji şirketleri dahil tüm paydaşlar sürece dahil edilmelidir.

Dinamik ve evrimsel bir yaklaşımla blockchain teknolojisinin yönetişime dahil edilmesi yasal anlaşmaların, oy verme işleminin ve mülkiyet haklarının otomatik olarak yönetilmesine ve olgunlaştırılmasına katkı sağlama potansiyeline sahiptir (Allen, & Berg 2020; Laatikainen, Li & Abrahamsson, 2023). Bu yaklaşımla gelişmekte olan ülkelerde kusursuz bir e-yönetişim modelinin uygulanması neredeyse imkânsız görünmektedir. Vatandaşlar, hükümetlerin dijital çağda haklarını koruyup koruyamayacağını ve nasıl koruyabileceğini ve mevcut politikaların ve yasal güvencelerin amaca uygun olup olmadığını giderek daha fazla merak etmektedir (OECD, 2022). Kapsamlı bir e-yönetişim ekosisteminin vatandaşların yaşamlarını iyileştirebileceği konusunda fikir birliği vardır. Hükümetlerin kamuoyunu ilgilendiren faaliyetleri gizli yürütmek eğiliminde olmalarına rağmen, dijital çağda karmaşıklığın devam etmesini bulunmaz bir nimet olarak görmelerine rağmen bireyler ve ilgili paydaşlar şeffaf bir e-yönetişim ekosisteminin hazırlanması için yasal yollarla her fırsatta mücadele etmelidirler.

### 1.6. Dijital Dünyada Merkeziyetsiz Yapıların Yükselişi

Yeni dünya düzeninde geleneksel kuruluşlar ve çeşitli otoriter yapılar önemini günden güne kaybetmektedir. Eski düzende basit prosedürler, çalışanlar için uygulanması karmaşık işlemler haline gelmekte ve işlerin yürütülebilmesi için çok fazla zaman ve maliyet harcanmaktaydı (Boztepe, 2018: 193-194; Polat ve Akçakaya, 2022: 250-251). Bununla birlikte basit işlemler için bile sayısız formlar ve imzalar gerekebilmekte, işlemler günlerce veya aylarca sürebilmekteydi. İçinde bulunduğumuz çağda ise BT'leri örgütlerin yapısını, işleyişini, performans ve değişimini etkileyen temel faktördür. Özel sektör ve kamu sektörü BT'den derin bir şekilde etkilenmektedir. Geçmişin ihtiyaçlarına göre oluşturulan kurumların sunduğu hizmetlerle toplumunun ihtiyaçlarını karşılamak imkânsız hale gelmiştir. Eski kurumların işleyiş biçimi sorunları çözmek yerine ilave sorunların ortaya çıkmasına neden olmaktadır. Giderek gelişen ve kullanım alanı yaygınlaşan dijital teknolojiler, birçok mesleğin uygulama alanında kendine yer bulmaktadır (Yıldırım vd., 2020: 3902). Yeni normal, geniş bant internet ve bulut destekli bilişim altyapısı üzerine inşa edilmektedir. (Aydın, 2023: 15). Yeni düzene ayak uyduran toplumlar refahlarını artırmaya devam ederken, ayak uyduramayanlar mevcut ekonomik

kazanımları dahi kaybediyorlar. COVID-19 pandemisi sürecinde dijital teknoloji kullanılarak yapılan toplantılar, uzaktan verilen dersler, çevrim içi yapılan sınavlar, dijital alışveriş platformlarından satın alınan ürünler çalışma hayatının ve yaşamın farklı bir boyutta sürdürülebileceğini alenen göstermiş oldu (Güngör, 2023).

Blockchain teknolojisiyle yapılan akıllı sözleşmeler aracıların ortadan kaldırılması için katalizör işlevi görmektedir (Bellavitis vd., 2023). Temel değişimlere bakıldığında aracı kurumların zamanla ortadan kalktığı görünmektedir. Blockchain verilerin dijital ortamda dağıtık bir yapıda, şifrelenerek, değiştirilemez bir şekilde kaydedilmesine ve transfer edilmesine imkân veren (Al-Rawy & Elci, 2021), her yeni işlemde birbiriyle ilişkilendirilen güvenli, şeffaf bir dijital kayıt defteridir. Merkeziyetsiz bir yönetişim modeli üzerine yoğunlaşan Web 3.0 uygulamalarında altyapı olarak kullanılan blockchain teknolojisi, verilerin çevrimiçi olarak sıralı bir şekilde ve dağıtık yapıda kayıt altına alınmasından ibarettir (Şenkardeş, 2023). Blockchain teknolojisiyle bireyler aracılara ihtiyaç duymadan ve herhangi bir bürokratik engele takılmadan "Peer-to-peer" (P2P) mantığıyla işlemleri gerçekleştirebilmektedirler. "Peer-to-peer" sistemi 2008 yılında asıl kimliği tam olarak bilinmeyen Satoshi Nakamoto tarafından dokuz sayfalık bir belge olarak duyurulmuştu. Bu sistemi özel ve değerli kılan onun merkeziyetsiz olmasıdır.

Blockchain teknolojisinin şeffaf bir şekilde işlemleri hızlandırması, maliyetleri azaltması gibi avantajlarından dolayı yöneten sınıfı sömürü taktiklerini değiştirmeye zorlamaktadır. Tüm düzeylerde merkezileşme ile merkezi olmayan yönetim arasındaki nihai denge, çok sayıda farklı çıkarların anlaşmaya varması gereken karmaşık bir politika meselesidir (Vrolijk ve Szajnfarber, 2015: 45). Dijital dünyada herkesin gerçekleri öğrenme imkânı olduğu için artık eski sömürü düzeninin temelleri sarsılmış durumdadır. Geleneksel imajlar ve anlatılar inandırıcılığını kaybetmiştir. Dijital platformlarda toplumun belli bir kesiminin nasıl ultra lüks hayat yaşadığını, öte yanda ise toplumun büyük bir kısmının açlık sınırının altında yaşam mücadelesi verdiğini, gerçekmiş gibi anlatılanların aslında yalan olduğunu anlamak için çeşitli kanıtlar vardır. Mevcut siyasi düzenin tam anlamıyla anayasal kılıfa uydurulmuş zorba bir düzen olduğu ve insanların korktuğu için sustuğu apaçık bilinen bir gerçektir. Gereken çözümlerin bulunması ve uygulanması dört gözle beklenmektedir. Tüm bu sorunlar göz önünde bulundurulduğunda zorba düzeni

değiştirmek için blockchain teknolojisinin birçok avantajı beraberinde getirdiği yaygın olarak kabul görmekte ve umut vermektedir (Veriter,2021). Blockchain alanında yetenekli çalışanlara yönelik talebin de her geçen gün artığı bilinmektedir.

Klasik düzende bireyler arasındaki her konuda bir aracı yer almaktadır. Vatandaşlar memnun kalmasalar dahi, başka seçenekleri olmadığı için aracı kurum ve kuruluşlardan hizmet almak zorunda kalıyorlar. Merkezi otoritelerden kurtulmak için tüm engellere rağmen çeşitli projeler gerçekleştirilmiştir. Merkeziyetsiz yapılar müşterilerin özgürleştiği ve verilerinin kontrolünün kendilerinde olduğu bir dünya olarak karşımıza çıkmıştır. Finans sistemini merkeziyetsiz bir yapıya dönüştürmek amacıyla Bitcoin geliştirilmiş, daha sonra diğer klasik sistemleri de merkeziyetsiz hale getirmek için 2015 yılında Ethereum piyasaya sürülmüştür. Bitcoin'in daha gelişmiş bir versiyonu olarak bilinen Ethereum kripto teknolojisi üzerine inşa edilmiş açık kaynaklı, merkezi olmayan bir bilgi işlem platformudur. Bu sistemle merkezi bir otoritenin katılımı olmadan taraflar arasında akıllı sözleşmelerle değer transferi yapmak mümkündür (Lumineau vd., 2021: 506; Murray vd., 2021). Ethereum gibi kripto sistemlerin kullanımı yaygınlaştıktan sonra noterlik ve benzeri kurumlara da ihtiyaç kalmayacağı anlaşılmaktadır. Bundan sonraki süreçte de Ethereum gibi kripto teknolojisi üzerine inşa edilmiş sistemlerin daha gelişmiş sürümleri ortaya çıkmaya devam edecektir. Merkezi otoritelerden ve aracılardan kurtulmanın en iyi yolu merkezi olmayan yapıların yaygın olarak kullanılmasıdır. Merkezi otoriteler dijital evrime ayak uydurmak zorunda kalsalar da mümkün olduğu kadar ellerindeki fırsatları kaçırmamak için direniyorlar. Blockchain teknolojisi üzerine inşa edilen merkeziyetsiz yapıların önemli avantajları olduğu gibi bazı dezavantajları da vardır. En büyük dezavantajlardan biri blockchain teknolojisinin en popüler hali olarak bilinen kripto paranın yasadışı eylemlerin gerçekleştirilmesi için de kullanılabilir olmasıdır. Kripto para transferleri ile ilgili bilgilerin anonimliğinin korunması terör faaliyetlerinin desteklenmesi, uyuşturucu ticareti, para kaçırmak gibi kötü amaçlı faaliyetlerin gerçekleştirilmesi için de kolaylık sağlamaktadır. Bu kapsamda ilerleyen süreçte uluslararası ölçekte çözüm üretmek oldukça büyük önem arz etmektedir.

Otonom organizasyonlar da örgütlenmeyi ve yönetişimi temelden dönüştürme potansiyeline sahiptir. Merkezi olmayan organizasyon yapısı, karar alma yetkisinin üst düzey liderliğin tekelinden orta ve alt kademe yöneticilere devredilmesine olanak

tanır. Bununla birlikte merkeziyetsiz kuruluşlarda aşağıdan yukarıya karar alma sürecinde, bürokratik engeller azaldığı için çeviklik artmaktadır. Merkeziyetsiz yapıların giderek daha popüler hale geleceği beklenmektedir. Geleneksel sistemlerin hantal yapısı, yüksek maliyetli olması, kısıtlayıcı özellikleri merkezi olmayan sistemlerin giderek gelişmesini ve yayınlaşmasını hızlandıracaktır. Veri akışının izlenebilir ve şeffaf olması nedeniyle blockchain teknolojisi fiziksel dünyadaki düzeni kökünden değiştirebilecek büyük bir potansiyele sahiptir.

### 1.7. Şeffaf Yönetim için Açık Veri Erişiminin Önemi

Şeffaflık, devletin kaynaklarının nasıl ve ne için harcandığını, kurumların ve kuruluşların iç işleyişini ve aldıkları fonların nasıl yönetildiğinin bilinmesini sağlar. Genelde az gelişmiş ve gelişmekte olan ülkelerin sorunu olarak algılanan yoksulluk ve yolsuzluk sorunu insanoğlunun var olduğu günden bugüne kadar geçen süre zarfında dünya üzerindeki tüm ülkeleri ilgilendiren önemli bir olgu haline gelmiştir (Öçal, 2023). Yoksulluğu ve yolsuzlukları azaltmak için şeffaf yönetim şekli çözüm olarak görülmektedir. Kamuoyuna hükümetin ne yaptığı hakkında bilgi sağlayarak hesap verebilirliği teşvik eden şeffaflığın temelini açık erişim verileri oluşturmaktadır. 2009 yılında Amerika Birleşik Devletleri'nde (ABD) Açık Hükümet Direktifinin yayınlanmasıyla açık veri erişimi popüler bir konu haline gelmiştir. Şeffaflık, katılım kültürü, yenilikçilik ve kuruluşlara, hükümetlere ve daha da önemlisi vatandaşlara karşı hesap verebilirlik gibi muazzam sosyal ve ekonomik değer sağlama potansiyeline sahiptir (Çaldağ & Gökalp, 2023:1).

Karmaşık bir süreç olduğundan dolayı şeffaflığın sağlanması dijital olanaklar yaygınlaşana kadar pek mümkün olmamıştır. Küresel sorunların çözülmesine yönelik planların hazırlanması ve uygulanması için ölçülebilen verilerin toplanması ve değerlendirilmesi mühim unsurlardan birdir. Veriler üzerinde toplama, sayma, gruplama, özetleme, eleme ve ayıklama gibi işlemlerin el ile veya bilgisayar ile işlenmesi sonucu enformasyona dönüştürülür (Bayraktar vd., 2022). Büyük miktarda verileri analiz ederek değerli enformasyona dönüştürmekle geçmişe dönük analizler yapmak ve ileriye dönük tahminlerde de bulunulmak mümkündür. Ekonomi, politika ve savunma gibi alanlarda rekabet, ulusal kalkınma, endüstriyel gelişme, bilimsel araştırma gibi önemli konularda, bugünün algılanmasında, geleceğin tahmin

edilmesinde büyük verinin etkisi her geçen gün artarak devam etmektedir (Jin, vd., 2015). Dijital olanaklarla, yoksulluğu ve yolsuzlukları azaltmak, iklim değişikliğinin etkisini azaltmak ve BM'nin Sürdürülebilir Kalkınma Hedefleri'nde tanımlanan diğer zorlukların üstesinden gelmek için potansiyel imkânlar mevcuttur (Diniz vd., 2022). BT'nin sunduğu imkânları kullanmadan kalkınmayı, insan haklarını, demokrasiyi tartışmak artık mümkün değil (Olga vd., 2019). Herhangi bir problemi çözmek için fırsatları ve riskleri belirlemede dijital ortamdaki verilerin önemi her geçen gün artmaya devam etmektedir. BİT Sürdürülebilir Kalkınma Hedefleri'ne ulaşmada önemli bir rol oynuyor ve aynı zamanda dijital dönüşüm sürekli olarak yeni karmaşık, belirsiz ve değerlendirmeye değer olgular yaratıyor (Diniz vd., 2022).

Vatandaşların büyük bir kısmı farklı nedenlerden dolayı yönetenlerin değişen söylemlerini, verdikleri vaatleri, ekonomi politikalarını, kendilerini etkileyen karar ve uygulamaları düzenli bir şekilde takip edip analiz edemediği için ülkelerinde ve dünyada ne olup bittiğini de tam olarak anlayamazlar. Dijital çağda çeşitli bilgi ve belgelerin dijital ortamda depolanması, istenilen zaman belirli parçaların bir araya getirilmesiyle gerçeklerin anlaşılması siyasi otoritenin işini zorlaştırmaktadır. Ve aynı zamanda propaganda yapmak isteyen trollerin amaçlarının anlaşılması için de dijital dünyada yeteri kadar ayak izleri mevcuttur. Bu koşullarda en önemli sorunlardan biri de yönetenlerin en güncel teknolojileri planlı bir şekilde kullanmalarına karşın, yönetilenlerin yüksek maliyetlerden ve vergilerden dolayı modern teknolojileri elde etme ve kullanabilme imkânlarından mahrum olmasıdır.

Bilgi edinme özgürlüğü konusunda yasal şeffaflık, hükümet bütçelerinin, harcamalarının ve vergilerinin açıklığıyla ilgili olan mali şeffaflık, kamu kuruluşlarında seçilmiş temsilcilerin açıklığıyla ilgili olan siyasi şeffaflık, bilginin yayılması ve kolektif eylemi harekete geçirmenin bir aracı olan e-şeffaflık, doğal kaynakların yönetimiyle ilgili şeffaflık mekanizmalarının etkileri vatandaşların özelliklerine, mali ve güvenlik kaygılarına bağlıdır (Chen & Ganapati, 2023). Temel yasal şeffaflık durumuyla karşılaştırıldığında, mali şeffaflık ve e-şeffaflık hükümet yolsuzluklarının azaltılmasında daha etkili bir rol oynadığı için daha çok önemsenmektedir. Uluslararası yasalara aykırı olan faaliyetler için hükümetlerin dolaylı yollarla kaynak tahsis etmesi mali şeffaflığın ve e-şeffaflığın yolsuzlukların azaltılmasında etkili olduğunu gösteren önemli bir nüanstır. Mali şeffaflık ve e-

şeffaflık, BM, Dünya Bankası, IMF ve Ekonomik İş birliği ve Kalkınma Örgütü (OECD) gibi birçok uluslararası kuruluş tarafından aktif olarak savunulmaktadır. Kapsamlı takip ve keskin caydırıcı cezalarla önemli mesafelerin katedilmesinin mümkün olduğu anlaşılmaktadır. Bütçeler şeffaf ve halkın erişimine açık olduğunda vatandaşlar ve yasa koyucular, hükümetlerinin kamu parasını nasıl toplayıp dağıttığını daha iyi kontrol edebilir ve gerekirse hesap sorabilirler (de Renzio & Wehner, 2017).

Çevrimiçi dünya, fırsatlarla dolu, uçsuz bucaksız bir alandır. Aynı zamanda, en azından üstel yayılma gücü ve bize sağlayabileceği görünür anonimlik nedeniyle değil, birçok yönden "çevrimdışı" dünyadan daha talepkârdır (Richardson & Milovidov, 2022: 26). Uluslararası düzeyde oluşturulan bir platform üzerinden dünya toplumunun yaşam kalitesini ayrıntılı bir şekilde yansıtan verilerin toplaması, analiz edilmesi, görselleştirilmesi ve yayınlanması prosesi gerçekleştirilirse özellikle gelişmemiş ülkelerde yolsuzlukların sayısını azaltmak mümkün olacaktır. Dijital dünyadaki, riskleri ve güvenlik açıklarını belirlemek, analiz etmek ve çözümler üretmek için veri merkezli mekanizmaların geliştirilmesi en uygun seçenektir (Rodríguez-Espíndola vd., 2022). Veri bilimini istatistikten ayıran şey, veri biliminin bütünsel bir yaklaşım olmasıdır (Mike, 2010). Dağınık ve karmaşık olan toplumsal teoriler yerine büyük veri kümelerini analiz edebilen algoritmalarla insanların yapamayacağı dijital kalıpları ve korelasyonları yapabilmek mümkündür.

Verileri etkin bir şekilde kullanarak devlet kurumlarından bağımsız istatistiki bilgiler ortaya koymakla adaletli bir düzen inşa etmek ve ulusal devletlerin işleyiş biçiminin şeffaflığını sağlamak mümkündür. Yasama yürütme ve yargının bağımsız olmadığı ülkelerde İstatistik Kurumu'nun enflasyon, işsizlik, kira artışı gibi pek çok başlıkta açıkladığı verilerin ve istatistik göstergelerin gerçeği yansıtmadığı bilinen bir gerçektir. Topladıkları muazzam miktarda verileri kendi çıkarları için başarılı bir şekilde kullanan Google, Amazon, Meta ve LinkedIn gibi şirketler tüm dünya vatandaşlarının da daha onurlu bir hayat yaşaması, siyasi ve toplumsal sorunların çözümü için de kullanabilirler. Veriler ve verilerden üretilen istatistiki bilgiler sadece eğitimli vatandaşlar için değil tüm vatandaşların karar vermek için kullanabilecekleri bir araç haline getirilmelidir.

Kuhn'un (1962) belirttiği gibi, bir paradigma, herhangi bir zamanda bir disiplindeki araştırmacıların önemli bir kısmı için ortak olan bilgiyi sentezleme ve dünyayı sorgulamanın kabul edilmiş bir yolunu oluşturur. Dijital ortamda ulusal devletlerini ve dünyayı sorgulamak, gerekli karşılaştırmalar yapmak, durum farkındalığı oluşturmak amacıyla bağımsız ve şeffaf istatistikler ortaya koyan paradigmalara ihtiyaç vardır. Karmaşık sorunlar tek boyutta açıklanamayacağına göre belli bir kuramsal yaklaşımla ve kavramsal çerçevede yazılı, sesli, görsel kanıtlarla birlikte birer yapı olarak incelenmelidir. Gerekli araştırmalar için dijital ortamlarda depolanan bilgi ve belgeler ölçme ve değerlendirme fırsatı sunmaktadır. Adil ve sürdürülebilir toplumsal yaşam için gerekli bilgilerin toplanması, sınıflandırılması, saklanması, paylaşılması ve raporlanması sürecinde dijital platformlar büyük ölçüde kolaylık sağlamaktadır. Örneğin veri gazeteciliği ortak çabalarla hoş ve anlaşılır bir şekilde hazırlanan veri hikayeleri hedef kitlelerin dikkatini çeken yenilikçi bir çözüm olarak uygulanmaktadır. Nitekim, iş birliği ve açık veri raporlaması, Latin Amerikalı gazetecilerin para ve güç arasındaki ilişkileri araştırarak hükümetin yolsuzluklarını ortaya çıkarmanın yolunu bulmasını sağlamıştır (de-Lima-Santos ve Mesquita, 2021'a). Bu gelişmeler, araştırmacı gazeteciliğin demokratik bir toplumu destekleyen bir denge ve kontrol sistemi olarak hizmet etmesi ihtiyacını ön plana çıkaran bir atmosferi ortaya koymaktadır (Borges-Rey, 2019).

Gündelik yaşamı kolaylaştırdığı için yaygın şekilde kullanılan büyük verinin işlenmesi, algoritmalar aracılığıyla karar verme ve yönlendirmede kullanılması beraberinde bazı kaygıları da getirmiştir (Sevda ve Sezgin, 2021). Bu noktada önemli olan yapay zekâ karar verici sistemlerini tasarlayanların dijital olanakları hangi amaçla kullanmak istedikleri sorunsalıdır. Önemli bir teknoloji olduğu kabul edilen yapay zekâ, günlük sosyal hayatı ve ekonomik faaliyetleri destekleyerek dünya ekonomilerinin sürdürülebilir büyümesine katkı sağlamakta ve çeşitli sosyal sorunları çözmektedir (Yazıcı, 2022). Morozov'a (2018) göre yapay zekâ teknolojilerini kullanarak büyük şirketler daha az harcayarak daha iyi üretecek, devletler enerji tüketimini, refahı, trafiği ve güvenliği daha iyi yönetecek, insanlar sahte haberlerle daha kolay mücadele edebilecektir.

Tarım, balıkçılık, ormancılık, gıda, ekonomi, finans, eğitim, kültür, spor, enerji, çevre, devlet ve kamu sektörü, sağlık, uluslararası sorunlar, adalet, hukuk sistemi, kamu güvenliği, nüfus ve toplum, bölgeler, şehirler, bilim teknolojisi ve ulaşımla ilgili daha faydalı kararların verilebilmesi için doğru veriler toplanmalı ve bilgisayar destekli yazılımlarla raporlanmalıdır. Dünyanın en büyük ekonomilerine sahip ülkelerin denetim ve dijital dönüşüm ile ilgili bilimsel çalışmalara daha fazla ağırlık verdiği görülmektedir. Büyük veri analizinin amacı organizasyonel karar verme ve yürütme süreçlerini geliştirmektir (Uladi & Arı, 2023). Karmaşık sorunların çözümüne yönelik gözetimli ve derin öğrenme yöntemleriyle hiper ölçekli veri setlerini toplamak ve sınıflandırmak için algoritmaların büyük ölçüde kolaylık sağladığı bilinmektedir. Özelikle son yıllarda algoritmalar kullanılarak siyasal algı yaratma, kamuoyu oluşturmak, gündem oluşturmak gibi topluma yönelik kontrol ve yönlendirme amaçlı operasyonlar gerçekleştirilmektedir (Kurnaz, 2022). Eğer hükümetler, uluslararası kuruluşlar ve büyük teknoloji şirketleri isterse algoritmalarla toplumun refah düzeyini yükseltmek için de faydalı projeler üretebilirler. Algoritmaların gücünü daha adil ve şeffaf bir dünya düzeni kurmak için kullanmak en önemli girişimlerden biri olabilir.

# İKİNCİ BÖLÜM

# DİJİTAL DÜNYA DÜZENİNDE HAK İHLALLERİ, HAK İHLALLERİNİN ETKİLERİ VE SONUÇLARI

## 2.1. Dijital Dünyada Çözüm Bekleyen Sorunlar

Dijitalleşmenin üretimden tüketime, iş ortamından ev ortamına kadar her alanda kendini hissettirdiği (İyigüngör, 2022) bir çağda dünyaya ülkelerini yönetenlerin başarısızlığından ve bencilliğinden kaynaklanan çok sayıda çözüm bekleyen sorunlar vardır. Bu bölümde ağırlıklı olarak siyasetle veya büyük teknoloji şirketleriyle bağlantılı olan dijital dünyada çözüm bekleyen sorunlara yer verilmiştir. Dijital dünyada gözetim, ifade özgürlüğü, dijital uçurum, toplumsal tabakalaşma, sansür, bilginin doğruluğu, yalan haber, siyasi propaganda için dijital olanakların kullanması, dijital dünya düzeninde itaat, direniş ve dalkavukluk, troller, botlar ve algoritmalar aracılığıyla algı yönetimi, ötekileştirme ve yankı odaları, dijital bağımlılık ve temel nedenleri, mahremiyet sorunu, uluslararası düzeyde yasal düzenlemelerin yetersizliği, ekonomik ve siyasi güç paylaşımı sorunu, hükümetlerin teknoloji şirketlerini kontrol altında tutma isteği, nefret ve ayrımcılık sorunu, kişisel verilerin toplanması ve korunmasına ilişkin sorunlar, ulusal ve uluslararası düzeyde dijital hegemonya, dijital diktatörlük, egemenlik amacıyla yapay zeka teknolojilerinin kullanımı, siber güvenlik gibi sorunlar çözüm beklemektedir. Bu sorunların hükümetlerin, büyük teknoloji şirketlerinin, sivil toplum kuruluşlarının ve bilinçli kullanıcıların iş birliğiyle çözülmesi mümkündür. Sorumluluk üstlenmesi gereken paydaşların neden harekete geçmek istemediği sorgulanmalıdır.

Dijital dünyada hak ihlallerine ilişkin yaşanan vakalarla ilgili örneklere aşağıda 2.1.1, 2.1.5, 2.1.7, 2.1.13, 2.1.14, 2.2 numaralı başlıklar altında yer verilerek nedenlerine ve sonuçlarına dikkat çekilmiştir.

### 2.1.1. Dijital Dünyada Gözetim ve İfade Özgürlüğü

Kökleri eski zamanlara dayanan gözetim olgusu akıllı cihazların yaygınlaşmasıyla zamandan ve mekândan bağımsız olarak bireyler, gruplar ve ülkeler hakkında özel bilgilerin toplanması ve çeşitli amaçlarla kullanılması

sürecidir. Lyon'a göre (2007: 14) 'gözetim' etkileme, yönetme, koruma veya yönlendirme amacıyla kişisel ayrıntılara odaklanmış, sistematik ve rutin dikkattir. Dijital gözetim devletlerin, hükümetlerin, ticari şirketlerin ve şahısların iletişim teknolojilerini kullanarak topladıkları bilgileri amaçları doğrultusunda kullanmalarıdır.

Dijital çağda kişisel bilgilerin kolay kaydedilmesi, depolanması ve dijital ortamda çeşitli amaçlar için kullanılması güç ve kontrol yapılarına olağanüstü gözetim fırsatı sunmuştur (Dolgun, 2015). Yunancada her şeyi gören göz anlamına gelen panoptikon kavramı günümüzdeki gözetim yapısını ve tekniklerini açıklamakta yetersiz kaldığı için, süreci tanımlamak için süperpanoptikon kavramı tercih edilmektedir. Yalnızca internet değil, nesnelerin interneti, bulut bilişim, akıllı aygıtlar, büyük veriyle ilgili gelişmeler ve öğrenen makineler gibi birçok gelişme panoptikon kavramının sınırlarını aştığına göre gözetimin "yeni" halini anlatmak için süperpanoptikon kavramı kullanılmaktadır (Yanık, 2017: 784).

Panoptikon, insanların kapsamlı bir şekilde izlenmesini mümkün kılan bir mimari tasarımı (hapishaneyi) ifade ediyor (Jannusch vd., 2021; Bentham, 2020). İnternet bağlantılı teknolojiler yaygınlaştıktan sonra dünya Jeremy Bentham tarafından tasarlanmış sekizgen biçimli bir yapı ve tam ortada gözetleme kulesinin bulunduğu hapishaneye benzetilmiştir. Foucault'a göre (1975: 200) panoptik mekanizma, sürekli görmeyi ve anında tanımayı mümkün kılan mekânsal bütünlükleri düzenler. Panoptikon olarak adlandırılan bu hapishane modelinin en önemli özelliği mahkumların hangi saatlerde takip edilip edilmediklerini bilmedikleri için kendilerini her zaman baskı altında hissetmeleri ve davranışlarını ona göre düzenlemeleridir. Panoptikon insanların belli mekânlarda denetim, disiplin ve gözetim altında tutulmasını sağlayan bir iktidar sistemi olarak işlev görmektedir (Eren, 2022 :70).

Dijital dünyadaki sistematik gözetim olanaklarının yönetilen sınıfa baskı yapılması, bireysel özgürlüklerinin kısıtlanması, manipüle edilmesi ve kontrol edilmesi için kullanılması ciddi bir sorun olarak devam etmektedir (Cohen, 2017; Zuboff, 2023). Dijital gözetimle daha müdahaleci devlet yapısı ortaya çıkmış ve ifade özgürlüğü bağlamında dünya açık bir hapishaneye dönüşmüştür. Hızlı teknolojik değişim nedeniyle gizliliğin yasal garantilerinin bilinen skandallarla boş

bir hayal olduğu kanıtlanmıştır. Demokratik değerlerle yönetilmeyen ülkelerde hükümetler, insan haklarını ihlal ederek biyometrik ve yapay zekâ destekli gözetleme sistemlerini kullanıyorlar (Freedom House, 2020). Ulusal devletlere güven azaldıkça gözetleme eyleminin daha sofistike bir şekilde yapılması hükümetler için önem arz etmektedir. Gözetim sayesinde otoriter hükümetler korkuyu tek tek tüm beyinlere yerleştirmiş ve gerektiğinde şantaj unsurları da devreye sokularak bireylere hükmetmek için zemin yaranmıştır. Bu uzamda gözetleme sistemlerin gelişmişlik düzeyine göre dünya genelinde Çin ilk sıralarda yer almaktadır.

Dijital teknolojileri üreten ülkeler, bir taraftan satışlardan muazzam ekonomik kâr elde ederken, diğer taraftan da bu teknolojileri gözetim amacıyla kullandıkları kanıtlanmıştır (Bauman vd., 2014). Snowden ve diğerlerinin paylaştıkları skandal belgelerde sadece ABD ile diğer devletler arasında değil, devletler arasında ve hükümetlerle bireyler arasındaki gözetim sisteminin mükemmel çalıştığı tüm dünya kamuoyuna gösterilmiştir (Snowden, 2019). Bireysel, kitlesel, yerel, evrensel olarak gerçekleştirilen gözetleme gerçeği korkunç bir silah ve kontrol aracı olarak nitelendirilmektedir. Sorunun en tehlikeli boyutu ise otoriter hükümetlerin kendilerine karşı çıkan bireyleri sistematik gözetim altına alma ve devletin imkânlarını kullanarak onların hayatını mahvetmek için sınırsız imkânlara sahip olmalarıdır. Bu durumda ulusal devlet sınırları dahilinde bireylerin güvende olmadıkları bilinen bir gerçektir. Bireyleri otoriter yönetimlerden korumak için hızlı ve etkili kararlar kabul edebilen tarafsız bir uluslararası kuruluşun faaliyet göstermesi iyi bir seçenek olarak görünüyor. Otoriter yönetimler bireyleri sindirmek ve susturmak için her türlü imkâna sahip oldukları için kurdukları düzen çeşitli manipülatif yöntemlerle yıllarca değişmeden devam etmektedir. Ulusal devlet sınırları dahilinde toplum için en uygun çıkış yolu kitlesel eylemlerin başlatılması, başka bir ifadeyle bireylerin haklarını aramak için birlikte hareket etmeleri gerekse de bu girişimler hiçte kolay değildir (Zuboff, 2019: 12-13).

Freedom House tarafından yayımlanan "Nette özgürlük 2020" raporunda (2020: 27-29) insan haklarının müdahaleci gözetimden korunması ile ilgili hükümetlerden talep olunması gereken önemli önlemler sıralanmıştır. Fakat bağımsız yargı/hukuk sisteminin olmadığı ülkelerde bu taleplerin düzenlenmesi ve uygulanması asla mümkün olmayacaktır. Ayrıca gelişmemiş ülkelerde yargı

sisteminin hantal olması nedeniyle sıradan davalar bile en iyi ihtimalle iki üç sene sonra sonuçlanmaktadır.

Dijital dünyada Facebook, Instagram, X ve YouTube gibi çeşitli platformların kullanıcıları algoritmalar aracılığıyla casus gibi gözetlemesi ve toplanan devasa miktarda verilerin çeşitli amaçlarla kullanılması çözüm bekleyen sorunlardan biridir. Bunun yanı sıra hükümetin bireyleri ve bireylerin de birbirini sosyal medya uygulamaları üzerinden gözetlediği de bilinen bir gerçektir. Gözetim endüstrisinin gelir kaynaklarından biri de ciddi insan hakları ihlaline neden olan casus yazılımlardır. En tehlikeli casus yazılımlardan biri İsrail'in NSO Grup yazılım firması tarafından piyasaya sürülen ve çeşitli amaçlar için kullanılan "Pegasus" adlı casus yazılımıdır. Pegasus yazılımının bulaştığı cihazın tam kontrolünü ele geçirme yeteneğine sahip olduğu tespit edilmiştir. Bu yazılım aracılığıyla telefonların kamerasını, mikrofonunu, ekranı, konum bilgilerini izlenmek ve içindeki verileri kopyalamanın mümkün olduğu ortaya çıkmıştır (Chawla, 2021). Pegasus yazılımı daha çok otoriter hükümetler tarafından satın alınarak gazetecilerin, muhaliflerin ve insan hakları savunucularının gözetlenmesi için kullanılmıştır (Katibah, 2023). Uluslararası Af Örgütü ve Paris merkezli kâr amacı gütmeyen medya kuruluşu olan Forbidden Stories liderliğinde yapılan araştırmalar sonucunda Pegasus müşterileri tarafından potansiyel olarak hedef alınan 50.000 cep telefonu numarasından oluşan bir listeye ulaşılmıştır. Listede aralarında pek çok tanınmış kişinin de bulunduğu 600'den fazla politikacı yer almıştır. Pegasus casus yayılımı, Washington Post muhabiri Cemal Kaşıkçı'nın Riyad yönetimi tarafından öldürülmesinin yanı sıra muhaliflere, gazetecilere ve hükümetlere yönelik bir dizi yasa dışı olayların gerçekleştirilmesinde kullanılmıştır (Kaster & Ensign, 2023).

Korona virüs hastalığı (COVID-19) nedeniyle vatandaşların biyometrik kayıtlarının kolay ve düzenli bir şekilde toplanması mevcut izleme cihazlarının daha kapsamlı bir düzeyde kullanılması için gereken yeni sofistike uygulamaların güncellenmesini de kolaylaştırmıştı (Freedom House, 2020). Biyometri ve yapay zekâ kullanan yeni gözetim teknolojilerini sıkı bir şekilde kısıtlanması sık sık gündeme getirilse de etkili bir sonuca ulaşılmamıştır. Hükümetlerin, otomatik sistemleri nasıl, ne zaman, nerede ve neden kullandıkları konusunda şeffaf olması demokratik değerlerle yönetilen ülkülerde faydalı olabilir, fakat kesin çözüm olmaz.

Gözetim korkusu, hükümetlere karşı olan güvensizlik ve hükümetlerin talimatıyla karar veren yargı sistemleri bireyleri susmaya mecbur bırakmıştır.

Dijital ortamda otoriter sistemlere karşı yapılan toplu veya bireysel eylemleri karşısına almak için hükümetler zaman zaman internete erişimin kısıtlanmasının yanı sıra sosyal medya platformlarındaki profilleri ve kanalları da engelleyebiliyor/ kısıtlayabiliyorlar. Bu tür engellemeler/kısıtlamalar ifade özgürlüğünün ve bilgi edinme özgürlüğünün önündeki en ciddi engellerden biridir. Avrupa İnsan Hakları Sözleşmesi'nin önsöz kısmında belirtildiği gibi ifade özgürlüğü yalnızca kendi içinde önemli bir hak olarak değil, aynı zamanda sözleşme kapsamındaki diğer hakların korunmasında da merkezi bir rol oynamaktadır. Bağımsız ve tarafsız mahkemelerce korunan ifade özgürlüğü hakkına geniş bir garanti sağlanmaksızın özgür bir ülke olmaz, demokrasi olmaz ve bu genel önerme inkâr edilemez (Frowein, 1997, aktaran Bychawska-Siniarska, 2018: 11).

Dijital gözetimin toplum için olumlu tarafı ise sinoptikon kavramıyla açıklanan çoğunluğun da azınlığı gözetleyebilmesidir. Toplumun, yönetenlerin yaşadıkları hayat tarzını ve yolsuzlukları izleme imkânı dijital gelişmelerin tek yönlü olmadığını ortaya koymuştur. Günümüz dünyasında her şeyin farkında olan, suskun ve huzursuz bir şekilde bekleyen büyük bir kitlenin harekete geçme potansiyeli güç ve kontrol yapılarının korkulu rüyasıdır. Tüm olumsuz koşullara rağmen vatandaşlar müdahaleci yeni gözetleme teknolojileri ile ilgili araştırmalar yaparak farkındalığını artırmalıdır. Sivil toplum kuruluşlarının, kontrolsüz veri toplamanın yol açtığı kişisel hakların ihlali konusunda halkı bilgilendirmek amacıyla yenilikçi girişimlerde bulunmaları önem arz etmektedir.

### 2.1.2. Dijital Uçurum ve Toplumsal Tabakalaşma Sorunu

Dijital bölünme olarak da tanımlanan dijital uçurum dijital çağın getirdiği yeniliklerden faydalanabilen ve faydalanamayan kesimler arasındaki uçurumu ifade etmektedir. Dijital eşitsizlik, teknoloji ve internet tabanlı gelişmelerin, enformasyon, hizmet ve kaynaklara ulaşma konusunda başat bir unsura dönüşmeye başladığı yıllardan itibaren üzerinde tartışmaların sürdüğü bir kavramdır (Fiğan vd., 2020: 2). Temel nedenleri güncel teknolojiye eşit olmayan erişim, sosyoekonomik eşitsizlikler, bireysel beceri ve motivasyonlar eşitsizliği gibi faktörlerin kombinasyonundan

ibarettir. Söz konusu eşitsizlikler gündelik yaşamda birçok eşitsizliğin de ortaya çıkmasını sağlar. Dijital bölünme en yalın haliyle bireyler, ülkeler ve bölgeler arasında bilişim teknolojilerine erişme ve teknolojinin sağladığı olanaklardan yararlanma açığıdır (Hüsnüoğlu & Öztürk, 2017: 8).

Dünya genelinde ülkelere göre internet bağlantılı güncel teknolojilerin kim veya kimler tarafından, nerede, nasıl, hangi amaçla ve ne kadar maliyetle kullanıldığı incelendiğinde dijital uçurumla gelir dengesizliğinin doğru orantılı olduğu tespit edilmiştir (Setthasuravich & Kato, 2020; Çapar & Vural, 2013; Torlak, 2020). Bu bağlamda e-katılımın önündeki en büyük engellerden biri olarak bilinen dijital uçurum eşit olmayan beceriler veya BT'ye erişim konusunda halkın dijital faaliyet ve süreçlerden dışlanması anlamına gelmektedir. Nitekim küresel Covid-19 pandemisi krizi döneminde dünya genelinde dezavantajlı öğrenciler çevrim içi eğitim olanaklarından yararlanmak için bilgi ve iletişim teknolojilerine erişemediğine göre dijital uçurum belirginleşmişti (Tutar, Tutar & Özlem, 2022; Yıldız &Akar Vural, 2020). Pandemi döneminde dezavantajlı çocuklarının çevrimiçi eğitim almak için karşılaştıkları erişim sorunları haklı eleştirilere neden olmuştu ve tüm eşitsizliklerin dezavantajlı grupların aleyhine olduğu tartışılmıştı. Dijital eğitimdeki fırsat uçurumu, eşitsizliklerin derinleşmesinde mühim rol oynamaktadır. Ülkelerin dijital eğitim eşitsizliklerini azaltmanın yollarını bulma ihtiyacı ve gelişen dünyada dijital teknolojinin eğitimde kullanımı yaygın bir girişim olarak ortaya çıkmıştı (Nerse, 2020: 434).

İlk başta dijital teknolojilerin yoksullukların ve yolsuzlukların azaltılmasına hizmet edeceği düşünülürken erişim eşitsizliğiyle totaliter rejimlere hizmet ettiği tartışılmaya başlanmıştır. Dijital uçurumu en aza indirmek için en önemli unsurlar kültür, yaşam boyu öğrenme, üretim ve yönetim olarak görülmektedir (Şengül, 2023: 36-37). Geliştirilen sofistike teknolojiler karşısında bireylerin ezilmemesi, durumun farkında olmaları ve sorumluluklarını yerine getirebilmeleri için dijital uçurumun azaltılması en önemli hedeflerden biri olmalıdır. Dünya genelinde az sayıda insan yapay zekâ, sanal asistanlar, blockchain gibi gelişmiş teknolojilerden yararlanırken geniş bir kitle için dijital olanaklar sosyal medya platformlarından ve Google'da yapılan basit aramalardan öteye geçmez. Günümüzde akıllı cihazlara sahip olmanın yanında onların kullanımı ve dijital okuryazarlık becerisi çok önemlidir. BT'ye

erişim sosyoekonomik, politik, kültürel, sosyal ve teknolojik faktörlerin etkileşimi ile şekillenmektedir (Fuchs, 2009: 41). Örneğin akıllı cihazlar için üretilen uygulamaların büyük bir kısmı yalnız ve yalnız akıllı cihazların son sürümlerini kullanarak bilgi veya hizmet almak mümkündür. Bu durumda açlık sınırının altında yaşayan kesimin akıllı cihazların son sürümünü almak için maddi gücü olmadığına göre gündelik hayatta vatandaşlara hizmet vermek amacıyla geliştirilen uygulamaları kullanma hakkından mahrum kalacaklardır. Dijital teknolojilerin güncel sürümlerine ve onları kullanım becerisine sahip olup olmama durumu "bilgi yoksulları" ya da "teknoloji yoksulları" adlanan yeni bir tabakanın ortaya çıkmasını sağlamıştır (Tayanç, 2021:144-145; Barrantes, 2007).

Tabakalaşma, toplumsal yapı ve değişim mekanizmasının anlaşılmasında hayati öneme sahip olan sosyolojik bir gerçekliktir (Murat, 2017: 294). Bireylerin kaynaklara, güce, özerkliğe ve statüye aynı şartlarda erişme imkânına sahip olmamasından dolayı toplum farklı sosyal tabakalara bölünür. Sosyal veya maddi anlamada tabakalaşma aslında bir nevi sosyal veya maddi eşitsizliği ima eder. Başka bir ifadeyle kaynaklar eşit bir şekilde ulaşılabilir olmadığı için toplumlar katmanlara ayrılır. Kültürel anlamda tabakalaşmanın ırk, sosyal sınıf ve cinsiyete dayalı olduğu kabul edilmektedir. Fakat en yaygın olarak bilinen tabakalaşma türü maddi eşitsizliklere dayanan sınıf temelli tabakalaşmadır (McLeod, 2013). Dijital erişimin gündelik yaşamda sağladığı olanakların erişilebilirlik düzeyi ülke bazında ve global ölçekte olmak üzere iki gruba ayrılmaktadır. Global ölçekte dijital uçurum ülkelerin gelişmişlik düzeyine göre farklı olduğu bilinmektedir; gelişmiş ülkelerde dijital uçurumun az, gelişmemiş ülkelerde ise fazla olduğu bulgulanmıştır. Ülke bazında dijital bölünme ise zengin/fakir, yaşlı/genç, kırsal/şehirli ve kadın/erkek arasındaki dijital bölünme olarak gruplandırılmıştır (Hüsnüoğlu & Öztürk, 2017: 18).

Refah düzeyi yüksek olan ülkelerde dijital uçurumun gelişmekte olan ve gelişmemiş ülkelere nazaran daha az olduğu bilinmektedir. Çünkü kapitalist dünya düzeninin doğasında var olan tüm eşitsizliklerin temel nedeni maddi sorunlardır. Maddi anlamda eşitsizlik kültürel sermaye, sosyal sermaye, fiziksel sağlık ve zihinsel sağlık alanında da eşitsizliklere neden olmaktadır. Buradan hareketle toplumsal tabakalaşmayı, maddi ya da simgesel ödüllere erişebilme anlamında toplumsal gruplar arasında ortaya çıkan yapısal eşitsizlik olarak tanımlayabiliriz (Murat, 2017).

Dijital çağda maddi gücü olmayan tabaka internet bağlantılı teknolojilere erişim imkânlarından mahrum kalmaktadır (Adak ve Mustafa, 2022). Özetle dijital uçurum/eşitsizlik bilgi edinme, öğrenme, fazla zaman ve maliyet kaybı olmadan hizmet alma konusunda eşitsizliğe neden olduğu için sosyal, kültürel, ekonomik anlamda da eşitsizliklerin artmasına yol açmaktadır. Kültürel sermaye bağlamında eğitim sistemi, aile, yaşam tarzı, inanç sistemi, davranış, bireyin eğilimleri, yaşam tarzı, habitus ve düşünce sistemi, farklı sosyal gruplar oluşturmaktan ziyade toplumsal hiyerarşilerin üretilmesini veya yeniden üretilmesini ve yayılmasını sağlayan araçlardır (Rasool, 2020: 490).

Dijital dünyada fırsat ve imkân eşitsizliğinin temel nedenlerine bakıldığında yolsuzlukların had safhada olduğu otoriter rejimler, tarafsız yargı bağımsızlığı sorunu, rekabete dayalı serbest piyasanın olmaması, gelir dengesizliği ve yetersiz telekomünikasyon alt yapısı çok etkili faktörlerdir. Dijital bölünme yetersiz altyapı, yüksek erişim maliyeti, zayıf politik rejimler, telekomünikasyon ağ ve hizmetlerinin verimsizliği gibi nedenlerle bilgi yoğun faaliyetlerin ekonomik ve sosyal faydalarını elde edememek olarak yorumlanabilir (Hüsnüoğlu & Öztürk, 2017: 18). Dijital uçurumun azaltılması ekonomik kalkınmadan ve kültürel sermaye birikiminin artırılmasına bağlı olduğu için kısa zamanda gerçekleştirilmesi pek mümkün olmayacaktır. Bu sorunun en azından azaltılması için uluslararası kuruluşların, büyük teknoloji şirketlerinin ve hükümetlerin ortak çözüm üretmesi gerekmektedir.

### 2.1.3. Dijital Dünyada Düşünce Özgürlüğü ve Sansür Sorunu

Düşünce ve özgürlük kavramlarından oluşan "düşünce özgürlüğü", algıların zihinde işlenmesi ve açıklanması sürecinde bağımsız olma, kısıtlama ve kısıtlanmalardan uzak olma, bir başka deyişle, özgürce düşünebilme ve ifade etme anlamı taşımaktadır (Ankaralı & Yılmaz, 2022: 281). Basit tanımıyla düşünce özgürlüğü bilgi edinirken, düşünürken ve düşünceleri açıklarken herhangi bir engelle karşılaşmamak anlamına gelmektedir. Fakat insanlık tarihi boyunca sansür ifade özgürlüğünü kısıtlayan en önemli sorunlardan biri olarak günümüze kadar devam etmiştir (Rheingold, 2000). Sansür basit tanımıyla egemen bireylerin kendilerine ve kurdukları düzene karşı tehlike arz eden düşüncelerin dile getirilmesini ve yayılmasını kısıtlamaktır. Bu sorun çağa uygun olarak her dönem farklı şekillerde

uygulanmıştır. Daha önce el yazmaları, yazılı ve görsel iletişim araçları, daha sonra işitsel ve görsel içerikler üretip yayımlayan kitle iletişim araçları sansür komisyonları tarafından denetlenmiştir. Otoriter yönetimlere karşı olan içerikler kısıtlanmış, yasaklanmış ve hatta fikir adamları vahşice katledilmiştir. Tarihte en kötü sansür örneklerinden bir de Antik Yunan filozofu Sokrates'in düşüncelerinden dolayı idam edilmesidir.

Dijital olanaklar yaygınlaştıktan sonra eski sansür mekanizmaları dijital çağın taleplerine cevap vermediği için yeni yöntemler geliştirilmiştir. Çünkü artık bireyler fikirlerini, sorunlarını otoriter yönetimlerin kontrolündeki kitle iletişim araçlarına muhtaç olmadan dijital platformlarda duyurabilme imkânına sahiptirler (Çildan vd., 2012). Bu gelişmelere karşı da yalan/sahte haber ve provokasyonlara karşı önlem almak, millî ve manevi/dini değerleri korumak, halkı kin ve nefrete sürüklemek, halkın veya devletin çıkarlarını, birliğini bütünlüğünü korumak gibi çeşitli nedenler ve yöntemlerle fikir ve ifade özgürlüğü sansürlenmektedir.

Otoriter kurumlar derinleştikçe hükümetler iktidarlarını sağlamlaştırmak için ifade özgürlüğüne yönelik tehditler ve basına yönelik kısıtlamalar da dahil olmak üzere daha fazla yöntem ve strateji kullanıyor (Andrzejewski vd., 2023: 627). Tüm yönetimler için her türlü fikrin ve özellikle kitle iletişim araçlarının kontrolü en önemli konulardan biri olmuştur. Sansürle ilgili yasalara bakıldığında hükümetlerin kamu yararını korumaktan başka hiçbir amaçları olmadığı belirtilse de uygulama aşamasında muhalif içeriklerin sık sık kısıtlanması veya yasaklanması ciddi huzursuzluğa neden olmaktadır. Giderek daha çok ülke, çocukları ve gençleri korumak bahanesiyle interneti düzenlemeye, kısıtlamaya, sansürlemeye çalışıyor (Uçkan, 2011: 106). Dijital olanakların yaygınlaşmasıyla otoriter hükümetler anlatıları sansürlemek amacıyla geliştirilen eski yaklaşımları güncellemek, yenilerini tasarlamak ve önlem almak amacıyla araçlar geliştirmek zorunda kalmıştır.

Dijital dünya aktif olarak düzenlenmekte, izlenmekte ve sansürlenmektedir. Fikir ve ifade özgürlüğünün önündeki engellerden biri de hipermedya içeriklerinin otoriter hükümetler ve büyük teknoloji şirketleri tarafından algoritmalar aracılığıyla sansürlenmesidir. Günümüzde, hipermedya içeriğini dağıtmak için kullanılan internet hizmetlerinin büyük çoğunluğu, sunuculara büyük ölçüde bağımlı olan ve çeşitli kalite ve güvenlik kaygılarına yol açan merkezi bir modeli izlemektedir (Núñez-

Gómez & Garcia-Font, 2022: 1). Web3 uygulamalarının yaygınlaşmasıyla, Bitcoin protokolünü temel alan DeScan gibi merkezi olmayan, sansüre dayanıklı bir indeksleme ve arama motoru en azından otomatik engellemelerin önüne geçebilir (de Vos vd., 2024). Ama yine de kuşkusuz otoriter hükümetler tiranlıklarını devam ettirmek için her yolu deneyeceklerdir. Örneğin Çin hükümeti tarafından yaratılan "Büyük Güvenlik Duvarı" adlı sansür ekosisteminde web siteleri yaygın olarak HTTP (Hyper Text Transfer Protocol) kullanımı yoluyla engellenir. Dijital ortamda rejimin tabiriyle "hassas kelimeler" (Ye & Zhao, 2023) filtrelenir ve akabinde içerikler engellenir, gerekirse bilgi kaynakları kapatılır/kara listeye alınır, sosyal medya hesapları kapatılır, gönderiler ve yorum bölümleri devre dışı bırakılır ve aynı zamanda dijital içerikler moderatörler tarafından kaldırılır (Andrzejewski vd., 2023: 638- 639). Bu sansürlerin yanı sıra Çin hükümeti siber saldırılar, dağıtılmış hizmet reddi (DDoS) saldırıları, kasıtlı bant daraltma, DNS zehirlenmesi (sahte sayfaları döndürme veya istenen siteyi başka bir siteyle değiştirme) alakasız bir IP adresinden içerik almak, VPN teknolojilerini engelleme ve veri dosyalarını monitör kontrol noktaları aracılığıyla incelemenin bir yöntemi olan Derin Paket Denetimi (DPI) gibi bir dizi yöntemler kullanmaktadır. Sıralanan sansür teknikleri dijital teknolojilerin gelişmesine paralel olarak geliştirilmektedir. Önemli olan kullanılan araç değil amaçtır. Bu arada Rusya'nın da Çin ile yarıştığı, zaman zaman birbiriyle iş birliği yaptıkları ve diğer otoriter hükümetlere rol model oldukları bilinmektedir. İsrail hükümeti de sansüre hizmet eden gözetim teknolojilerini geliştiren ülkeler arasında ilk sıralarda yer almaktadır. Sansür uygulamak için yapılan işlemler doğası gereği kötü amaçlıdır. Çin'deki bir araştırma ekibi, yapay zekâ kullanarak internetteki "zararlı bilgileri" %91 doğruluk oranıyla filtreleyebilen bir metin sansürü uygulaması geliştirdiğini bildirmişti (Chen, 2022). Zaten daha önce de Çin ve Rusya gibi ülkelerde yapay zekâ teknolojilerinin ve insanların sansür amacıyla kullandığı bilinmekteydi.

Günümüzde fikir ve ifade özgürlüğüne karşı ön sansür, otosansür, dolaylı sansür veya yumuşak sansür yöntemleriyle mali, yasal ve algoritmik baskı yapılmaktadır. Tabii ki gerçek anlamda dezenformasyonla mücadele amacıyla hak ihlallerine karşı toplumun yasalarla güvence altına alınması temel gereksinimlerden biridir. Fakat hükümetlerin yolsuzluklarını anlatan gazetecilerin, insan hakları ve

demokrasi aktivistlerinin veya siyasi düzene karşı haklı eleştiriler yapan bireylerin bu yasa kapsamında kısıtlanması veya engellenmesi yaygın olarak bilinmektedir. Yani hükümetler bir taraftan dijital hakları yasal güvence altına aldıklarını iddia ederken diğer taraftan da bireylerin haklarını ihlal ettikleriyle ilgili eleştirilerle karşı karşıyadırlar. Aslında tüm otoriter yönetimlerin amacı hükümet yanlısı trollerin de aktif katılımıyla ve mevzuatla otosansür mekanizmasını devreye sokmaktır. Dijital dünyada sansürün çoğu yayınlanmadan önce gerçekleşmektedir. Uzun bir ortak evrim süreci boyunca netizenler ve sansür sistemi birbirini şekillendirmektedir (Ye & Zhao, 2023: 8). Otosansür bireylerin bilinçli ya da bilinçsiz kararlar verirken neyin politik olduğuna dair anlayışlarını, duyarlılık duygusunu, bir konuyu ele alıp almama veya nasıl ve hangi üslupla dile getirmeleri konusunda bir fren rolü oynamaktadır. Çevrimiçi gözetim, içeriği doğrudan sansürlemese de gözetlendiklerini bilen ve tepki olarak davranışlarını değiştirebilecek bireyleri korkutmaya hizmet eder (Andrzejewski vd., 2023: 640). Yumuşak sansür olarak da bilinen dolaylı sansür, ifade özgürlüğü bağlamında içeriği doğrudan yasaklamadan kısıtlamanın bir yoludur. Otosansür politikalarının gerçekleştirilmesi ve etkisinin artırılması için bilim insanlarının da katılımıyla kapsamlı araştırmalar, analizler yapılmakta ve devasa miktarda maddi kaynaklar harcanmaktadır (Linvill vd., 2022; Feng & Guo, 2013). Büyük teknoloji şirketleri ve çeşitli yatırımlar yapan şirkeler hükümetlerin cezalarından ve para cezalarından kaçınmak için sıklıkla otosansür uygulamak zorundadırlar. Dünyanın dört bir yanında otoriter hükümetlerin amaçlarına uygun olarak otosansür uygulayamayanlara çeşitli cezalar verilmektedir.

Kurdukları düzenin devam etmesi için devletin tüm imkânlarını seferber eden hükümetler iletişim ve bilgi akışını kontrol etmek için harcadıkları enerjinin ve kaynakların küçük bir kısmını bile devletin kalkınması için harcamamaktadır. Sonuç olarak halk günden güne fakirleşirken yöneltenler zenginleşmeye devam ediyorlar. Dijital dünyadaki sansür sorununu ele alan çalışmalarda sansür hükümetlerin, vatandaşların çevrimiçi aktivitelerini kontrol etme, serbest bilgi akışını kısıtlama ve bu bağlamda çevrimiçi kullanıcıların ifade özgürlüğünü ihlâl etme uygulamaları olarak tanımlanmaktadır (Tekeli, 2021: 165-166). Örneğin, Nikaragua'nın 2020 yılındaki kabul ettiği yasaya göre (madde 28) "bir kişinin onuruna veya prestijine iftira atmak veya bir kişinin sırlarını ifşa etmek" amacıyla teknoloji kullanımı

suçundan iki ila dört yıl hapis cezası öngörülmektedir. Böylece kısıtlamaların yasal mevzuatlar yoluyla da uygulanabilmesi için ek hareket alanı sağlandığı görülmektedir. Genel olarak otoriter rejimlerde, dijital içerik sansürünün en temel biçimlerinden biri sosyal dışlanma riskinin yanı sıra web sitelerinin engellenmesidir. Aynı zamanda otoriter yönetimler sadece ülke sınırları dahilinde kendilerine karşı olanları kısıtlamak, tehdit etmek ve hapse atmakla kalmaz muhaliflerin yurtdışında yaşayan aile üyelerini de kısıtlamak için de her türlü yola başvurdukları bilinmektedir.

Günümüzde sansür yaşamın her alanında teknik güçlüklerin arkasına gizlenmiştir. Özelikle telefonların dinlemesi, izlenmesi ve diğer dijital sansür biçimlerinin uygulanmasıyla birlikte troller, botlar ve hükümet yanlısı kullanıcılar dijital ortamda muhalif anlatıları bastırmak için çeşitli yollar buluyorlar. Günümüzde dijital medya sahiplerinin satın alınması veya korkutularak susturulması da bilinen sansür yöntemlerinden biridir. Gazetecilerin tutuklanması veya acımasızca katledilmesi de bir çeşit sansürdür. Yetkili kurum ve kuruluşlar teknik altyapı konusunda yatırım yapmaması ve özellikle kırsal alanlarda insanların internet kullanma imkânlarının ellerinden alınması da bir çeşit sansürdür. Hala dünyayı nüfusunun yaklaşık %30'u hiçbir şekilde internet kullanım hakkına sahip değildir, kalan yüzde %70'in de en azından yüzde %35'nin limitsiz ve kaliteli internet bağlantısına sahip olmadığı tahmin edilmektedir. Sansür, demokratik olmayan rejimlerin kullanabileceği tek yol değildir (Saka, 6 Haziran 2022). Alternatif olarak, bilgileri sansür yoluyla azaltmak yerine dikkat dağıtıcı enformasyon bolluğu yaratmak ve arama sonuçlarını gizlemek gibi daha incelikli yöntemler kullanıcılar tarafından daha az fark edildiğine göre tercih edilmektedir (Roberts, 2018). Uygulanan çeşitli sansür yöntemlerinden hükümetlerin dijital ortamdaki muhalefeti engellemek amacıyla her yolu denedikleri anlaşılmaktadır.

### 2.1.4. Yanlış Bilgi ve Dezenformasyon Sorunu

Sorunlu bilgiler yayınlanma niyetine göre iki kategoriye ayrılmaktadır; yanlış (misenformasyon) ve yanıltıcı (dezenformasyon) bilgiler. Yanlış bilgi yanlışlığı kasıtsız olan, yanıltıcı bilgiler ise kasıtlı olarak yayımlanan içeriklerdir. Dezenformasyon, kasıtlı olarak yanlış veya yanıltıcı olan bilgidir (Jack, 2017: 3).

Kapsamına ve hedefine göre dezenformasyon girişimleri farklılık göstermektedir. Elbette yalan söylemek ve yaymak yeni bir şey değil, ancak yanlış veya yanıltıcı bilgilerin kasıtlı olarak yayılması geçtiğimiz yüzyılda yeni teknolojilerin etkisiyle patlama yaşamıştır (O'Connor & Weatherall, 2019). Kimi zaman dezenformasyon kampanyaları çok sayıda sosyal medya hesapları, video kanalları ve internet siteleri üzerinden kapsamlı ve koordineli bir şekilde yürütülürken kimi zaman da küçük boyutta gerçekleştirilir. Demokratik süreçler de dezenformasyonun büyük ölçekli ve sistematik yayılması nedeniyle giderek daha fazla zorlanmaktadır (Against Disinformation, 2018). Dijital siyaset çağında dezenformasyon dijital ortamdaki bir çeşit virüs gibidir. Bulaştığı yerlerden temizlenmesi kolay değildir. Toplumun dijital dünyadaki yanıltıcı bilgileri ayırt edebilmesi, ihbar edebilmesi ve yayamaması için sürekli bilinçlendirilmesi gerekiyor. Yanıltıcı bilgilerin kasıtlı olarak oluşturulmasına ve paylaşılmasına yönelik caydırıcı cezaların verilmesi, etkili ve kapsamlı proaktif yasal çerçevelerin geliştirilmesi ve uygulanması yalnız uluslararası bir anlaşmayla mümkün olabilir.

Açık dezenformasyonların genellikle hükümet destekli medya tarafından yürütüldüğü bilinmektedir (Wilson & Starbird, 2020). Hem fiziksel hem de dijital dünyada yarattığı sorunlarla sürekli gündem olan Rus yönetimi koordineli dezenformasyon kampanyalarının yürütülmesinde de dünya ülkeleri arasında ilk sıralarda yer almaktadır (Jack, 2017; Against Disinformation, 2018: 3; McFaul, 2019; Pacheco vd., 2020). Art niyetli hükümetler ve bireyler siyasi, ırksal ve ekonomik ayrımları derinleştirmeye çalışarak toplumun bakış açılarını çıkarları doğrultusunda değiştirmeye çalışıyorlar. Yanıltıcı içerikler, küresel ölçekte çeşitli aktörlere hizmet ettiğinden, yabancı ve yerli dezenformasyon arasındaki ayrım ve kamu diplomasisi ile propaganda arasındaki ince çizgiyi bulanıklaştırmıştır. Son on yılda hükümetlerin politikalarının çoğu, başta Rusya olmak üzere yabancı, devlet destekli dezenformasyona odaklanmıştır (Veriter, 2021: 1). Koordineli gruplar tarafından kullanılan düzinelerce hesaplardan yanıltıcı içeriklerin paylaşılması titizlikle tespit edilip önlem alınsa da topluma vereceği zarar uzun zaman alabilmektedir.

Hükümetler veya siyasi kurumlar tarafından belirli bir seçimi, ideolojiyi veya bakış açısını desteklemek veya ona meydan okumak amacıyla üretilen yanıltıcı

bilgiler kitlesel propagandaya dönüşebilmektedir. Son dönemde yanlış bilgilerin etkileri ve sonuçları küresel barışa tehdit oluşturabilecek boyutlara ulaşmıştır (Stewart, 2021). Bu nedenle dijital çağın çarpıtma, pazarlama ve düpedüz yalanların çağı olduğu tartışılmaktadır. Dezenformasyon operasyonlarında genellikle botlar kullanılarak algoritmik güçlendirmeye dayalı olarak duygusal tepkileri tetiklemek için tasarlanmış mesajların hızla yayılması sağlanır (Veriter, 2021). Dezenformasyon yayanlar çoğu zaman art niyetini belli etmeden botları, trolleri kullanarak amacına ve hedefine yönelik yanıltıcı içerikler paylaşmaktadırlar (Echendu, 2021). Ayrıca çevrimiçi platformlar, reklam verenler ve reklam endüstrisi, dezenformasyon sorununun üstesinden gelmede önemli bir role sahiptir; çünkü sorunun ölçeği, platformların kötü niyetli aktörlerin dezenformasyon mesajlarını yükseltme, hedefleme ve yayma yeteneğiyle doğrudan ilişkilidir (Against Disinformation, 2018). Bazı kullanıcıların da farkında olmadan dezenformasyon yayarak bu tür faaliyetlere katkı sağladıkları da bilinmektedir.

Dezenformasyonla ilgili başka bir sorun ise politikacıların medya kurumlarını yalan haber yapmakla suçlamasıdır. Geçtiğimiz on yılda dünyada meydana gelen pek çok sosyal hareket ve seçim süreçleri ulusal ve ulusüstü aktörlerin dijital alandaki mücadelesine sahne olmuştur (Kurnaz, 2022: 1). Örneğin yalan/sahte haber anlamına gelen “Fake news” kavramı 2016 yılında ABD’deki başkanlık seçimleri sırasında Donald Trump tarafından sık sık kullanıldıktan sonra moda bir kavram haline gelmişti. Hükümetlerin, siyasi kuruluşların, politikacıların ve bireylerin kendilerine karşı olan doğru haberlere bile çoğu zaman “fake news, deepfake, montaj veya şantaj” deyip kurtulmaya çalıştıkları sık sık haberlere yansımaktadır. Otoriter eğilimlere sahip hükümetler, kendileri siyasi muhaliflere karşı ötekileştirmek amacıyla dezenformasyon yayarken, rejimlerine karşı olan haber kaynaklarını dezenformasyonla mücadele kapsamında cezalandırıyorlar. Art niyetlerinden dolayı samimi olmadıkları yaygın olarak bilinmektedir.

Sahte haber furyasının sorumluluğu arama motorları ve sosyal medya ağları olarak bilinir, fakat kullanıcılar da bu olaya derinlemesine dahil oluyorlar. Çünkü kullanıcıların davranışları ve inançları yeni medyanın işleyişi için temel teşkil ediyor. Avrupa Komisyonu’nun Dijital Hizmetler Yasası (DHY) ve Dijital Pazarlar Yasası (DPY), platformların şeffaflığını ve hesap verebilirliğini ve ayrıca araştırmacıların

verilere erişimini artıracak yeni önlemler önermektedirler (EDRİ, 2020), ama dezenformasyona karşı mücadele sadece sözlü taahhütlerin yanı sıra gerekli eylemlerle de desteklenmelidir.

Yerli ve yabancı dezenformasyonla mücadele etmek amacıyla hükümetleri ve teknoloji şirketlerini etkili çözümler geliştirmeğe mecbur bırakmak için kullanıcıların dijital haklarına odaklanmaları gerekmektedir. Gelinen noktada yapay zekâ, iş dünyasında ve dünya genelinde olumlu anlamda köklü değişimler yaratmanın yanı sıra yapay zekâ destekli sosyal botların insanlara yanlış bilgi vererek manipüle etmesi gibi zorluklar da yarattığı bilinmektedir (Hajli vd., 2022). Bu zorlukları dünya toplumunu derinden etkileyerek çatışma ortamı yaratmaktadır. Yapay zekâ teknolojilerinin desteğiyle oluşturulan veya yayılan zararlı içerikleri kısıtlayan veya yasaklayan katı düzenlemelerin yapılması en azından sorunları azalta bilir. Bu konuda AB önemli rol üstlenerek zararlı yapay zekâ içeriklerinin kontrol altına alınması amacıyla çaba harcamaktadır. AB'nin hazırladığı yasal düzenlemelerle teknoloji şirketlerinin dünya toplumunun yararına kararlar kabul etmek zorunda kaldıkları da zaman zaman görünmektedir. Örneğin Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok, X'in de aralarında bulunduğu önde gelen 20 teknoloji şirketi tarafından 2024 seçimlerinde zararlı yapay zekâ içeriklerini tespit etmek ve karşı koymak için birlikte çalışma konusunda anlaştıklarını beyan etmişler (MSC, 2023). Beyan niteliğinde olan anlaşmanın taahhütleri yapay zekâ tarafından oluşturulan zararlı içerik, dezenformasyon ve silahlanmanın tanımlanması açısından inceliklerden yoksun (Csernatoni, 2024) olsa da ufuk açıcı niteliktedir. Büyük teknoloji şirketlerinin bu tür kararlar almak zorunda kalmasında AB tarafından oluşturulan yasal çerçevelerin ve bilim adamlarının büyük etkisi olduğu bilinmektedir. Dijital dünyadaki hak ihlallerinin mevcut olduğunu ve karşısının alınması için büyük teknoloji şirketlerin sorumluluk üstlenmesi umut vericidir. Bu yönde daha fazla toplumsal talepler ileri sürülmeli ve tüm paydaşlar tarafından desteklenmelidir.

Dezenformasyonun oluşturduğu tehdide karşı toplumsal dayanıklılığın artırılması için kamuoyunun daha fazla bilinçlendirilmesi şarttır (Against Disinformation, 2018). Çünkü artık dijital teknolojilerin çoğalması ve medya sahipliğinin ve içerik oluşturmanın demokratikleşmesiyle birlikte sahte haberler,

yanlış bilgilendirme ve dezenformasyon inkâr edilemez bir şekilde toplumun her dokusuna nüfuz etmiştir (Dame Adjin-Tettey, 2022). Yanlış bilgi ve dezenformasyonla mücadele edebilmek için teknoloji şirketlerinin, hükümetlerin ve bilinçli kullanıcıların uluslararası bir kurumun kontrolünde koordineli bir yaklaşımla kapsamlı bir şekilde mücadele etmeleri gerekmektedir. Hükümetin tüm birimlerinin (hibritle mücadele, siber güvenlik, istihbarat ve stratejik iletişim toplulukları, veri koruma, seçim, kolluk kuvvetleri ve medya yetkilileri dahil) birleşerek dezenformasyona karşı birlikte mücadele etmeleri önerilmektedir (Against Disinformation, 2018: 5). Lakin özelikle gelişmemiş ülkelerde hükümetler yanlış bilgi ve dezenformasyonla mücadele eder gibi görünseler de kendileri yasaları kolaylıkla çiğnemeye alışıktırlar. Bu durumda devletin imkânlarını istedikleri gibi kullanan ve insanların haklarını ihlal eden hükümetleri yalnız ve yalnız ulusüstü kuruluşlar dizginleye bilir.

### 2.1.5. Siyasi Propaganda İçin Dijital Olanakların Kullanılması

Latince kökenli olan propaganda kavramı herhangi bir söylemin, fikrin veya ideolojinin hedef kitleyi psikolojik olarak etkilemek amacıyla yaygınlaştırılması anlamına gelmektedir. Propaganda bugünkü anlamıyla ilk kez Antik Yunan sofistleri tarafından söz söyleme sanatı çerçevesinde uygulanmıştır (Gürgen, 1990: 135-136). Propaganda daha çok kamuoyunun yönetenler tarafından yönlendirilmesi ve kontrol edilmesi anlamında hafızalara kazınmıştır. Siyaset bilimi literatürüne göre her siyasi adayın başarısı, onun siyasi mesajlarına ve propagandasına bağlıdır (Abudu vd., 2023). Devletler propagandayı, halklarını veya o ülkede yaşayan etnik grupları etkileyip, onlar üzerinde baskı kurmaya yönelik kullanabilmektedir (Özer & Kartal, 2023). Yönettikleri ülkelerin sınırları dahilinde sınırsız güce sahip olan otoriter hükümetler istedikleri zaman sansürün yanı sıra, medya kuruluşlarını rejimlerini öven veya yücelten haberler yayınlamaya mecbur edebilirler. Fakat doğrudan hükümeti öven veya yücelten propaganda halk nezdinde etkili olmadığı için bu yöntem mümkün olduğu kadar tercih edilmemektedir. Bu nedenle rejimler de kamuoyunu yönlendirmek için yumuşak propaganda yöntemlerini kullanmaya üstünlük verirler. Yumuşak siyasi propagandaların yapılması ve yaygınlaştırılması için muazzam dijital olanaklara sahip olmalarına rağmen otoriter yönetimler kaba ve

ağır propaganda yöntemlerine de başvurmaktadırlar. Kaba ve ağır propaganda yöntemleri muhalefeti caydırabilir, halkı korkutabilir ve kısa vadede rejimin yönetimini kolaylaştırabilir. Ancak kaba ve ağır propaganda yöntemleri devletin meşruiyetini ve halkın memnuniyetini aşındırarak rejimin uzun vadeli beklentilerini kötüleştirebilir (Huang, 2018).

Hükümetler milyonlara ulaşmak için İnternet'in anonimliğinden, sosyal ağların mikro profil oluşturma yeteneğinden ve koordineli hesap ağlarını otomatik olarak oluşturma ve yönetme kolaylığından yararlanıyorlar (Martino vd., 2020). Günümüzde izleyicileri gerçeklik diye bir şeyin olmadığına ikna etmek amacıyla propaganda gerçekliğin kendisine savaş açmıştır (Saka, 2022). Bu olgunun dozu halkı ülkelerinin geliştiğine inandırmağa çalışan hükümetler tarafından kaçırılmıştır. Milliyetçilik duygularının tetiklenmesi, dijital platformlardaki düzensizlik otoriter hükümetler için can simidi niteliğindedir. Ülkeyi yekpare bir bütün olarak temsil etmek ve vatandaşlarının temsiliyetini göz ardı etmek, milliyetçiliğin kalbinde yatan ikili düşüncenin kilit bir bileşenidir (Zhang, 2020: 165). Ancak gelinen noktada toplumu yönetebilmek için sadece milliyetçilik enstrümanı değil tüm kültürel değerlerin propagandası yapılmaktadır.

Büyük verinin dijital siyasetteki temel işlevi propaganda makinesinin seçmenlerin algı ve ilgilerine yönelik içeriklerle çok daha verimli işlemesini sağlamaktır (Kurnaz, 2022: 20). Propaganda sürecinde botlar hem demokratik hem de demokratik olmayan toplumlarda aktif bir şekilde kullanılmaktadır. Robot kelimesinin kısaltması olarak tanımlanan botlar, bilgisayar veya yazılımlar üzerinde herhangi bir aktiviteyi yerine getirme özeliğiyle otomatik çalışan yazılımlardır (Amanzholova vd., 2019). Bot aktivizminde botlar, dijital aktivizm eylemlerini desteklemek veya bozmak için kullanılmaktadırlar (Zinderen, 2021:109). Botların bazı yararlı işlevleri olsa da son yıllarda daha çok demokratik süreçleri manipüle etmek gibi kötü amaçlar için de kullanıldıkları yaygın olarak bilinmektedir. Bot aktivizmine ilişkin mevcut literatür, botların kamusal söylemi olumsuz etkilediğini, ağırlıklı olarak birbirlerini ve kendi kamplarındaki diğer kullanıcıları retweetlediklerini ve sıklıkla olumsuz ve nefret dolu duyguları ifade ettiklerini göstermiştir (Keller & Klinger 2019; Duan vd., 2022; Kermani vd., 2023). Bununla birlikte, Twitter (X) üzerinde gündem olan bir konu veya aktivist bir hareket muhalif

gruplar tarafından botlar aracılığıyla manipüle edilebilmekte veya engellenebilmektedir (Zinderen, 2021:109).

Bazı siyasi rejimler, muhalifleri susturmak ve resmi devlet mesajlarını iletmek, seçimler sırasında oyları etkilemek ve eleştirmenleri, insan hakları savunucularını, sivil toplum gruplarını ve gazetecileri karalamak için botları kullanıyorlar (Woolley & Howard, 2018). Öte yandan diğer devletlerin iç politikalarını değiştirmek amacıyla dezenformasyonun bilişimsel propaganda amacıyla kullanılması 2016 ABD ve 2017 Fransa başkanlık seçimlerinden sonra önemli bir araştırma konusu haline gelmişti. Rus hükümeti başlattığı bilişimsel propaganda kampanyasıyla 2016 ABD ve 2017 Fransa başkanlık seçimleri sırasında oyları etkilemeye çalışmıştır (Zhang vd., 2021; Lemke & Habegger, 2022). Ayrıca 2020 yazında ABD'deki #BlackLivesMatter (BLM) protestolarının Rus hükümeti tarafından körüklenmesi de sosyal medya üzerindeki nüfuz operasyonlarına dikkat çekmişti (Bradshaw vd., 2023). Manipülatif algoritmalar, "trash-streaming", "post truth", "deep fake", yankı fanusu gibi sorunlar propagandanın doğasını daha da karmaşık hale getirmiştir. Kişiselleştirilmiş propaganda yöntemleriyle içerikler kişinin ilişki durumuna, eğitimine, kariyerine, sosyal yaşamına, politik aktivizmine, modaya, dil stiline göre şekillendirilebilmektedir (Saka, 2022). Özetle son yıllarda global bir sorun olan bilişimsel propagandanın yükselişe geçtiği ve demokratik süreçleri olumsuz etkilediği bilinmektedir.

Howard ve arkadaşları (2023) bilişimsel propagandayla ilgili yaptıkları çalışmada algoritma önyargısına, manipülasyona ve yanlış bilgiye karşı mücadele etmek amacıyla uluslararası bir bilimsel iş birliği çerçevesinde Uluslararası Bilgi Ortamı Paneli'nin (IPIE) oluşturulmasını savunmuşlar. Siyasi propaganda amacıyla dijital olanakların nasıl kullanıldığı ve dikkat dinamiklerini nasıl etkiledikleri ile ilgili toplumun bilinçlenmesi önem arz etmektedir.

### 2.1.6. Dijital Dünya Düzeninde İtaat, Direniş ve Dalkavukluk

Aile, eğitim, hukuk, siyaset ve din gibi kurumlarda itaat çok etkili bir olgudur (Odabaşı, 2021: 74-75). Otorite tarafından komuta edilen birey veya toplum normalde itaat eder. İtaat, sosyal hayatın içinde her zaman her yerde vardır ve toplumsallığın kaçınılmaz bir özelliğidir (Milgram, 1963, aktaran Yükselbaba, 2017).

Bir nevi otosansür rolü oynayan itaat olgusu bireylerin içgüdülerini veya özgürlüklerini kısıtladığı için otoritelerin özgürlük alanını genişletmektedir. Mecbur kalmadığı sürece itaat etmek bireyin doğasına aykırıdır. Weber'e göre otoriteye itaati oldukça güçlü umut ve korku duyguları belirlenmektedir. Ülkelerin siyasi koşullarına göre bireylerin korkuya dayalı itaat düzeyi farklılık göstermektedir. Tarihi tecrübemiz, itaatin erdem sayılıp ödüllendirildiği, itaatsizliğin ise erdemsizlik addedilip cezalandırıldığına işaret eder (Odabaşı, 2021:33).

Ülkelerin gelişmişlik düzeyine göre korkuya dayalı itaate karşı direnç düzeyi değişiklik göstermektedir. Son zamanlarda aile, eğitim ve din gibi kurumlarda itaat eyleminin azaldığı gözlemlenmektedir (Fleming, 2005; Glaser, 2018). Aile, eğitim ve din gibi kurumlarda itaatin eskiye nazaran azalmasında bireylerin farklı ülkelerde ve kültürlerde yaşam koşullarını/standartlarını dijital dünyada izleme ve özenme olgusu önemli rol oynamaktadır. Artık eskisi gibi şiddet veya zorbalık içeren olayları saklamak pek mümkün değil ve bireysel anlamda evrensel insan ve hayvan haklarının ihlali sosyal medya platformlarında ciddi tartışmalara/tepkilere yol açabilmektedir (Fernandes vd., 2020). Bu gelişmeler şiddete ve zorbalığa meyilli veya alışkın olanları çekindirmektedir. Aynı zamanda sevgiye, saygıya dayalı ve menfaat karşılığında itaatin veya dalkavukluğun da yaygın olduğu bilinmektedir.

Hukuk ve siyaset alanında özellikle antidemokratik ülkelerde korkuya dayalı çıkar amaçlı itaat/dalkavukluk/pohpohlama/yalakalık olgusu artarak devam etmektedir. İtaat, bireysel eylemi politik amaca bağlayan psikolojik mekanizmadır (Milgram, 1963: 371). Lidere yönelik ritüelleştirilmiş pohpohlamanın varlığı antidemokratiktir veya otoriter bir kişilik kültüdür (Danziger, 2021). Dijital dünyada gelişmiş gözetim teknolojileriyle bireylerin takip edilmesi ve hükümetler tarafından devletin imkânlarıyla cezalandırılması bireyleri susmaya, itaat etmeye ve dalkavukluk etmeğe mecbur bırakmıştır. Bu uzamda, gündelik gözetim giderek yoğunlaşarak sistematik bir süreç halini almakta ve iktidarın, bireyler üzerindeki hegemonyasını ve hedonizme dayalı denetim işlevini kolaylaştırmaktadır (Okmeydan, 2017: 62). Zorunlu pohpohlama, müzakereye dayalı karar alma ve hesap verebilirliğin demokratik ilkelerini altüst eder (Danziger, 2020).

İnsanlığın uzun ve kasvetli tarihini düşündüğünüzde, isyan adına işlenenden çok daha korkunç suçların itaat adına işlendiğini görülmüştür (Milgram, 1963: 371).

Dünya tarihinde milyonlarca insanın çeşitli işkencelerle katledilmesi aslında sadece emir veren otoritelerin suçu değildir, itaat edip emirleri uygulayan bireyler de suç ortağı olmuştur. George Orwell 1984 romanında 'düşünce polisleri'nin toplumu sürekli gözetleyerek üzerinde uyguladığı baskı mekanizması ile iktidarın aleyhinde düşünüp davranmanın suç kabul edildiği kültüre dikkat çekmiştir (Dağ, 2020: 110-116). Günümüz dünyasında totaliter toplum yapısı içerisinde bireylerin hükümet ve büyük teknoloji şirketleri tarafından sistematik bir şekilde aralıksız gözetlenmesi, dijital ayak izlerinin her zaman internette ulaşılabilir olması, korkuya dayalı itaat ve dalkavukluk eğilimlerini pekiştirmektedir. Dijital vatandaşlık özellikle ticari ve devlet temelli aktörlerin müdahalesine karşı savunmasız görünmektedir (Pangrazio & Sefton-Green, 2021: 23). Kamusal alanın tamamen yok olması, sosyal platformlarda gündemin daha çok dedikodu ve gereksiz bilgilerle işgal edilmesi de bir nevi itaat anlamına gelmektedir.

Ülke sınırla içinde direniş göstermek pek kolay olmadığı için bölgesel ve küresel endişeler yaratan konulara karşı protestolar daha çok sınırların ötesinde ve vatandaş olmayanlar tarafından gerçekleştiriliyor (Cooke, 2021). Bu şekilde itaatsizlik ulusötesi itaatsizlik olarak tanımlanmıştır. Ülke sınırları içinde toplumun bir kısmı hükümetle iyi geçinmek için çeşitli yollara başvurmaktadır. Örneğin güçlü olanların yanında yer alabilmek için yalakalık/dalkavukluk yapmak, onlarla birlikte fotoğraflar çektirip paylaşmak basit bir ifadeyle bencil ve amacı beli olan davranışlardır. Dijital dünyada güçlü olanların yanında görünmek istemek ve yalakalık yapmak zaafı da otoriteye itaat etmenin bir türüdür. Liderlere, yöneticilere "reis, kral" gibi lakaplar takmak, alakasız benzetmeler yapmak, alakasız nitelikler atfetmek ve yanıltıcı övgüler yağdırmak da dalkavukluk türleri arasındadır.

Dalkavukluk/yalakalık veya pohpohlama çağında yaşadığımıza dair ifadeler kesinlikle yeni değil. Bu fenomen demokratik değer ve süreçlerle bağdaşmasa da çeşitli amaçlarla çağlar boyunca siyasi söyleme eşlik etmiştir (Danziger, 2021). Dalkavukluk ve pohpohlama insanlarda daha fazla heyecan yarattığı için dalkavuklukla nezaket arasındaki ince çizgi göz ardı edilmektedir. Bu olgunun etik bir davranış olmamasının bilinmesine rağmen yapılan araştırmalara göre insanların %95'inde işe yaradığı tespit edilmiştir (Nasr Esfahani, 2011).

Bazı toplumların geri kalmışlığı ekonomik sermayenin eksikliğinden değil, övülmekten hoşlanan, dalkavukluktan hoşlanan, ahlaki bağlılığı olmayan otoritelerin varlığından kaynaklanmaktadır (Hasanzadeh & Shakeebaee, 2023: 60). Ezop'un "Tilki ve Karga" masalında dalkavukluğun kötü niyetle yapıldığı ve bir şey elde etmek için stratejik olarak diğerinin kibrini tatmin ettiği bir etkileşim olduğu anlatılır (Danziger, 2020). Gözetim olgusu, iktidarın kendi hegemonyasını kurup güç elde etmek ve elde ettiği gücü koruyarak geliştirmek üzerine kurulu araçsal bir süreci tanımlamaktadır (Okmeydan, 2017: 54). Otoriter rejimlerde dijital gözetim sofistike bir şekilde arttıkça itaat ve dalkavukluk eğilimi de artmaktadır, direniş ise tam tersi olarak azalmaktadır. Dalkavukluğun manipülatif olduğu, etik bir davranış olmadığı ve sosyal açıdan toplum için olumsuz sonuçlar doğurduğu algısı pekiştirilmelidir.

### 2.1.7. Troller, Botlar ve Algoritmalarla Algı Yönetimi

Dijital teknolojiler dünya toplumu için birtakım faydalar sağladığı gibi zararlı eylemlerin gerçekleştirilmesi için de muazzam fırsatlar sunmaktadır. Hükûmetler propaganda amacıyla güncel teknolojileri, trolleri veya isimsiz hesapları ve botları koordineli bir şekilde kullanmak için her türlü imkâna sahip olduğuna göre yönettikleri toplumlardan kat kat avantajlı konumdadırlar. Merriam-webster sözlüğünde trol "kışkırtıcı, alakasız veya saldırgan yorumlar veya diğer rahatsız edici içerikler yayınlayarak çevrimiçi ortamda kasıtlı olarak başkalarını kızdıran kişi" olarak tanımlanmıştır. Trol ağları çevrimiçi söylemi manipüle etmek amacıyla yalan ve sahte haberleri yayarak, muhalif olanlara küfür ve hakaret ederek hedeflerine ulaşmak için uğraşırlar.

Tarih boyunca iletişim teknolojileri statükoyu rahatsız eden sosyal ve kültürel değişimlerin ateşleyicileri olmuştur (Hermida, 2017). Bu bağlamda dijital dünyada ifade özgürlüğünün otoriter yönetimler tarafından çeşitli yöntemlerle kısıtlanması ciddi sorun teşkil etmektedir. Sosyal medya platformlarında, çevrimiçi topluluklarda, sohbet odalarında genellikle başkalarını kışkırtmaya, kutuplaştırmaya çalışan, haksız, mantıksız ve tutarsız tavırlar sergileyen internet trolleriyle sık sık karşılaşılmaktadır. Takma adlarla veya anonim hesaplarla yürütülen bu tür art niyetli kampanyalar literatürde trolleme olarak tanımlanmıştır. Trolleme faaliyetleri internet bağlantılı teknolojiler yaygınlaşmaya başladığı zamandan itibaren başlatılmıştır. Sadece ulusal

düzeyde değil uluslararası boyutta özelikle seçim süreçlerini hedef alan trolleme kampanyaları düzenlenmektedir.

Yapılan araştırmalara göre Rus hükümetine bağlı İnternet Araştırma Ajansı'nın dünyanın diğer ülkelerindeki seçim süreçlerini hedef aldığına dair birtakım bulgular ortaya çıkmıştır. İnternet trollemesi Hibrit bir savaş aracı olarak kullanılmaktadır. Letonya örneğinde (Fokin, 2016) olduğu gibi birçok ülkeye yönelik trolleme kampanyaları yürüten trollerin Rus hükümeti tarafından finanse edildiği bilinmektedir. Rusya-Ukrayna savaşı sürecinde de Rusya hükümeti trolleme operasyonları yürütmüştür. Rus hükümetiyle bağlantılı hesapların sosyal medya platformları üzerinden ABD'de siyasi söylemi, 2016 ve 2020 ABD Başkanlık seçimlerinin sonuçlarını etkilemek için kampanya yürüttüğü de tespit edilmiştir (Linvill vd., 2019; Fichman & Akter, 2023). ABD, Çin ve diğer birçok ülkeler de hedeflerine ulaşmak için zaman zaman trolleme faaliyetleri yürütmektedirler (Murphy, 2023). Özetle benzer eğilimler neredeyse dünyanın tüm ülkelerinde yaşanmaktadır.

Organize sosyal medya manipülasyonunun küresel envanterine bakıldığında siber birliklerin, sosyal medya üzerinden kamuoyunu manipüle etmeye kararlı hükümet, askeri veya siyasi parti ekipleri olduğu bilinmektedir (Bradshaw & Howard, 2017). Zaten otoriter yönetimlerin yönettiği toplumlarda hem çevrimiçi hem de çevrimdışı ortamlarda yönetenlerin izni veya bilgisi dışında herhangi bir eylem gerçekleştirmek pek mümkün değildir. Trollerin kamu kaynaklarıyla finanse edilmesi ve hükümet yetkilileri tarafından organize bir şekilde çalıştıkları gündemden düşmeyen bir gerçektir. Trollerin görevi hükümete muhalif olanlara toplu şekilde saldırıp sindirmektir. Gerçekleri çarpıtmakla görevli olan troller birkaç sosyal medya hesabı açıp hükümetin yolsuzluklarını ve başarısızlıklarını dile getiren herkesi milli değerleri de kullanarak linç ederler.

Dünyanın birçok ülkesinde hükümetlerin politikalarını ve çıkarlarını savunan maaşlı trolleri vardır (Sobolev, 2019; Alhazbi, 2020). Trollerin işe alınması suç sayılmalı ve takibi uluslararası bir kuruluş tarafından yapılmalıdır. Hatta farklı çıkar gruplarının da kendilerine ait trol desteleri bulunmaktadır. Eski trollerden bazılarının mekanizmanın işleyişi ile ilgili bilgileri kamuoyuyla paylaştıkları da haberlere yansımıştır. Trolleme kampanyalarının ağırlıklı olarak seçim ve savaş dönemlerinde

yürütüldüğü görülmektedir. Genel olarak ülkelere, kişi veya sosyal gruplara yönelik ya savunma ya da saldırı amaçlı yürütülen kampanyaların trollerin çekirdek kadrosundan gelen talimatlara göre şekillendiği bilinmektedir. En kötüsü ise gelişmemiş ülkülerde hükümetlerin devlet bütçesinden muazzam miktarda kaynak ayırarak muhalif kesimleri trolleyerek suç işlemleridir.

Rus trollerinin trolleme kampanyaları yürütmek için sosyal medya ağlarından en çok Telgraf'ı, Instagram'ı, X'i, TikTok'u kullandıkları tespit edilmiştir. Ayrıca Çin merkezli sosyal medya platformu TikTok'un yöneticileri tarafından da Avrupalı kullanıcıların Rus dezenformasyon ağı tarafından hedef alındığı belirtmiştir. Dünya toplumu, küresel çapta faaliyet gösteren sosyal medya şirketlerinin manipülasyonlara ve toplumsal kutuplaşmalara karşı sorumlu bir şekilde hareket etmesini sağlamalıdır (Reisach, 2021). Örneğin Twitter (X) sırasıyla Çin, Rusya ve Türkiye'den devlet bağlantılı bilgi operasyonları yapan 32.242 hesabı kalıcı olarak askıya almıştı (X, 2020).

Troller adeta tam teçhizatlı askerler gibidir. Gerektiği zaman hedefi imha etmek için topluca harekete geçerler. Algoritmalar ise otonom silahlar gibidir hedefe imha ederler. Bu konularda bilgili olmayanların sosyal medya platformlarındaki organize saldırıları anlaması kolay değildir. Kuşkusuz ki bu tür organizasyonların arkasında siyasi ve ekonomik bir güç vardır. Trolleme faaliyetleri dünya genlinde demokratik süreçlerin işleyişini engellemektedir. Bu nedenle trolleme faaliyetlerine karşı gereken önlemleri almak için uluslararası bir standardizasyon hazırlanmalıdır. Trolleme kampanyalarının etkisini azaltmak için vatandaşların bilinçlenmesi, trollerle ilgili kapsamlı araştırma ve analizler yapabilecek sivil toplum kuruluşlarının kurulması ve desteklenmesi büyük önem arz etmektedir.

Algı yönetimi süreçlerinde botların ve algoritmaların da kullanıldığı yaygın olarak bilinmektedir. Son yıllarda büyük veri araçlarını, otomasyon amaçlı yazılmış bilgisayar algoritmalarını ve kişiselleştirilmiş verileri kullanarak siyasal algı yaratma, siyasaları yönlendirme, kamuoyu oluşturma, gündeme yön verme gibi amaçları olan dijital siyaset yöntemine 'bilişimsel propaganda' (computational propaganda) adı verilmektedir (Kurnaz, 2022: 12). Botların veya kötü niyetli otomasyonun siyasette kullanılması olumsuz etkileri nedeniyle ciddi bir bilimsel ilgi görmektedir (Kermani vd., 2023: 2). Botların aynı siyasi görüşe sahip kullanıcılar tarafından üretilen

içeriğin tüketimini artırdığını ve siyasi yankı odaları sorununu daha da kötüleştirdiği bilinmektedir (Ferrara vd., 2020). Yalan haber üreten botlar ve seçimli tüketimin artmasına neden olan sosyal medya algoritmaları özellikle seçim dönemlerine toplumu kutuplaştırmak için kullanılmaktadırlar (Kurnaz, 2022: 20). Belirli bakış açılarını güçlendiren ve sosyal medyada seçilen aktörlerle etkileşime giren sosyal botlar veya algoritmik aracılar, koordineli eylem yoluyla çevrimiçi tartışmayı ve hatta kamuoyunu etkileyebilir (Duan vd., 2022). Çünkü botlar insanlardan daha fazla tweet üretme ve yayma kapasitesine sahiptir.

Tek bir kişi veya küçük bir grup insan tarafından kolaylıkla koordine edilebilen botlar bir fikir birliği yanılsaması yaratmak için kullanılmaktadır. Bazı sosyal medya botları yasal bilgileri toplayıp dağıtırken, diğerleri insanlarla iletişim kuruyor ve onları taciz ediyor, trend olan algoritmaları manipüle ediyor ve sistemleri spam ile dolduruyor (Woolley & Howard, 2018). Dahası, botlar popülerlik ipuçlarını manipüle edebilir ve ötekileştirilmiş grupların üyeleri gibi davranabilirler (Kermani vd., 2023). Pandemi sırasında botların, Twitter kullanıcı popülasyonunun yaklaşık yüzde 9'nu oluşturduğu ortaya çıkmıştı (Duan vd., 2022; Shi vd., 2020; Zhang vd., 2023). Botlar hem sol hem de sağ eğilimli söylemlerin kendi kendini daha da güçlendirmesini sağlamaktadır (Vosoughi vd., 2018).

Sosyal medyadaki sponsorlu trol hesapların ve botların davranışları dışsal motivasyonları nedeniyle sıradan kullanıcılardan farklı olduğu ve şüpheli davranışlarını tamamen gizlemeleri mümkün olmadığı için yapay zekâ teknolojileriyle tespit edilmesi mümkündür (Alhazbi, 2020). Bununla birlikte sosyal medya platformlarındaki sponsorlu içeriklerin üst kısmında "sponsorlu" ibaresi görünmektedir. Bu ibareye tüm sosyal medya platformlarında yer verilmesi ve kullanıcıların bu tür içeriliklere kuşkuyla yaklaşması güvenlik açısından faydalı olacaktır. Dijital platformların temel iş modeli kullanıcı bilgilerinin algoritma analizi yoluyla onların ilgisini çekme olasılığı yüksek olan paylaşımları göstermek üzerine kurulmuştur. Ayrıca platform yöneticileri algoritmalar aracılığıyla içeriklerin görüntülenmesiyle ilgili istedikleri gibi karar verme seçeneğini üretebilme imkânına sahiptirler.

Hesaplamalı propaganda ve sosyal medyada otomatik hesapların kullanımı özellikle Rus hükümetinin yurtdışındaki faaliyetleriyle yaygın olarak dünya

genelinde ilgi uyandırmıştır (Stukal vd., 2019). Hükümetler sosyal medya platformlarının temel iş modelini bilen uzmanları kullanarak algı yönetimi için mümkün olan imkânlardan faydalanmaktadırlar. Algı yönetimi sürecinde kişiselleştirme mekanizmalarıyla kişiye özel içeriklerin algoritmalarla belirli bir çerçevede izole edildiği ve yankı odalarında inançların güçlendirildiği bilinmektedir. Bu düzenlemenin büyük teknoloji şirketleri tarafından kullanıcı davranışları esas alınarak bilinçli yapılmasıyla birlikte kullanıcıların da inanç güçlendiren içerikleri istemesi mühim rol oynamaktadır (Chaykowski, 2018, January 11).

Sosyal medya platformlarında arka plandaki algoritmaların konfigürasyonu manipülatif bir rol oynamasıyla birlikte, kullanıcıların bilişsel referansları onları sahte haberlerin büyümesi için verimli bir alan yaratarak, filtre baloncuklarını ve yankı odalarını geliştirmeye yönlendiriyor (Borges & Gambarato, 2019: 605-606). Örneğin, X'e (Twitter'a) yeni girmiş birine ilk takip ettiği hesapların ve kullanıcının siteye verdiği bilgileri kullanılarak benzer başka hesaplar önerilmektedir. Bu sayede, kullanıcıların ilgilerini çekme olasılığı düşük kişilerle zaman kaybetmemesi sağlanmaktadır (Kuş, 2021: 7). Benzer bir durum içerik önerileri için de geçerlidir. Bazı ekipler, yüzlerce sahte hesabı yöneten bir avuç kişiden oluşur (Bradshaw & Howard, 2019: 17). Eskiden algıyı yönetenler dünyayı yönetir ifadesi dijital dünyada sistematik ve bilinçli operasyonların yaygınlaşmasıyla algoritmaları yönetenler dünyayı yönetiyorlar olarak değişmiştir. Dünyayı algoritmaların yönettiği doğrudur, ama algoritmaları kimlerin hangi amaçlarla kullandıkları sorgulanması gereken önemli bir konudur.

### 2.1.8. Dijital Dünyada Ötekileştirme ve Yankı Odaları

Her sosyal grup ve o grubu temsil eden bireyler farklı zamanlarda farklı bağlamlarda ötekileştirmeye maruz kalabilmektedir (Sağlam & Yaşar, 2017:135). Ötekileştirme sürecinde ötekileştirenin ya farklı olanı anlama kapasitesinden yoksun olduğu, ya da kasıtlı olarak, kötü niyetle ötekileştirmeye çalıştığı bilinmektedir. Genelde erdemli bireyler empati kurarak farklı kültürlere, görüşlere, fikirlere ve bireylere saygı duymaya üstünlük vermektedirler. Her kimlik ötekinin dolayımında ve ancak onunla birlikte var olabiliyorsa bütün kimlikler bir referans çerçevesine ihtiyaç duyar ve hiçbirinin tümüyle özsel olmadığını gösterir (Erkan, 2019). Bu

nedenle siyasi tercihler, ideolojiler, kimlikler, inançlar, etnik köken, cinsiyet ve kültürler arasında kıyaslama yapmak anlamlı ve etik değildir.

Dijital dünyada genelde ötekileştirme pratiklerinin siyasi çıkar amacıyla gerçekleştirildiği sık sık görülmektedir. Her ne kadar nefret söylemi sıklıkla ifade özgürlüğü kisvesi altında uygulansa da aslında ağırlıklı olarak siyasi alanda başkalarının düşüncelerini ve ifade özgürlüğünü engellemek amacıyla uygulandığı bilinmektedir (Pérez-Escolar & Noguera-Vivo, 2022). Politik amaçlı kin ve nefret söylemlerinin hedefleri ve sonuçları analiz edildiğinde kasıtlı yapıldığı anlaşılmaktadır. Ağırlıklı olarak kin ve nefret dolu medya içeriklerinin toplumda korkuyu canlı tutmaya çalışan otoriter yönetimlerin ve çeşitli güç yapılarının amaçlarına hizmet ettiği görülmektedir. Mevcut sorunların çözümü imkânsız değildir. Kapsamlı araştırma ve doğru yapılandırılmış stratejilerle daha az kutuplaşmış bir dijital dünya yaratmak her zaman mümkündür (Alatawi vd., 2021: 19-20).

Dijital dünyada ötekileştirmek amacıyla üretilen içeriklerin kimin veya kimlerin çıkarlarına hizmet ettiğini anlamak ve anlatmak için kollektif bir çaba harcamak gerekir. Ötekileştirmenin psikolojik ve politik bileşenlerinin etraflıca tetkiki, söz konusu fenomenin toplumsal çıktılarının ayrıştırıcı etkisini bertaraf edebilmek için bir başlangıç noktasıdır (Mahmut, 2023). Bilinçsiz bireyler için önemli detayları fark etmek ve dikkatli davranmak kolay olmayacaktır. Gerçek kaynaklardan alınan içerik özellikleri ile tıklama tuzağı, komplo teorileri, sahte haberler, nefret söylemi, önemsiz bilim ve söylentiler şeklindeki yanlış bilgi kaynakları arasında önemli farklılıklar olduğu tespit edilmiştir (Carrasco-Farré, 2022). Uluslararası kuruluşlar, hükümetleri, yerel sivil toplum kuruluşlarını, bilinçli vatandaşları ve büyük teknoloji şirketlerini bu konularda çözüm üretmeye mecbur edebilirler. Zararlı bilgi kaynaklarıyla ilgili farkındalık oluşturmak dezenformasyona ve ötekileştirme sorununa karşı etkili bir çözüm olabilir.

Ötekileştirme eğiliminin derinleşmesinde yankı odalarının da büyük etkisi vardır. Yankı odaları kişilerin eğilimlerini ve tutumlarını güçlendirebileceği gibi fikirler arasındaki kutuplaşmayı artırıp şiddetlendirme özelliğine de sahip olan alanlardır (Değer, 2022). Yankı odaları siyasi kutuplaşma ve yanlış bilginin yayılmasını teşvik ettiğine göre ciddi bir sorun olarak görülmektedir. Algoritmalar

aracılığıyla tavsiye edilen haber tüketimi (filtre baloncukları) yankı odalarının etkisini artırmaktadır. Kullanıcılar sadece benzer görüşleri paylaşan diğer kullanıcılarla etkileşime girdiklerine göre yankı odalarında bir nevi kendi sanal kabilelerini oluşturarak homojenize edici bir etki altında kalabilmektedirler (Narin, 2018). Yankı odası etkisi, göreceli olarak kapalı bir sosyal sistem içinde görüşlerin iletişim ve tekrar yoluyla güçlendirildiği durumu tanımlar (Zhu vd., 2021). Zihin kısıtlayan etkileri nedeniyle, yankı odaları, rekabetçi görüşleri sansürleme doğası ile sosyal medyada iletişim kurma ve bilgi paylaşımında önemli bir sorun olarak ortaya çıkmıştır (Medeni vd., 2020: 537). Bireyler yakın çevrelerinin görüşlerinden etkilendiğine göre en çok oy alan partilerden veya adaylardan hangisini destekliyorlarsa o partinin veya adayın kazanacağına inanmaktadır. Destekledikleri parti veya aday kazanmadığı zaman ciddi bir şaşkınlık yaşarlar. Rus hükümetiyle bağlantılı ajansların yankı odalarının sağladığı avantajları kullanarak ABD'de, Avrupa ülkelerinde ve dünyanın diğer ülkelerinde seçimleri manipüle etmek amacıyla çalışmalar yürüttükleri bilinmektedir (Linvill vd., 2019; Fichman & Akter, 2023).

Hem algoritmik hem de psikolojik etkenler bireylerin yakın çevresinden etkilenmesini sağlamaktadır. Yapay zekâ teknolojilerinin gelişmesine paralel olarak yakın çevreden etkilenme durumu daha da derinleşecektir. Ağırlıklı olarak bireyler muhalif görüşleri veya fikirleri dinlemek zahmetine katlanmak istemezler ve birçok konuda bir aydınlatıcıyı veya bilen birini çokta sorgulamadan dinlemeye eğilimlidirler. Dijital platformlardaki yankı odalarında kullanıcılar psikolojik olarak daha tatmin edici olduğuna göre kendileriyle benzer şekilde düşünen insanlarla bilgi paylaşımı yapmayı tercih ederler (Bouvier, 2022). Bununla birlikte kullanıcılar görüşleriyle örtüşen bilgileri sorgulamadan kabul etmek, beğenmek veya paylaşmaya meyillidirler. Bu anlamda bir konu ya da bir sorun hakkında sosyal medyada egemen olan düşüncenin toplumun genel algısının oluşumuna hizmet edeceği gerçeğinden yola çıkıldığında, sosyal medyada yankı odalarının etkisi göz ardı edilmemesi gereken önemli bir husus olarak kendini gösterir (Değer, 2022: 36). Yeni medyadaki yankı odalarında kullanıcıların önceden var olan inanç ve görüşlerini destekleyen görüşlerle etkileşime girdiği ve diğer bakış açılarını dışlayıp itibarsızlaştırması gibi

sorunlarla birlikte durdurulamaz bir dalga için bir umut olarak da görülmektedir (Alatawi vd., 2021).

### 2.1.9. Dijital Bağımlılık ve Temel Nedenleri

Dijital dünyada farklı bağımlılık türleri temel sorunlardan biri olarak bilinmektedir. Dijital video oyun bağımlılığının günden güne artmasının yanı sıra, sosyal medya gibi ortamlarda fotoğraf, haber, video gibi içerikleri paylaşma ve beğeni toplama isteği bireyleri farkında olmadan bağımlı yapmaktadır (Akçay, 2020). Çevrimiçi teknolojinin diğer faaliyetlere ve ilişki kurma tarzlarına zarar verecek şekilde aşırı kullanımı hem fiziksel hem de zihinsel riskleri artırdığı bilinmektedir (Richardson & Milovidov, 2022: 70). İnternet bağlantılı teknolojilerin dünya düzenine yön vermesinin asıl nedeni dezavantajları ile birlikte insanların gündelik yaşamlarını anlamlı ölçüde kolaylaştırmasıdır. Öğrenmek, bilgi edinmek gibi önemli faaliyetlerinin yanı sıra eğlenme ihtiyacının da masrafsız veya az masrafla karşılanması internet bağlantısı olan bireyleri adeta dijital ortama zincirlemiş durumdadır.

Dijital bağımlılığın nispeten en az tartışılan ve en önemli nedenlerinden biri dünya toplumunun büyük bir kısmının uğraşacak bir işinin olmamasıdır. Boş zaman sıkıntısının yaygın bir duygusal durum olduğu ve bağımlılıklar yaratan çeşitli davranışlara yol açtığı bulgulanmıştır (Miller vd., 2014; Biolcati vd., 2018; Bingöl & Eker, 2022). Özellikle işsizlik oranlarının yüksek olduğu ülkelerde boş durmaktan bunalmış bireylerin internette boş vakit geçirmeleri şaşırtıcı olmamalıdır. Dolayısıyla nomofobik davranışların (Wen vd., 2023) sergilenmesinde boş vakit ve tatminsizlik duyguları çok etken faktörlerdir. Örneğin Covid 19 salgını zamanı çocukların evde daha fazla vakit geçirmesine paralel olarak dijital bağımlılık eğilimlerinin arttığı tespit edilmiştir (Şenol vd., 2024; Li vd., 2021). Daha spesifik olarak yapılan bir araştırmada sıkılma eğilimi yüksek olan kızların ve oğlanların, sıkılma eğilimi düşük olan erkeklere ve kızlara göre dijital bağımlılık riskinin daha fazla olduğu bulgulanmıştır (Biolcati vd., 2018).

İnternete sürekli bağlı kalma ve bağlantının olmadığı yerlerde kaygılanmanın/strese girmenin (Akçay, 2020: 67) tek suçlusu internet bağlantılı teknolojiler değildir. Dijital bağımlılığa neden olan tüm faktörler arasında, can

sıkıntısının yoğun internet kullanımı için ortak bir tetikleyici olduğu ve özellikle sorunlu internet kullanım davranışına yol açabileceği kanıtlanmıştır (Wang, 2019). Boş zaman ve can sıkıntısına ilaveten daha önce tek amaç için kullanılan pahalı cihazların yakınsamasıyla akıllı mobil cihazların hepsinin bir arada olan çok amaçlı kullanıma uygun hale gelmesi dijital bağımlılığı tetikleyen önemli bir gelişmedir (Ezemenaka, 2013). Özetle dünya toplumunun büyük bir kısmının işsiz olması ve yapacak anlamlı işlerinin olmaması da dijital bağımlılığı tetikleyen en önemli sorunlardan biridir. Öte yandan çocukların dijital bağımlılıktan korunması üzerinde durulması gereken önemli bir konudur. Çünkü dijital bağımlılık konusunda çocuklar veya gençler yetişkinlere nazaran daha yüksek risk gruplarıdır. Dijital bağımlılık öğrencilerin dönem ödevi yazma, sınava çalışma, haftalık okuma ödevlerine uyma, idari görevleri yerine getirme, toplantılara katılma ve genel olarak akademik görevlerini yerine getirme gibi sorumluluklarını ertelemelerine neden olduğu tespit edilmiştir (Hayat vd., 2020; Alblwi vd., 2020). Özellikle çocukları dijital ortamdaki zararlı içeriklerden ve bağımlılıktan korumak için ebeveynlerin sorumluluk üstlenmesi gerekmektedir.

Chen ve arkadaşları (2020) tarafından yapılana araştırma sonucunda harçlığı yüksek olan, aile ortamı kötü olan, internet kullanım süresi ebeveynleri tarafından kısıtlanmayan, yüksek depresyonda olan, öz-yeterliği ve özsaygısı düşük olan erken ergenlerin internet bağımlılığına daha yatkın olduğunu tespit edilmiştir. Ampirik kanıtlara dayanan 87 araştırmanın incelenmesi sonucunda dijital bağımlılığa karşı önlemlerin dört ana kategori altında toplandığı bulgulanmıştır; psiko-sosyal, yazılım aracılı, farmakolojik ve birleşik. Yapılan araştırmalara göre önerilen karşı önlemlerin bağımlılık yaratan dijital kullanımı azaltmada etkili olduğu gösterilmiştir (Cemiloglu vd., 2022). Özellikle boş zamanlardaki can sıkıntısı göz ardı edilemeyecek kadar dijital bağımlılığı tetikleyen etkiye sahiptir (Selçuk, 2019).

Dijital bağımlılığa karşı önerilen güncel yaklaşımlar dijitalin aşırı kullanımına yönelik sorumluluğu ağırlıklı olarak bireye yüklerken, dijital cihaz ve hizmetlerin tasarımı da dikkat çeken ve aşırı kullanımı pekiştiren etkileşimli, akıllı ve kişiselleştirilmiş doğaları nedeniyle sorumluluk taşımalıdır (Altuwairiqi vd., 2019; Cemiloglu vd., 2022). Çözüm olarak sivil toplum kuruluşlarının, hükümetlerin ve büyük teknoloji şirketlerinin birlikte çalışarak gereken yasal düzenlemeleri yapması,

sosyoekonomik durumun iyileştirilmesi ve her türlü bağımlılıktan sakındırmak amacıyla toplumun bilinçlendirilmesi ve farkındalığın artırılması gerekmektedir.

### 2.1.10. Dijital Çağda Mahremiyet Algısının Dönüşümü

Arapça kökenli olan mahrem kelimesi, gizli tutulan, alenen açıklanmayan ya da gösterilmeyen anlamına gelmektedir. Literatürde farklı şekillerde ifade edilen mahremiyet kavramı, genel olarak "gizli olan, özel bilgi" şeklinde tanımlanır (Kütükoğlu, 2019: 273). Mahremiyet paradigması, yaşamın özel ve kamusal alanları arasında bir fark olduğunu ve teknolojik ilerlemeyle bu alanlar arasındaki sınır çizgilerinin bulanıklaştığını öne sürmektedir (Kovanic & Spac, 2022: 186). İnternet bağlantılı teknolojilerin mahremiyetin ihlali hususunda tetikleyici rol oynadığı tartışılmaktadır. Dijital dünyada mahremiyetin ihlali istisnalarla birlikte kullanıcıların izin verdikleri kadar fiziksel alanlarında gerçekleşmektedir. Mahremiyet dijital dünyada kamusal alan ve özel alan ayrımının merkezinde yer alan kavramlardan biridir. Neredeyse insanlık tarihi kadar eski olan mahremiyet olgusunun kültürden kültüre ve aynı toplum içerisinde zamana göre veya bireylerin dünya görüşüne göre değiştiği bilinmektedir (Korkmaz, 2013). Dijital dünyada da sürekli değişen teknolojik ve sosyal koşullar nedeniyle insanların mahremiyete ilişkin tutumları farklılık göstermektedir.

Laudon ve Laudon'a (2011: 131-132) göre mahremiyet, bireylerin özel hayatının gizliliğinin korunması, devlet dahil diğer kişi veya kuruluşların gözetiminden veya müdahalesinden uzak olması gereken özel bir alandır. Mahremiyetin bireysel bir tercih meselesi olmasıyla birlikte zaman zaman siyasi bir çekişme malzemesi olarak kullanıldığı da bilinen bir gerçektir. Genel olarak mahremiyetin ihlali insanların kendilerine bağlı ve kendilerine bağlı olmayarak iki şekilde gerçekleşmektedir. Birincisinde insanlar yeterince dikkatli ve bilinçli olmadıkları için, ikincisinde ise diğer insanların, örgütlerin, hükümetin gözetimi veya müdahalesiyle mahrem bilgilerin ihlali söz konusudur. Dijital dünyada eğlenmek, boş zaman geçirmek, gündemi takip etmek, arkadaş edinmek, bilgi alışverişi yapmak, takipçi sayısına bağlı olarak para kazanmak gibi pek çok yönde tatmin olmak mümkün olduğu için cazip görünmektedir. Veri kapitalizminin (West, 2019) ve platform kapitalizminin (Srnicek, 2017) yükselişi, kişisel verilere ilişkin yapısal

dinamikleri değiştirerek mahremiyet hakkının doğasına itiraz etmiştir (Kovanic & Spac, 2022). Mahrem içeriklerin kullanıcılar tarafından bilinçli olarak paylaşılmasındaki en önemli motivasyonlarından biri de çok takipçi edinerek reklamlardan para kazanmaktır. Tüketim toplumunun üyeleri kendileri birer tüketim metasına dönüşmüştür (Turan, 2022).

İnsanlar her ne kadar dijital dünyada gördükleri ve özendikleri içeriklerin etkisinde kalsalar da nihayetinde doğaları gereği meyilli oldukları davranışları sergilemeye isteklidirler. Dijital dünyadaki olanaklarla mahremiyet kamusal alanı işgal etmiş, sömürgeleştirmiş ve geleneksel dünyadaki ayrıcalığını kaybetmiştir (Bauman ve Lyon, 2013). İnternet bağlantılı teknolojilerin getirdiği en önemli değişim zaten var olan davranış ve tutumların kayda alınabilir olmasıyla daha çok insan tarafından bilinmesini sağlamasıdır. Gerçek hayatta mahremiyet "kişinin tek yönlü olarak belirlediği alan" iken, dijital dünyada ise mahremiyet dijital teknolojileri, o teknolojileri üretenleri ve tüketenleri içeren çok boyutlu dinamik bir süreçtir (Barkuş & Mustafa, 2019). Tamamen yok olmasına ilişkin endişelere rağmen günün sonunda mahremiyet algısını dijital olanakların etkisiyle sosyal, ekonomik ve kültürel koşullar şekillendirecektir. Zuboff'a göre (2019), mahremiyet gözlerimizin önünde yok olmuyor, ancak sahipleniliyor, bir araya getiriliyor ve ticari metaya dönüştürülüyor. Dijital çağda insanların gizli kalmasını istedikleri bilgilerin veya davranışların mümkün olduğu kadar dijital ortama düşmemesi konusunda dikkatli ve bilinçli olmalarında yarar vardır. Çünkü dijital ortama düşen hiçbir bilgi sır değildir.

### 2.1.11. Dijital Dünyada Ekonomik ve Siyasi Güç Paylaşımı Sorunu

Dünya genelinde bölgesel ve yerel düzeyde hegemonyalarını devam ettirebilmek için tüm hükümetler teknolojik bağımsızlık ve bilgi kontrolünü elde etmek için çabalamaktadır. Mevcut düzende teknolojik bağımsızlık ve bilgi kontrolü ABD'nin tekelinde olsa da Çin hükümeti teknoloji alanındaki iddialı çalışmalarla büyük rakip konumundadır. Rusya hükümeti de dijital egemenliğini elde etmek için çabalasa da henüz ABD ve Çin menşeli/merkezli teknolojilere bağımlı konumdadır. Öte yandan büyük teknoloji şirketleri dünya genelinde gelir adaletsizliği ve bilgi kontrolü açısından hükümetler için ciddi sorun teşkil etmektedir (Veriter, 2021). Bu nedenle teknoloji şirketlerini güvenlik sorunu olarak adlandıran hükümetler fırsat

buldukları taktirde onlara büyük miktarda para cezaları vermektedirler. Devletlerin güçlü özel şirketlere karşı etkili önlemler alması bekleniyor, ancak aynı zamanda vatandaşlar üzerinde kendi kontrollerini genişleten teknolojilere de ilgi duyuyorlar (Andrew & Bernard, 2021). Hükümetler dezenformasyonla mücadele tedbirleri kapsamında büyük teknoloji şirketlerinden yasal temsilciler talep ederek kısmen de olsa bilgi kontrolünü sağlamaya veya kendilerini yasal koruma altına almaya çalışıyorlar. Büyük teknoloji şirketleri de yasaklanmak, kısıtlanmak, cezai yaptırımlarla karşılaşmak, değer kaybetmek ve aleyhte propaganda endişesiyle kullanıcıların aleyhine ilkelerinden tavizler vermektedirler. Dijital uzamda kullanıcıların haklarını ihlal ettikleri için ne hükümetler ne de teknoloji şirketleri masum değildir. Merkeziyetsiz platformlar yaygınlaştıktan sonra teknoloji şirketleri de hükümetlerle ilişkilerini yeniden gözden geçirmek zorunda kalacaklar.

Veri sömürgeciliği, tekno-sömürgecilik ve dijital sömürgecilik ABD ve Çin için hem ekonomik hem de hegemonik anlamda ciddi avantajlar sağlamaktadır. Her ne kadar çok tartışılmasa da dijital dünyada ABD ve Çin'in tahakkümü ve sömürü düzeni diğer dünya ülkelerini rahatsız etmektedir. Örneğin Rusya'nın Batı ile gerginleşen ilişkileri dijital dünyada da devam etmektedir. Fakat Rusya, kamu altyapısında ve özel sektörlerinde büyük ölçüde Batı teknolojilerine bağımlıdır (Epifanova & Dietrich. 2022; 1). Teknolojik bağımsızlık ve bilgi kontrolü konusunda iddialı çalışmalar gerçekleştiremeyen Rusya hükümeti meşruiyet krizi karşısında dolaylı yollarla (siber saldırılarla) bilişim sektöründeki istikrarı bozmaya çalışıyor. Bu tür girişimlerin temel nedeni dijital dünyada ekonomik ve siyasi güç paylaşımı sorunu olduğu anlaşılmaktadır.

Parlamentolar da diktatörler de teknolojinin hızına yetişemeyince veri yığınlarının altında eziliyorlar, hükümetler ülkeyi idare etseler de gidişata yön veremiyorlar ve ülkelerinin yirmi yıl içinde nerede olacağını kestiremiyorlar (Harari, 2016). UNCTAD tarafından yayımlanan Dijital Ekonomi Raporuna (2021) göre, ABD merkezli dev teknoloji şirketleri küresel veri değer zincirinin tüm bölümlerine dünya genelinde en fazla yatırım yapan şirketlerdir. Global düzeyde platform hizmetleri aracılığıyla kullanıcıların kişisel verilerini toplamasına, denizaltı kabloları ve uydular aracılığıyla verilerin iletilmesine, veri depolama merkezlerine, yapay zekâ teknolojilerine, yapay zekâ aracılığıyla veri analizinin yapılmasına, işlenmesine ve

kullanımına, küresel bulut altyapı alanlarına ciddi yatırımlar yapmaktadırlar (UNCTAD, 2021: 2-3). ABD merkezli teknoloji şirketlerinin teknoloji alanlarına muazzam ölçüde yatırım yapmaları sonucunda ortaya çıkacak tablo dünya ülkeleri arasında ekonomik dengesizliği artıracaktır. Dünyanın bir kısmının aşırı zenginleşmesi diğer kısmının ise aşırı yoksullaşması da kutuplaşma ve şiddet olaylarının artmasına neden olacaktır.

ABD ve Çin merkezli uluslararası şirketlerin yerel kalkınmayı baltaladığı, piyasaya hâkim olduğu ve esas olarak dijital mimarinin yapısal hakimiyeti yoluyla emperyal kontrol biçimlerine yol açtığı bilinmektedir. Diğer taraftan belirli alanlarda tekelleşen teknoloji şirketleri üreten tüketicilere ait verileri kullanarak hızla büyümekle birlikte diğer ülkeleri hem beyin göçüne hem de gelir kaybına uğratmaktadır (Derdiyok vd., 2020). Dünyadaki hiper ölçekli veri merkezlerinin yarısı, dünyadaki en yüksek 5G benimseme oranları, son beş yıldaki yapay zekâ startuplarının tüm finansmanının yüzde 94'ü, dünyanın en iyi yapay zekâ araştırmacılarının yüzde 70'i ve dünyanın en büyük dijital platformlarının piyasa değerinin neredeyse yüzde 90'ı ABD ve Çin merkezli şirketlerinin kontrolündedir (UNCTAD, 2021). Veriye dayalı dijital ekonomiden faydalanma kapasitesi açısından ABD ve Çin bu kadar ön plandayken diğer ülkelerin sömürülmesi ve dijital tahakküm altında kalması kaçınılmazdır.

ABD ve Çin'in ekonomik egemenlik anlamında tekel gücü, fikri mülkiyet hakları, küresel gözetim girişimleri, teknoloji hegemonyası ve ideolojik tahakkümü giderek yaygınlaşmaktadır. Yine UNCTAD tarafından yayımlanan Dijital Ekonomi Raporuna (2019) göre, blockchain teknolojileriyle ilgili tüm patentlerin yüzde 75'nin, Nesnelerin İnterneti'ne yapılan küresel harcamaların yüzde 50'nin, bulut bilişim pazarının yüzde 75'den fazlasının ve dünyanın en büyük 70 dijital platform şirketinin piyasa kapitalizasyon değerinin yüzde 90'ının ABD ve Çin'in tekelinde olduğu belirtilmiştir. Öte yandan ABD dijital olanaklarla gelişmekte olan ülkelerin üst düzey yöneticilerin malvarlığı veya yolsuzluklarıyla ilgili kapsamlı bilgi toplayarak çıkarları doğrultusunda kullanmaktadır. Örneğin ABD en son teknolojileri kullanarak Filipinli liderlerin ağlarının yanı sıra mali durumlarını, mülklerini, siyasi bağlılıklarını ve akrabalık ağlarını tespit ve analiz ederek ABD'ye karşı direnişleri yatıştırmak için kullanmıştır (Kwet, 2019). Benzer senaryoların diğer ülke liderleri

içinde kullanıldığı muhalif kesimlerce ifade edilmektedir. Özellikle gelişmekte olan ülkelerin otoriter yöneticileri uluslararası anlaşmaları ihlal ettiklerine göre ABD isterse elindeki somut delillerle hesap sorabilir. ABD'nin hesap sormamasının nedeni ise kuşkusuz ki söz konusu liderlerin ABD'nin istediği doğrultuda hareket etmeleridir. Bu tür liderler yönettikleri toplumlar için beka sorunudur. Veri sömürgeciliğinin eşitsizlikleri artırma ve marjinalleştirmeyi ilerletme yönündeki sonuçları derindir ve politika yapıcıların daha fazla dikkatini gerektirmektedir (Arora vd., 2023: 6).

Güçlü tekelleşme dinamikleriyle birlikte birçok karanlık tarafları olan büyük teknoloji şirketlerinin kısa sürede kazandıkları olağanüstü ekonomik ve siyasi gücün global sorunlara neden olması kaçınılmazdır. Giderek büyüyen dijital uçurum, gelişmekte olan ülkeleri, özellikle de en az gelişmiş ülkeleri daha da geride bırakma tehlikesi taşıyor (UNCTAD, 2021). Yüksek ve düşük gelirli ülkeler arasındaki dijital uçurumun, yapay zekâ teknolojilerinin toplumsal etkisi (hem faydaları hem de riskleri) açısından büyük eşitsizliklere yol açması muhtemeldir (The World Economic Forum, 2024). Şimdilik dijital teknolojilerin ve veri madenciliğinin sağladığı avantajlarla ve deneyimleriyle ayrıcalıklı bir konumda olan ABD merkezli şirketleri uluslararası düzeyde uygun şekilde düzenlemek için yeni bir yaklaşım ortaya koymak zaruridir. Bu bağlamdaki dengesizlikler ve güç mücadelesi uluslararası kurumlar, büyük teknoloji şirketleri ve hükümetlerin iş birliğiyle kontrol altına alınmalıdır.

### 2.1.12. Dijital Dünyada Nefret ve Ayrımcılık Sorunu

Sık kullanımına karşın "nefret söylemi"nin evrensel olarak kabul gören bir tanımı bulunmamaktadır (Weber, 2009). Bir kişinin veya grubun din, dil, etnik kimlik, engellilik, yaş, cinsiyet, siyasi görüşünü, ideolojisini, cinsel yönelimini hedef alan, çoğu zaman önyargıya dayalı, olumsuz ve saldırgan ifadelerdir (Watanabe vd., 2018). Siber Suç Sözleşmesi'ne ek olarak 1 Mart 2006 tarihinde yürürlüğe giren bilgisayar sistemleri üzerinden işlenen ırkçılık ve yabancı düşmanlığı niteliğindeki suçların cezalandırılmasına yönelik "Ek Protokol" nefret söyleminin internet aracılığıyla yayılmasına yönelik yasal ve diğer tedbirleri almayı taahhüt etmiştir (Weber, 2009: 7). Nefret söylemi, ötekileştirmeyi ve düşmanlaştırmayı, çeşitlilikle

ilgili tahammülsüzlüğü körüklemektedir. En kötüsü ise nefret söyleminin politik amaçlarla kasıtlı olarak sistematik bir şekilde üretilip paylaşılmasıdır.

Dijital mecralar ifade özgürlüğüne zemin hazırladığı gibi nefret ve taciz sorunu gibi toplumu olumsuz etkileyen içeriklerin de paylaşılması için uygun mecralardır (Çağlar & Ayber, 2022). Başka bir ifadeyle dijital mecralar nefret söylemleriyle bireylerin "biz" ve "öteki" olarak kutuplaştırılmasını ve söz konusu söylemlerin nefret suçuna dönüşme riskinin artmasını desteklemektedir. Özelikle yeni medyada kin ve nefret söylemi dünya toplumu için psikolojik ve duygusal anlamda ciddi bir sorun olarak devam etmektedir. Aynı zamanda kin ve nefret içerikli söylemler sadece psikolojik ve duygusal anlamda kötü etkilemez, zulüm suçuna varan nefret söylemi şiddete, suç işlemeye ve ardından fiili şiddet eylemlerinin daha aşırı biçimlerine teşvik eder (Fino, 2020).

Ayrışma ve kutuplaşma yaratan, duygusal ve psikolojik toplumsal dışlanma ve filli şiddet eylemlerine neden olan nefret söylemleri/suçları, belirli bir kişi, grup, etnik köken, cinsiyet, din veya fikirleri hedef alarak düşmanca ve aşağılayıcı ifadeler içeren iletişim biçimidir (Aksakallı, 2023). Yeni medya ortamlarında kendilerini daha fazla vatansever olarak göstermeye çalışan, adil olmayan, bencillik ve ayrımcılık yapan, toplumu kutuplaştırmaya çalışan, kasıtlı olarak nefret söylemi kullananlarla ilgili haberlerin altında yapılan yorumların toplumun büyük bir kısmı tarafından (beğenilmedi butonuna tıklanarak) beğenilmediği görülmektedir. Hatta bu tür bireyler veya sosyal gruplar toplum tarafından ülkelerinin beka sorunu olarak tanımlanmaktadır.

Dijital mecralarda kullanıcılar çeşitli nedenlerden dolayı hem tanıdıkları hem de tanımadıkları kişilere karşı nefret söylemleri kullanabilmektedir. Daha çok siyasi düşüncelerin, dini veya felsefi inançların farklılığı nedeniyle nefret söylemlerinin yaygın olarak kullanıldığı bilinmektedir. Önyargıların artmasına, yalan ve yanlış bilgilerin yayılmasına, sosyal grupların birbirine karşı düşmanca bir tutum içerisine girmelerine yol açan nefret söylemlerini (Koçoğlu, 2014) mağdura karşı bağnazlığın rol oynadığı bir politika alanı olarak düşünmek belki daha yerinde olacaktır (Iganski, 2008). Nefret suçu, bir bireye karşı gerçek veya algılanan ırkı, etnik kökeni, dini, ulusal kökeni, engelliliği, cinsel yönelimi veya cinsiyeti nedeniyle işlenen cezai bir eylemdir (Rayburn vd., 2003: 1). Schweppe'ye göre (2021) nefret suçunun

işlenmesinde hedef alınan kişi değil, daha çok bu kişilerin fail açısından temsil ettiği şeydir. Ancak nefret suçunun neden işlendiği sorusunun da dikkate alınması konusunda genel bir görüş birliği vardır (Peršak, 2022). Castaño-Pulgarín ve arkadaşları (2021) tarafından yapılan çalışmada internet ve sosyal medyanın çevrimiçi nefret söylemi için nasıl bir fırsat oluşturup oluşturamayacağına ilişkin 2389 makaleden 67'si seçilerek analiz edilmiştir. İlk aşamada çevrimiçi nefret söylemi türleri, dini nefret söylemi, çevrimiçi ırkçılık, cinsiyete dayalı çevrimiçi nefret ve siyasi nefret söylemi ile ilgili 33 makalede siber nefretin çoğunlukla bunların altında yatan ideolojiler tarafından desteklendiği tespit edilmiştir. Etik dışı birçok davranışa zemin hazırlayan dijital ortamlarda paylaşılan nefret dolu içeriklerin politik amaçlarla paylaşıldığı yaygın olarak bilinmektedir (Bilge, 2016; Claussen, 2018).

Siber panoptik ortamın yapısı, büyük verinin işlenişi ve çıkar gruplarınca kullanılması, manipülatif algoritmalar, "trash-streaming", "post truth", "deep fake", yankı fanusu ve bunun gibi daha birçok yeni etik problem alanı, dijitalleşen medya ile hayatımızdaki yerini almıştır (Varış & Avşar, 2022). Bu noktada da bireylerin bilinçli davranmaları veya farkında olmadan politikacıların çıkarları doğrultusunda nefret içerikli bencil söylemlerini yaymamaları oldukça önemlidir. Nefret söyleminin hangi amaca hizmet ettiğini, kimin yararına ve toplumun zararına olduğu ile ilgili ince ayrıntıların dahi farkındalığına sahip bireylerden oluşan bir toplum yaratmak için çabalamak gerekmektedir.

Dünya genelinde kin, nefret ve ayrımcılık söylemleriyle ilgili bireylerin sivil ve siyasi hakları hem ulusal hem de yerel düzeyde yasal düzenlemelerle güvence altına alınmıştır. Ayrıca her türlü nefret suçu ve nefret söylemi AB suçları veya Avrupa suçları listesine de dahil edilmiştir (Peršak, 2022). Ancak yasaların uygulanması aşamasında çevrimiçi nefret söylemi ile etkin biçimde mücadele etmenin yanı sıra, bu içeriklerle ve ifade özgürlüğü arasında dengenin korunmasıyla ilgili sorunlar yaşanmaktadır (Claussen, 2018). Zaman zaman hükümetler bireylerin ifade özgürlüğünü kısıtlayarak rejimlerine karşı haklı eleştiriler yapanları bile halkı kin ve düşmanlığa tahrik etme veya diğer gerekçelerle suçlayıp cezalandırabilmektedir. Bu tür sorunların çözülmesi için Avrupa İnsan Hakları Mahkemesi (AHİM) gibi tarafsız uluslararası bir kuruluşun veya kuruluşların dünya

genelinde yetkilendirilmesi önem taşımaktadır. Nefret söylemi ve söylentilerin aynı zamanda komplo teorileri ve nefret söylemine benzediği ya da tıklama tuzağı ve önemsiz bilginin diğer yanlış bilgi kategorilerinden ziyade gerçek kaynaklara daha çok benzediği bilinmektedir (Carrasco-Farré, 2022). Dijital teknolojinin manipülasyon yapmak için uygun olma özelliği, anlık küresel etkileşim sunan yapısıyla birleştiğinde nefret söyleminin üretilmesi, meşrulaştırılması hatta olmayanı oluyor gibi göstererek önlenemez bir hızda yayılması dünya toplumunun huzur ve barışını olumsuz etkilemektedir.

Nefret suçları hukuk, politika ve programlama literatüründe tanımlanmalı, ölçülebilmesine yönelik bilimsel yaklaşımlar ortaya konulmalı, sistematik yaklaşımla incelenmeli, caydırıcı cezalar işlevsel hale getirilmeli ve çelişkili kararlarla ilgili AİHM gibi tarafsız uluslararası bir kuruluş yetkilendirilmelidir. AİHM'ye göre devletlerin uluslararası hukuk çerçevesinde kin ve nefret söylemlerini yasaklamasına ve bu tür söylemlere maruz kalanların korunmasına dair yükümlülüğü vardır (Türay, 2016; Peršak, 2022). Aynı zamanda nefret suçlarıyla etkili bir şekilde mücadele etmek için eğitim ve farkındalık çalışmalarının artırılması önemlidir. Dijital dünyada nefret suçlarına karşı önlem alınabilmesi ancak toplumun daha bilinçli, erdemli ve dirençli hale gelmesiyle mümkün olabilecektir.

### 2.1.13. Kişisel Verilerin Toplanması ve Korunmasına İlişkin Sorunlar

Günümüz dünyasında dijital ekonominin temelini veriler oluşturmaktadır. Veri dünyasında sadece kişisel veriler değil aynı zamanda nesnelere, doğaya ve canlı organizmalara ait olan veriler de çok değerlidir. Akıllı telefonlar, tablet bilgisayarlar, sensörler, tıbbi ekipmanlar, web trafiği kayıtları, sosyal ağlardaki etkileşimler ve eczacılık, meteoroloji, simülasyon gibi alanlarda çözümler sunan bilimsel araştırmalar gibi birçok kaynak, büyük verinin büyümesine katkıda bulunmaktadır (Schneider, 2012: 6; Aktan, 2018). Verilerin çok yönlü doğası mevcut tahakküm alanlarını genişletmekle birlikte veri pazarı yüzlerce milyar dolar hacme ulaşmıştır. Aynı zamanda veri yönetişimi ve veri sömürgeciliği ABD ve Çin gibi dijital dünyadaki lider ülkelere muazzam fırsatlar sunmaktadır. Kullanıcıların verileriyle ve karşılığını ödemedikleri emekleriyle trilyonlarca dolar servet edinen teknoloji şirketlerinin yaklaşık hepsinin Silikon Vadisi'nden yönetilmesi ve ABD'nin dünya

genelinde muazzam ekonomik ve politik güce sahip olması dünya genelinde ciddi dengesizliklere neden olmaktadır. Kuşkusuz ki verileri ve dijital emekleri sömürülen devletler/hükümetler bu duruma sessiz kalmak istemeyecekler ve pastadan pay alabilmek için çeşitli girişimlerde bulunacaklar.

Geçmişte arazilerin ve diğer doğal kaynakların ele geçirilmesi yoluyla sömürgeci yayılmanın tarihsel süreçleri ile kişisel verilerin kapitalizme girdi olarak hizmet sunmasına ilişkin çağdaş süreçler arasında benzerlik vardır (Couldry & Mejias, 2020). Veri derlemeleri, pratiklerin, maddiliklerin, bölgelerin, bedenlerin ve öznelliklerin karmaşık bir düzenlemesi yoluyla tarihsel sömürgeleştirme biçimlerini güçlendirmektedir (Ricaurte, 2019). Günümüzde petrolün veri olduğu düşünülürse, bu gerçeğin ülkeler arasında ciddi ekonomik ve sosyal uçurumlar oluşmasına katkı sağladığını da söylemek yanlış olmaz (Birol, 2021). Başka bir ifadeyle veri sömürgeciliği, orantısız teknolojik getiriler yoluyla dijital olgunluk ve teknolojik ilerlemedeki boşlukları da genişletmektedir (Arora vd., 2023). Couldry ve Mejias'e (2020) göre veri sömürgeciliğinin kendine özgü doğası insan yaşamının sayısız yönünü kapitalizmin hammaddesi haline getirmiş ve ele geçirmiştir. Ülkeler arasında ekonomik uçurumu derinleştiren veri sömürgeciliği sürekli izlemeye dayanan, sosyal ayrımcılık ve davranışsal etki için benzeri görülmemiş yeni fırsatlar sunan yeni bir sosyal düzenden başka bir şey değildir (Couldry & Mejias, 2019). Sosyal bilimlerde büyük veri kullanımı, gözetimden etiketlemeye ve toplumsal eşitsizliklerin yaygınlaşmasına kadar birçok başlıkta riskler barındırırken, bu risklerin odağında kişisel verilerin korunması hakkına yönelik ihlaller yatmaktadır (Yılmaz & Özcan, 2022: 475).

Özelikle ABD ve Çin'in veri sömürgeciliği ile ilgili politikalarını bir bütün olarak anlamak için, çağdaş kapitalizmin sömürgeci düzenini bir bütün olarak anlamak gerekir. Veri ekonomisindeki uçurum düşük ve orta gelirli ülkelerin dijital sistemlerin değerinin orantısız bir şekilde yüksek gelirli ülkelere (ABD, Avrupa ve Çin) akmasıyla derinleşmektedir (Yıldız, 2021: 457-458; Heeks, 2022). Dijital ekonomik güçle ABD'nin ve Çin'in hegemonik davranışlar sergilemesi ve küresel eşitsizliklerin artması sorgulanmalıdır. Veri kapitalizminin bilgi asimetrileri, karşılığı ödenmeyen emek ve sosyal kontrol şeklindeki hoş olmayan olayların (West, 2019) yanı sıra ABD ve Çin sahip oldukları teknolojik imkânlarla diğer ülkeleri tahakküm

altında tutmaya çalışmaktadır. Gelişmiş gözetleme teknolojilerine sahip olan ülkeler dünya genelinde otoriter yönetimleri yaptıkları yolsuzluklarla, birinci dereceli akrabalarının yurt dışındaki malvarlığına el koymakla ve uluslararası mahkemelerde yargılamakla tehdit ederek köleleştirmeye ve dünya genelinde bölgesel kutuplaşmaları derinleşmeye devam ediyorlar.

ABD yönetimi ulusal güvenlik tehdidi nedeniyle Çin üretimi olan dijital ürünlerin, hizmetlerin ve platformların ABD'de (Menaldo ve Wittstock, 2021), Çin hükümeti de ABD üretimi olan dijital ürünlerin, hizmetlerin ve platformların ulusal güvenlik tehdidi nedeniyle Çin'de kullanılmasını ve erişimini yasaklamıştır (Qin vd., 2017; Xu & Albert, 2014). Teknoloji tekelcileri olan bu iki ülke karşılıklı önlemler aldığına göre kimin piyasaya sürdüğüne bağlı olmayarak tüm teknolojilerin ve veri temelli platformların güvenilir olmadığı anlaşılmaktadır. Rusya, Çin, İran ve Kuzey Kore ile bağlantılı uygulamaların sınırlanması konusunda geniş yetkileri olan ABD Başkanı TikTok'un yasaklanmasına ilişkin yasa tasarısı imzalamıştır. Başkan Joe Biden tarafından imzalanan yasaya (Oxford Analytica, 2024) göre TikTok uygulaması ya ABD merkezli bir şirkete satılacak, ya da yasaklanacaktır. Bu bilgi ABD merkezli teknoloji şirketlerinin ABD yönetiminin kontrolünde olduğuna dikkat çekmektedir. Ayrıca bu gelişmeler diğer dünya ülkelerinin de ABD merkezli ürünlere ve uygulamalara yönelik güvenlik tehdidi nedeniyle bu şekilde işlem yapabileceğini çağrıştırmaktadır.

Verilerin korunmasıyla ilgili dünya genelinde zaman zaman çeşitli skandallar yaşanmaktadır. Bu bağlamda en çarpıcı skandallardan biri Cambridge Analytica skandalıdır. Bir veri analizi şirketi olan Cambridge Analytica yaklaşık 87 milyon Facebook kullanıcısının hesaplarından izinsiz topladığı verileri, ABD ve İngiltere'nin kritik seçim ve referandum süreçlerini etkilemek amacıyla kullanmıştır (Özdemir, 2022: 25-26). İzinsiz toplanan verilerin ABD'de 8 Kasım 2016 tarihinde yapılan genel seçimlerde oy verme tercihlerini etkilemek amacıyla kullanıldığı tespit edilmiştir (Hinds vd., 2020). Mark Zuckerberg Cambridge Analytica skandalı ile ilgili ABD Senatosunda ifade verdiği zaman kullanıcı bilgilerini koruyamadıkları için hatalı olduklarını kabul edip özür dilemiştir. Büyük verinin dijital siyasetteki temel işlevi propaganda makinesinin seçmenlerin algı ve ilgilerine yönelik içeriklerle çok daha verimli işlemesini sağlamaktır (Kurnaz, 2022: 20). Veri sızıntısıyla ilgili

Facebook örneğinde olduğu gibi diğer sosyal platformlarında da bu tür sorunların yaşanması muhtemeldir. 2022 sonbaharının başlarında kimliği bilinmeyen bilgisayar korsanları Washington'un "ulusötesi suç örgütü" olarak tanımladığı Rus paralı asker grubu Wagner'e bağlı birliklere ait olan bir milyondan fazla belgeye erişim sağladı (Dossier Center, 2023). Wagnerleaks olarak tarihe geçen belgeler dijital dünyada kişisel verilerin toplanması ve korunmasına ilişkin ciddi sorunlar olduğunu gösteren skandallardan biridir. Sızdırılan belgelerde ABD'nin hasımlarını ve müttefiklerini gizlice dinlediği de ifşa edilmişti.

Dünya genelinde sızdırılan on milyonlarca belge arasında vergi cennetleri ve offshore şirketlerle ilgili sızdırılan belgeler dünya toplumunun dikkatini daha çok çekmiştir. Çünkü vergi cennetlerinde saklanılan paraların büyük bir kısmının otoriter yönetimlerin halktan çaldığı paralar olduğu tahmin edilmektedir. Lüksemburg Sızıntıları, Panama Belgeleri, Bahamalar Sızıntısı, Paradise Belgeleri Sızıntısı ve Pandora Belgeleri sızıntıları offshore şirketlerle ilgili bilinen örneklerdir (Wagner & Zeume, 2023). Aynı zamanda ulusal düzeyde de kişisel verilerin toplanması ve korunmasına ilişkin boşluklar özelikle otoriter rejimler için birçok avantaj sağlamaktadır. Hükümetler, verimlilik ve modernlik adı altında vatandaşların kişisel verilerini toplayarak kontrol ve gözetim amacıyla kullanıyorlar. Veriler, dışlanmış ve savunmasız grupların tahakkümünü güçlendirerek korku şantaj gibi sorunların artmasına neden olmaktadır. Mobil cihazların ve sosyal medyanın yaygın kullanımıyla birlikte, yeni sosyal katılım biçimlerinin vaadi ile kötüye kullanım ve kötüye kullanma tehdidi veya zarar verme ve taciz riski arasında sürekli bir gerilim ortaya çıkıyor (McCosker vd., 2016: 1). Ağırlıklı olarak bu gerilimin merkezinde verilerin toplanması ve saklanmasına yönelik uygulamalar yer almaktadır. Kişisel verilerin toplanması ve saklanması çok boyutlu bir konu olduğu için kapsamlı önlemlerin alınması gerektirmektedir.

Her ne kadar hukuki bir kesinliğe ulaşmasa da biyoetik haklar, siber uzay hakkı, kişisel verilerin korunması hakkı gibi hak kategorileri dördüncü kuşak insan hakları arasında değerlendirilmektedir (Yılmaz & Özcan, 2022: 474). Gizlilik, kendi başına değerli olan ve özerklik, kimlik, güvenlik, katılım ve refah için hayati önem taşıyan hem bir araç hem de bir amaçtır (Stoilova vd., 2019). Freedom House'a (2020) göre, hükümetler, algoritmaya dayalı ayrımcılık durumlarında vatandaşların

haklılarını koruyabilmek amacıyla itiraz ve tazmin için yasal düzenlemeler hazırlamalıdır. AB Genel Veri Koruma Yönetmeliği'nin 9. maddesinde özel nitelikli kişisel verilerin işlenmesi kapsamında ırk veya etnik köken, siyasi görüş, dini veya felsefi inanç, sendika üyeliğini ortaya koyan verilerin, genetik verilerin, biyometrik verilerin, sağlık, yaşam ve cinsel yönelimle ilgili verilerin izinsiz kullanımı yasaklanmıştır (Regulation, 2016: 96-97). Aynı zamanda veri sahibinin rızası olmadan kişisel verilerin farklı amaçlarla kullanılmasıyla ilgili belli koşullara da yer verilmiştir. Bununla birlikte AB'nin Genel Veri Koruma Yönetmeliği'ne göre bireylerin kişisel verileriyle ilgili üç kritik gizlilik hakkına sahip olmaları gerektiği vurgulanmıştır; (i) açık rıza (veri katılımı), (ii) unutulma / silme) ve (iii) taşınabilirlik (veri aktarımı) (Ke & Sudhir, 2023).

Kişisel verilerin hedefli reklamcılık ve çeşitli ticari amaçlarla kullanılması günümüz dünyasında sık sık karşılaşılan bir sorundur. Kişisel verilerin etik olmayan biçimlerde ele geçirilerek kullanıcıların ürünleştirildiği 'veri ekonomisi', dijital siyasette ideolojiden bağımsız olarak tüm aktörler tarafından benimsenmiştir (Kurnaz, 2022: 20). Ulusal düzeyde yasal düzenlemelerin yetersizliği, mahkemelerin bağımsız olmaması, hükümetlerin kişisel verilerinin güvenliğini sağlamak için yeterli düzeyde kaynak ayırmaması, çeşitli güvenlik açıkları nedeniyle devletin elindeki veri havuzlarından verilerin sızdırılması gibi sorunlar kişisel verilerin güvende olmadığını göstermektedir (Rahma vd., 2023). Freedom House'a (2020) göre, birçok ülkede, devlet yetkilileri tarafından daha geniş veri toplamayı kolaylaştırmak için siber güvenlik standartları kasıtlı olarak zayıflatılmış da olabilir.

E-devlet uygulamalarından elde edilen kişisel verilerin internet ortamında ticari amaçla satışa sunulması akla gelebilecek en kötü örneklerden biridir. Kişisel verileri e-devlet havuzlarından elde eden kişilerin ticari şirketleri ziyaret ederek verileri satma girişiminde bulundukları haberlere yansımıştır. Kişisel bilgilerin satışıyla uğraşanlar veri gizliliğini ihlal ederek (adres, eğitim, meslek, cinsiyet, ekonomik durum, ailede kaç kişi olduğu, araç bilgileri ve sağlık bilgileri) topladıkları verileri ticari şirketlere satmaya çalıştıkları ifşa edilmiştir. Söz konusu verilerin devletin arşivlediği veri havuzlarından çekildiği ortaya çıkmıştır. Ticaretle uğraşanlar potansiyel müşterilere ait bilgilere ihtiyaç duyduğuna göre yasadışı yollarla veri toplayanlar bu fırsatı değerlendirmeye çalışmaktadır. Ürün veya hizmet satmak

amacıyla ticari kurumlar tarafından yapılan telefon aramalarından da kişisel verilerin güvende olmadığı anlaşılmaktadır. Nesnelerin interneti, yapay zekâ teknolojileri (Arora vd., 2023), tek taraflı/dayatmalı kullanım politikaları ve zorunlu çerezlerin kabulü gibi uygulamalarla bu skandallar daha da artacaktır.

Kullanıcılar başka seçenekleri olmadığı için kişisel verilerin kullanımına ilişkin aydınlatma metinlerini okumadan kabul etmektedirler. Sosyal platformları, uygulamaları, hizmetleri ve cihazları kullanabilmek için herkes dayatılan sözleşmeleri kabul etmek zorunda bırakılmıştır. Özetle kullanıcıların gösterdikleri rıza keyfi olarak değil başka alternatifleri olmadığından gösterilmektedir. Ayrıca kişisel verilerin işlenmesi ile ilgili yapılan sözleşmeler o kadar uzun ve karmaşık metinlerden oluşmaktadır ki, onları oturup tek tek okumak için uzun bir zaman ve anlama kapasitesi gerekiyor. Örneğin, Google'ın (Fuchs, 2016) 2011 gizlilik şartları 10917 karakterden oluşurken, 2012 gizlilik şartları yüzde 30 civarında bir artışla 14218 karaktere yükselmiştir. Bu artan rakamlar da gizlilik politikalarının her geçen gün daha karmaşık hale geldiğinin göstergesidir. Ürün ve hizmet sunan şirketlerin müşteri verilerini nasıl kullandıklarını, verilere erişimi olan üçüncü taraflara ilişkin ayrıntıları ve üçüncü tarafların verileri kullanmasına nasıl izin verildiğini teknik olmayan bir dille açıklamaları zorunlu hale gelmelidir. Fakat kişilerarası, kurumsal, ticari alanda kişisel verilerin iş ve pazarlama amaçları doğrultusunda nasıl toplandığı ve kullanıldığı detaylı açıklansa da uzun ve küçük puntolarla yazılmış metinleri okuyup anlamak kolay olmayacağına göre dünya genelinde kullanıcıların tüm haklarını güvence altına alan bir standardizasyon hazırlamak için çaba gösterilmelidir.

Neto ve arkadaşları (2021) tarafından yapılan araştırmada 10.000'den fazla veri ihlali vakasından en büyük 430 veri ihlali vakası seçilerek incelendiğinde pek çok komplikasyon arasında standardizasyon eksikliği ilk sırada yer almıştır. Genel Veri Koruma sorunuyla ilgili küresel bir standardın olmamasından dolayı ABD'ye, Çin'e ve AB'ye özgü üç farklı yaklaşım ortaya çıkmıştır. Veri koruma kapsamında ABD'de pazar temelli yaklaşım, Çin'de devlet temelli yaklaşım, Avrupa'da veri gizliliğine yönelik hak temelli yaklaşım politikaları izlenmektedir. Ulusötesi veri yönetişimine tek tip ve sürdürülebilir bir çözüm oluşturmak ve küresel veri gizliliğinin geleceğini öngörmek amacıyla bu temel modellerin uyumlaştırılması

zaruridir (Lin, 2024). AB dijital dünyada ABD ve Çin gibi kendine özgü ekosistem oluşturmak için yeterince yatırım yapmasa da hak temelli yaklaşımla büyük teknoloji şirketlerine muazzam miktarda cezalar vererek sorunları azaltmak için çaba harcamaktadır.

Gelişen dijital ekonomiyle birlikte, kişisel verilerin ekonomik ve politik çıkarlar için uygunsuz kullanımı kamuoyunda geniş endişelere yol açmaktadır (Liu & Lu, 2024). Siyasal iktidarlar her geçen gün gözetim teknolojileri sayesinde denetim ve kontrol mekanizmalarını geliştirerek hayatın her alanına nüfuz etmektedirler. Teknoloji, denetim ve kontrolü sağlayan mekanizmanın ötesine geçip kişi davranışlarını şekillendiren temel bir iktidar aracı haline gelmiştir. Siyasal iktidarlar sahip oldukları teknolojik araçlarla gelenekselin dışında kişileri kesintisiz olarak izleyebilmekte, dinleyebilmekte, takip edebilmekte ve hatta onları biçimlendirebilmektedir (Taha, 2023). NBC 7 Investigates tarafından elde edilen belgelere göre, ABD hükümetinin göçmen kervanına bağlı aktivistleri, gazetecileri ve sosyal medya fenomenlerini gizli bir veri tabanıyla takip ettiği ve bazı durumlarda onların pasaportlarına ilişkin sistemde uyarılar yerleştirdiği ortaya çıkmıştır (Jones vd., 2019). Edward Snowden (2013) olayı, sızdırılan WikiLeaks belgeleri (2006-2016, 10 milyon belge), Panama belgeleri (2016, 2.6 terabayt belge) ve Pentagon belgeleri (2023) yüzde yüz veri güvenliğinin mümkün olmadığını ve zaman ilerledikçe dijital gözetleme teknolojilerinin her geçen gün daha da geliştirilerek kullanıldığını göstermiştir. Günümüze kadar sızdırılan belgeler "buzdağının sadece görünen kısmı" olarak nitelendirilse de verilerin güvende olmadığına ilişkin büyük ölçüde detaylar içermektedir.

2018 yılında yürürlüğe giren bir AB düzenlemesi olan Genel Veri Koruma Yönetmeliği kapsamında bugüne kadar büyük teknoloji şirketlerine büyük miktarda cezalar verilmiştir (Daigle & Khan, 2022). Fakat İrlanda Veri Koruma Komisyonu (DPC) tarafından Meta'ya verilen 1,2 milyar euro para cezası şimdiye kadar teknoloji şirketlerine verilen rekor cezalardan biridir (Beesley, 2023). Tüm dünya ülkeleri yasal düzenlemeler yapmak konusunda birlikte hareket etme hususunda kararlı adımlar atsa büyük teknoloji şirketleri genel veri koruma standartlarını hazırlayıp uygulamak mecburiyetinde kalabilir. Bununla birlikte genel veri koruma standartlarını ihlal eden büyük teknoloji şirketlerine rekor miktarda cezalar vererek

onları hizaya getirmek mümkündür. Ama nedense diğer dünya ülkeleri büyük teknoloji şirketlerine karşı AB gibi cesur adımlar atamamaktadır. Genel Veri Koruma Yönetmeliği sadece Avrupa ülkeleri için değil daha da geliştirilerek tüm dünya ülkeleri için uygulanmalıdır.

Özetle verilerin değerinin her geçen gün artmasıyla birlikte kişisel verilerin toplanması ve korunmasına ilişkin ciddi sorunların olduğu yaygın olarak bilinmektedir. Kişisel verilerin toplanması ve korunmasına ilişkin sorunların temel kaynağı hükümetlerin ve büyük teknoloji şirketlerinin çözüm üretmemesi ve politika eksikliğidir. Kişisel verilerin ihlaline paralel olarak dijital teknoloji üreten ve yayan şirketlerin servetleri her geçen gün katlanarak artmaktadır. Bu alandaki kritik soru büyük dijital ağ yapılarında bulunan kişisel verilere kimin sahip olması gerektiğidir (Çilingirtürk & Demirci, 2020: 82). Veri sahipleri kişisel verilerin toplanması, saklanması ve kullanımı hususunda en azından dijital teknoloji şirketleri ve hükümetler kadar yetkilendirilmelidir. Bununla birlikte herhangi bir içerik kullanıcılar tarafından yayınlandığında mülkiyetin platform sağlayıcısına verilmesi adil bir uygulama değildir. En azından bir kısmı fikir sahibine devredilmelidir. Kullanıcılar ve veri üreticileri maddi anlamda veri işlenme süreci sonucundaki gelirlerinden en azından yüzde 70 oranda pay alabilmelidirler. Aksi taktirde büyük dijital ağ yapılarına karşı toplu şekilde kullanımdan imtina eylemleri başlatılabilir ve dünya toplumu yararına anlamlı sonuçlar elde edilebilir.

Çıkarcı teknolojilere ve baskın veri epistemolojilerini dijital dünyadaki diktatörlere rağmen sosyal adalet, insan haklarının savunulması ve doğa hakları lehine tersine çevirmek her zaman mümkündür (Ricaurte, 2019). Yeter ki dünya toplumu bilinçlensin ve harekete geçsin. Sınır ötesi veri ve para akışlarını yönetmeye yönelik uluslararası çerçevenin hazırlanması, veriye dayalı dijital ekonominin dünya toplumun kalkınması için harcanmasına yönelik tutarlı uluslararası politikaların ve stratejilerin izlenmesi gerekir. Kuruluşlar içinde ve arasında veri yönetimine yönelik anlamlı yaklaşımlar, dijital inovasyonu kolaylaştırmak ve bireyler, kuruluşlar ve toplumlar için sosyal, ekonomik ve teknik faydalar ile riskleri dengelemek açısından kritik öneme sahiptir (Davidson vd., 2023). Kişilerarası, kurumsal ve ticari bağlamda veri gizliliğinin yasal ve etik çerçevesi tüm dünya toplumunu kapsayacak şekilde

hazırlanmalıdır. Kişisel verilerin toplanması ve saklanması ile ilgili düzenlemeler kesinlikle global ölçekte hazırlanmalı ve uygulanması takip edilmelidir.

### 2.1.14. Evrensel Siber Güvenlik Ekosisteminin Geliştirilmesi

Siber güvenlik, dijital sistemlerin korunmasının ötesinde verilerin yetkisiz erişime ve dağıtıma karşı da korunmasını ifade eder (Ciolan, 2014). Aslan ve arkadaşlarının (2023) yaptığı tanıma göre siber güvenlik, bilgi sistemlerindeki kurum, kuruluş ve kişilerin oluşturduğu elektronik ortamdaki iletişimin, yaşamın, entegrasyonun, maddi veya manevi varlıkların ve verilerin güvenliğinin, bütünlüğünün ve gizliliğinin korunması anlamına gelmektedir. Siber güvenlik ihlali, herhangi bir bilgi sisteminin veya güvenlik politikalarının gizliliğini kolayca tehlikeye atabilir (Neciyev & Pazarbaşı, 2024: 58). Siber güvenlik önlemlerinin temel amacı dijital dünyadaki yaşamın güvenliğini sağlamaktır. BT global düzeyde önemli avantajlar sağladığı için insan yaşamının her alanına nüfuz etmekle birlikte bazı ciddi tehdit ve riskleri de beraberinde getirmektedir. Söz konusu tehditlerin listesinde ilk sırada siber güvenlik, siber suç, siber saldırı, siber savaş gelmektedir. Söz konusu riskler/sorunlar ulusal sınırları aşarak ağır tahribatlara neden olabildiği için evrensel düzeyde etkin ve kapsamlı çözümlerin üretilmesi zaruridir. Siber güvenliğin çok disiplinli doğası ve siber güvenlik kaygılarının toplum genelinde yaygınlığı göz önüne alındığında, standartlaştırılmış bir terminolojiye sahip olmak, bunu kullanmak ve siber güvenlik ve siber güvenlik riskinin ne anlama geldiğine dair kapsamlı bir ortak anlayış geliştirmek gerekir (Cains vd., 2022: 1).

Güvenlik riskleri ve tehditlerinin yeri ve zamanı kötü sürpriz olabildiğine göre olağanüstü önlemlerin alınmasını zaruridir. Dijital ortamın kullanımının yaygınlaşması sonucunda geleneksel suçlar da dijital ortama kaymıştır (Aslan vd., 2023: 1). Meydana gelen siber saldırılar sonucunda bireyler, kurum ve kuruluşlar, işletmeler ve devletler çok yüksek maliyetlerle karşılaşmaktadırlar (Öztürk, 2018). Siber Fiziksel Sistemleri siber saldırılara karşı korumak için her an teyakkuzda olmak gerekiyor. Dijital dünyadaki gelişmelere paralel olarak siber güvenlikle ilgili dünya genelinde güvenlik önlemlerine olan ihtiyaç her geçen gün artmaktadır. Öte yandan siber güvenlik önlemleri yapay zekâ teknolojilerinin yaygınlaşmasına paralel olarak daha da önemli hale gelmektedir. Yapay zekâ, ağlara ve bağlantılı altyapıya öngörülemeyen etkilerle otonom olarak hareket edebilen tüm saldırı ve savunma

sistemlerini etkinleştirerek siber savaş yeteneklerini artıracaktır (The World Economic Forum, 2024). Bundan sonraki savaşlarda veri tabanlı yapay zekâ teknolojisiyle idare olunan otonom silahların yaygın olarak kullanılmasıyla birlikte siber güvenlikle ilgili endişelerin de artacağı öngörülmektedir. Bulut bilişim, nesnelerin interneti, sosyal medya, kablosuz iletişim ve kripto para birimleri gibi gelişen teknolojiler siber uzayda güvenlik endişelerini artırıyor (Aslan vd., 2023: 1). Bu gelişmelere paralel olarak güvenlik önlemlerine yönelik yaklaşımların da güncellenmesi zorunlu hale gelmiştir. Fiziksel dünyada olduğu gibi dijital dünyada da güvende olmak bireylerin en temel ihtiyaçlardan biridir. Maslow'un ihtiyaçlar hiyerarşisi çalışmasında fizyolojik ihtiyaçlardan sonra güvenlik ihtiyacı gelmektedir (McLeod, 2007). Fakat gelinen aşamada dijital dünyada uluslararası iş birliğini teşvik ederek toplumu siber suçlara ve savaşlara karşı korumanın yeterli düzeyde olmadığı bilinmektedir. Yapay zekâ teknolojilerinin etkisiyle siber saldırıların daha da sofistike hale geleceği öngörülmekle birlikte kullanım amacına bağlı olarak yapay zekâ teknolojilerinin siber tehditlerle mücadele etmek için kolaylık saklayacağı da düşünülmektedir (Karasoy & Gezici, 2023).

Akıllı cihazların yaygınlaşması, nesnelerin interneti ve makine öğrenimi teknolojilerinin entegrasyonu, üretim, iletişim, otomobil, tarım, sağlık gibi çeşitli sektörlerde yapay zekanın rehberliğinde otomasyona giden yolu açtı (Uddin & Kumar, 2023). Yeni dünya düzeninde çip temelli teknolojilerin etkisiyle güvenlik tedbirleri ve uluslararası güvenlik sistemleri tamamen farklı bir boyuta evrilmiştir. Dijital dünyada işlenen suçlar mekândan bağımsız gerçekleştirildiği için uluslararası düzeyde siber suçları tanımlayan ve güvence altına alan politikalar izlemek, mümkün olduğu kadar kısa sürede sıkı yaptırımlar uygulamak büyük önem arz etmektedir. Tehdidin çok boyutluluğu savunma için de benzer bir yaklaşımı zorunlu kılmaktadır (Bıçakcı, 2014). Kapsamlı tedbirlerin alınması için tüm paydaşların (aktif kullanıcılar, sivil toplum kuruluşları, hükümetler, uluslararası kuruluşlar ve büyük teknoloji şirketleri) iş birliği yaparak çözüm üretmesi temel bir zorunluluktur.

Başlangıçta daha basit amaçlar ve yöntemlerle gerçekleştirilen siber saldırılar artık devletler düzeyinde, otomatize edilmiş, daha sık, karmaşık, yıkıcı, tespiti zor ve hedef odaklı olmaya başlamıştır (Bilgi ve İletişim Güvenliği Rehberi, 2020; Strang & Vajjhala, 2023). Dijital dünyadaki siber saldırıların, savaşların ve kişisel verilerin

ihlali ile ilgili yaşanan skandalların temelinde dijital dünyada ekonomik ve siyasi güç paylaşımı sorunu dayanmaktadır. Siber saldırılar ABD ve Çin dahil tüm dünya ülküleri için ciddi bir tehdit olarak görünmekte ve zaman zaman endişe verici skandallar yaşanmaktadır. Özellikle Rusya'nın ABD'ye karşı siber saldırılar düzenlemesi, zarar vermesi ve bu tür saldırıların her an düzenlenebilme ihtimalinin olması endişelere neden olmaktadır.

> *Yeterince karmaşık bir siber saldırı ABD'nin güç ağını çökertebilir, ABD uçuş kontrol merkezlerini dağıtabilir, nükleer santrallerde sayısız kazaya ve kimyasal sızıntılara yol açabilir; polisin, ordunun ve istihbarat servislerinin iletişim ağlarını bozabilir, mali kayıtları silerek trilyonlarca doların kime gittiğinin izini bile bırakmadan buhar olup uçmasına neden olabilir (Harari, 2016: 484).*

Yenikleri engellemeden, etkili politikalar izlenerek kritik altyapıların siber saldırılardan nasıl korunacağı, siber uzayda olası bir çatışma durumunda galip gelmek için askeri bir gücün nasıl organize edileceği, eğitileceği ve donatılacağı, ulusal devlet ve terörist grupların siber uzayda saldırılar düzenlemesinden nasıl caydırılacağı ve siber uzaydaki çatışmaların nasıl kontrol edileceği titiz bir şekilde incelenmesi gereken konulardır (Voo vd., 2022). En uç noktada, kolayca yayılan, tespit edilmekten kaçan ve uygarlığımızı tehdit eden, iyi tasarlanmış bir virüs gibi yapay zekanın yol açabileceği insanlığın yok olma tehdidi dayanmaktadır (Pavel vd., 2023). Siber savaşların ve diğer siber saldırı türlerinin yükselişi, ülkeler arasında diplomatik ilişkiler için de yeni zorluklar yaratmaya devam etmektedir. Bu zorlukların çözümüne yönelik hükümetler daha fazla çaba harcamak zorunda kalacaklar. Siber güvenlikle ilgili yaşanan ve bitmek bilmeyen sorunlar (Aslan vd., 2023) uluslararası bir kurumun kontrolünde hükümetlerin ve büyük teknoloji şirketlerinin iş birliğiyle evrensel düzeyde güvence altına alınmalıdır.

Yapılan analizlere göre devletlerin yalnızca düşmanın altyapısını ve yeteneklerini yok etmeye veya devre dışı bırakmaya çalışmadığı, aynı zamanda ulusal siber savunmaları güçlendirmeyi ve geliştirmeyi, diğer devletlerden istihbarat toplamayı, ulusal siber ve ticari teknoloji yetkinliğini artırmayı, siber saldırıları kontrol ve manipüle etmeyi amaçladıkları açıktır (Voo vd., 2022). Bilgi savaşı için büyük bütçe harcamaları yapan hükümetler yüksek kapasiteli siber birlik ekipleri çalıştırarak yurt içi ve yurt dışı operasyonlar gerçekleştirmektedirler (Bradshaw & Howard, 2019: Bates & Rose, 2022). Bu kadar bireysel çabadansa uluslararası siber

normları geliştirmek ve teknik standartları tanımlayarak konusunda anlaşmak daha anlamlı olacaktır. Fakat tüm dünya toplumunun yararına kararların alınmamasının nedeni bölgesel güç olmak isteyen hükümetlerin bencil politikalar izlemesinden kaynaklanmaktadır. Örneğin ABD ve Çin arasında teknoloji dünyasında ciddi bir rekabet ve casusluk suçlamaları vardır. Her iki ülke de siber saldırılarla karşı karşıya kalmış ve birbirlerini siber casuslukla suçlamışlardır (Balcı Candan & Güzelipek, 2023).

Dijital sistemlerle ilgili her ne kadar önlem alınırsa alınsın yine herhangi bir işlem yaparken "sıfır güven" veya "asla güvenme" mantığıyla yaklaşmak, mümkün olduğu kadar doğrulama işlemlerini titizlikle yapmak önem arz etmektedir (Wylde, 2021). Fakat bu durum tüm kullanıcılar için ulaşılabilir değildir. Lisanslı programların fiyatları pahalı olduğu için kullanıcıların lisanssız programları kullanmak zorunda kalması kişisel cihazlardaki bilgilerin ve işlemlerin güvenliğini dışardan müdahalelere açık hale getirerek riske atmaktadır. Bununla birlikte lisanslı programların kullanımı da söz konusu programları üreten şirketler için hem maddi hem de politik anlamda özel bir önem taşımaktadır. Bilgilerini güvende tutmak için para ödemek durumu olan kullanıcılar programları üreten şirketlere dolaylı bir şekilde "bilgilerim değerlidir" mesajı vermiş oluyorlar. Muhtemelen lisanslı yazılımları kullananların bilgileri ve işlemleri büyük teknoloji şirketleri tarafından özel bir kategoride değerlendirilmekle birlikte ticari ve politik anlamda gözden geçirilmektedir. Özetle lisanssız programların kullanımı güvenli olmadığı gibi lisanslı programların da kullanımı yüzde yüz güvenilir değildir. Hukuki süreç başlatılarak hak ihlallerine karşı çıkmak ve tazmin etmek mümkün olsa da kanıtlanması çoğu zaman kolay değildir. Çeşitli nedenlerden dolayı teknoloji şirketlerinin hükümetlerle iş birliği yapması kullanıcılara yönelik yapılan hak ihlallerinin kanıtlanmasını ve tazmin edilmesini daha da zorlaştırmaktadır.

Dijital teknolojilerin doğru kullanımıyla dünya toplumuna çok büyük yarar sağlamak mümkün olduğu gibi yanlış kullanımıyla da tam tersine ciddi zararlar vermek ve tahribatlara yol açmak mümkündür. Akıllı teknolojilerin sürekli geliştirilmesiyle birlikte siber güvenlikle ilgili sorunlar da güncellenmektedir. Bu nedenle herhangi bir güvenlik uygulamasını veya antivirüs programlarını önermek kalıcı bir çözüm değildir. Yeni tip siber saldırılara karşı yeni savunma tekniklerinin ve antivirüslerin

geliştirilmesi gerekmektedir. İnternet bağlantılı teknolojilerin yaygın olarak kullanılmasıyla siber uzayda zaman zaman çeşitli saldırılar gerçekleştirilmektedir. Söz konusu saldırılardan bazılarına aşağıda yer verilmiştir;

1999 Kosova krizi sırasında Çin'in ABD'nin ve NATO'nun web sitelerine saldırması dünyada ilk siber saldırı olarak tarihe geçmiştir (Kişman & Güleç, 2021: 151). 2007 yılında NATO üyesi olan Estonya'ya yapılan siber saldırı ve arkasından 2008'de Gürcistan'a yapılan siber saldırılar ve 2009-2010 yılında İran'a karşı Stuxnet saldırısı gerçekleştirildikten sonra dünya ülkeleri önlem almak için harekete geçmiştir (Ermiş, 2018). Stuxnet, 2010 yılında İran'ın Buşehr ve Natanz'daki nükleer tesislerini sekteye uğratmak için ABD ve İsrail tarafından kullanılan kötü amaçlı yazılımdı (Baezner & Robin, 2017). Bu yazılım santrallerin temel denetleyicilerini yok etmek amacıyla tasarlanmıştı.

Yaşanan kötü örneklerden biri de Aralık 2015'te Ukrayna'da elektrik şebekesine[1] "BlackEnergy" adlı kötü amaçlı yazılımla yapılan siber saldırıdır (Cherepanov & Lipovsky, 2016). 1 ila 6 saat süren elektrik kesintisinden yaklaşık 225.000 tüketici olumsuz etkilenmiştir (Duo vd., 2022: 785).

Güncel bir örnek olarak verilebilecek verileri şifreleyerek fidye ödemesi talep eden kötü şöhretli yazılımlardan biri de WannaCry saldırısıdır. Bu uluslararası siber tehdit dalgasının dünya çapında 150'den fazla ülkeyi etkilediği bildirilmektedir (Hsiao ve Kao, 2018: 1). Bununla birlikte dünya genelinde şirketlerin kabusuna çevrilmiş fidye yazılımlarından biri de Cryptolocker olmuştur (Çelik & Çeliktaş, 2018: 115-116). Bu tür saldırılarla saldırganlar, kurbanların bilgisayarlarında bulunan dosyaları şifreledikten sonra anahtara erişim için fidye talep etmektedirler. Günümüzde de böyle saldırıların gerçekleşme ihtimali hep vardır. Bu tür saldırıların daha çok Rusya, Ukrayna, Hindistan, Çin menşeli olduğu bilinmektedir (Duo vd., 2022).

COVID-19 salgını döneminde (2020) ABD dahil birçok ülkede sağlıkla ilgili departmanlara ve laboratuvarlara siber saldırılar yapılmıştır (Lallie vd., 2021). Saldırganlar fidye almak amacıyla hastanelerden araştırma verilerini çalma ve hastanenin tüm bilgi işlem ağını kapatma girişiminde bulunmuştur. Örneğin 2020

[1] Güç şebekesi, bir enerji santrali, iletim ve dağıtım istasyonları, tüketiciler, kontrol merkezleri ve iletişim ağlarından oluşan tipik bir Siber Fiziksel Sistemdir (Duo vd., 2022: 785).

yılında Çek Cumhuriyeti'ndeki Brno Üniversite Hastanesine yapılan saldırı hastanenin tüm bilgi işlem ağının kapatılmasına, ameliyatların başka bir tarihe ertelenmesine ve tıbbi bakımın riskli duruma düşmesine neden olmuştur (Dönmez & Torun, 2022: 10). Bu saldırı hastaların tedavi sürecini büyük ölçüde olumsuz etkilemiştir. Benzer şekilde devlet destekli olduğu iddia edilen siber saldırılar Birleşik Krallık'taki bir aşı deneme grubuna ve acil durum hastanelerini inşa eden inşaat şirketine yönelik, ABD Sağlık Ajansı'na yönelik ve COVID-19 aşısı geliştiren Birleşik Krallık, ABD ve Kanada üniversitelerine yönelik düzenlenmiştir (Muthuppalaniappan & Stevenson, 2021: 1-2).

Başka bir örnek ise ABD'nin en büyük petrol boru hattı Colonial Pipeline'a yönelik düzenlenen fidye yazılımı saldırısıdır. Bu saldırının 8 Mayıs 2021 tarihinde DarkSide hack grubu tarafından gerçekleştirildiği ortaya çıkmıştır (INSIGHT, 2021). Petrol boru hattını açabilmek için "Colonial Pipeline Company" tarafından saldırganlara beş milyon dolar karşılığı kripto para fidye verildiği iddia edilmektedir. Çevrimiçi güvenlik kapsamında uluslararası standartların oluşturulması amacıyla 2001 yılında Budapeşte uygun mevzuatı kabul etmek isteyen devletlerin katılımına açık bir sözleşme hazırlanmıştır. Sözleşme, özellikle telif hakkı ihlalleri, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlalleriyle ilgilenen, İnternet ve diğer bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası antlaşmadır. Ayrıca, bu antlaşma bilgisayar ağlarının aranması ve müdahale edilmesiyle ilgili bir dizi yetki ve prosedür içerir (Önok, 2013). NATO üyesi çeşitli ülkelerin özellikle Almanya, Fransa gibi güçlü ülkelerin ve ABD'nin siber tehlikenin farkında oldukları, ciddi çalışmalar yürüttükleri ve siber tehditlere karşı önlem aldıkları bilinmektedir (Kişman & Güleç, 2021: 152). Fakat tüm önlemlere rağmen en gelişmiş ülkeler bile siber uzaydaki tehditlerin kaygısıyla yaşamaktadır.

Yeni nesil saldırı ve kaçırma teknikleri nedeniyle siber uzayda güvenlik duvarları, izinsiz giriş tespit sistemleri, antivirüs yazılımları, erişim kontrol listeleri vb. geleneksel koruma sistemleri artık sofistike saldırıların tespitinde etkili olamadığına göre yenilikçi, kapsamlı ve global düzeyde çözümlerin üretilmesine acil ihtiyaç vardır (Aslan vd., 2023). Siber güvenlikle ilgili tehditler ve riskler artamaya devam ederken hükümetler ve uluslararası kuruluşlar önlem almak amacıyla bir dizi yatırımlar yaparak hem ulusal hem de uluslararası düzeyde siber tehditler ve risklerle

mücadele etmeye çalışıyorlar. Fakat siber tehditlerden ve risklerden korunmak için paydaşların bireysel mücadeleleri (Solmaz, 2023) hem fazla zaman hem de fazla kaynak talep etmektedir. Sonuç ise beklendiği gibi olmamaktadır. Geleneksel yöntemlerle kontrol altına alınamayan siber tehditler hükümetlerin gücünü ve yetkisini aştığı için hükümetlerle özel sektör tehditlerle başa çıkabilmek amacıyla ortak çıkarları çerçevesinde etkili iş birliği yapmak zorundadır (Li, & Liu, 2021: 8183-8184). Bu nedenle dünya genelinde evrensel siber güvenlik ekosisteminin geliştirilmesi hem daha az masraflı hem de daha güvenilir olacaktır. Bununla birlikte evrensel düzeyde siber güvenlik kültürü geliştirmek ve yaygınlaştırmak dijital yaşamı korumak için en iyi yaklaşımlardan biri olabilir (Gcaza & Von Solms, 2017). Bu bağlamda idari tabanlı yönetim, politikalar, standartlar, prosedürler, risk değerlendirmesi, ticari amaçlı girişimler, atanan sorumluluklar tüm dünya toplumu için standart hale getirilebilir. Söz konusu siber güvenlik ekosistemi yaptırım gücü olan tarafsız bir uluslararası kuruluş tarafından tüm dünya ülkelerini kapsayacak şekilde oluşturulmalı, yasal düzenlemeler hazırlanmalı, uygulanması takip edilmelidir. Yasal düzenlemeleri uygulamak istemeyen hükümetlere karşı gerekirse zor kullanılmalıdır. Bu evrensel yapı siber saldırılara ve savaşlara karşı bilgi paylaşımını artırır ve savunma stratejilerinin geliştirilmesini kolaylaştır. Koordineli bir şekilde hareket etmek, siber saldırılara hızlı ve etkili yanıtlar verme kapasitesini artıracaktır (Çalıkoğlu, 2024: 11). Bölgesel olarak hükümetler ve kurumlar tarafından siber saldırılara ve savaşlara karşı kolektif mücadele etmek amacıyla yapılan anlaşmaların evrensel düzeyde tek bir merkez tarafından yönetilmesi dünya toplumu için güvenliğin ve gizliliğin korunmasına büyük katkı sağlayacaktır.

### 2.2. Ulusal ve Uluslararası Düzeyde Dijital Hegemonya

Hegemonya kavramı ilk defa Antik Yunan'da şehir devletleri içinde baskın olanları tanımlamak için kullanılmıştır. Marx ve Engels tarafından temelleri atılan ve Lenin tarafından geliştirilen hegemonya kavramı, Gramsci tarafından siyasal alanla sınırlı içeriğinden kurtarılarak genişletilip değiştirilerek üst sınıfların alt sınıflara üstünlüğü olarak değerlendirilir hale gelmiştir (Canöz vd., 2023: 335). Hegemonya geleneksel olarak uluslararası arenada karşı karşıya gelen devletler arasındaki güç dengesini ifade etmek için kullanılır (Nugent & Vincent, 2008: 216). Başka bir

ifadeyle bir devletin veya sosyal grubun diğerleri üzerindeki üstünlüğünü dayatması anlamına gelmektedir. Dolayısıyla baskın olabilmek için güçlü devletler veya sosyal gruplar her türlü olanakları kullandıkları gibi dijital olanakları da gerekirse insan haklarını da ihlal ederek çıkarları doğrultusunda kullanmaktadırlar. Özelikle ABD ve Çin gibi teknoloji üreten ülkelerin dijital dünyada hegemonik politikalar izlemesi diğer ülkeler için sorunlar yaratmaktadır. Örneğin sosyal paylaşım platformları, yazılımlar ve teknolojik cihazlar da hegemonyanın sürdürülmesi için etkili araçlardır. Özetle teknoloji üreten ülkeler ve büyük teknoloji şirketleri kullanıcıların kişisel verilerini toplayarak hem bilgi hem de ekonomik anlamda üstünlük taslama imkânına sahip olmaktadırlar.

Pandemi döneminde birçok sektörde şirketlerin değer kaybetmesine rağmen Facebook, YouTube, X (Twitter), Instagram gibi dev sosyal medya platformları ve teknoloji şirketleri değer kazanmıştı. Söz konusu şirketler en çok kullanıcı kitlesine ve etkiye sahip şirketlerdir (Yıldız, 2021). Aktif kullanılmaya başlandığından itibaren dünyada yaşanan toplumsal olaylar zinciri göz önünde bulundurulduğunda, etken yapısı, düşük maliyeti ve her zaman güncel olmak gibi özellikleri sayesinde sosyal medyanın gücü ve etkisi kanıtlanmıştır. Böyle güçlü ve etkili dijital platformlar sahiplerinin muazzam hegemonik güce ulaşmasına hizmet etmektedir. Sosyal medya platformlarının faydaları inkâr edilemez, ancak sahip oldukları gücün ve etkinin kontrolsüz kalması zaman zaman sorgulanmakta ve endişe yaratmaktadır.

Arap Baharı'nın (2010-2011) oluşumunda ve koordinasyonunda önemli rol oynayan sosyal ağları kendilerine karşı bir tehdit olarak gören Rus yönetimi 2012 yılında egemen devletlerin kendi yönetimi üzerinde kontrol sahibi olması gerektiğini öne sürerek ABD'nin dijital dünyadaki hegemonyasını kınamıştı. Birkaç ay sonra, Haziran 2013'te Edward Snowden, NSA tarafından başlatılan devasa bir ağ gözetim programı kapsamında toplanan skandal belgeleri dünyaya açıklamıştı (Glasze vd., 2023). 2022 yılında hükümet sırlarını sızdırmaya başlayan 21 yaşındaki BT uzmanı Jack Teixeira, ABD'nin Ukrayna ve Rusya savaşındaki operasyonları ve rolü hakkında gizli ve son derece hassas olduğu düşünülen belgeleri 28 Şubat 2023 tarihinde yayımlamaya başlamıştı (Royal, 2023). Diğer veri sızıntısı vakaları gibi, Teixeira vakası da dijital dünyadaki güvenlikle ilgili kaygıları tekrar gündeme getirmişti. Dijital dünyadaki ahlaki değerlerin ve ulusal güvenliğin ABD tarafından

ihlal edilmesi dünya genelinde ABD'nin dijital hegemonyasının kınanmasına ve hükümetlerin dijital ağları kontrol etmek için yasal düzenlemeler yapmalarına yol açmıştır (Glasze vd., 2023).

Facebook, X (Twitter) ve diğer sosyal platformlar, siyasi motivasyon, eğitim düzeyi, gelir düzeyi, geçmiş paylaşımlar gibi değişkenleri hesaplayarak kullanıcılara uygun gördükleri içerikleri önerebilmektedir (Fayyaz vd., 2020). ABD ve Çin merkezli teknoloji şirketler özel mülkiyetleri olduğunu iddia ettikleri kişisel verileri siyasi ve ticari operasyonlar için kullanmaktadırlar (Pronzato, 2023). Günümüze kadar sosyal medya platformlarında milyonlarca kullanıcının hesapları kuralları ihlal etme gerekçesiyle engellenmiştir. Ama ABD eski Başkanı Donald Trump'ın X (Twitter), Facebook ve Instagram hesaplarının kalıcı olarak engellenmesi büyük tartışmalara neden olmuştu (Seeliger ve Baum, 2024). Aynı zamanda bu dev şirketlerin gücünü kontrol altında tutmak için yasal düzenlemelerin yetersiz kaldığı konusu da tekrar gündeme gelmişti. Trump'ın engellenme sürecine bakıldığında Silikon vadisindeki teknoloji şirketlerinin nasıl muazzam bir hegemonik güce ve ortak hareket etme özelliğine sahip oldukları daha net anlaşılmıştı.

ABD eski Başkanı Donald Trump'ın X'te (Twitter'da) engellendikten sonra Facebook, YouTube, Instagram da Trump'ın hesaplarını engellemişti. Akabinde Reddit, Shopify, Snapchat, Twitch, Pinterest, Apple, Google ve Amazon da eyleme katılarak hep birlikte Trump'ı sansürlemiştiler. Anlaşılan sosyal medya şirketleri istedikleri zaman herhangi bir kullanıcıyı, özellikle siyasetçileri sansürlemek isterse onlara karşı çıkabilecek hiçbir gücün olmamasıydı. Örneğin Meta, 9 Şubat 2024 tarihinde İran'ın Dini Lideri Ayetullah Ali Hamaney adına açılan Instagram ve Facebook hesaplarını, 7 Ekim'de İsrail'e saldıran Hamas'a verdiği destekle ilgili eleştirilerin ardından kaldırmıştı (Gambrell, 2024). Bundan sonraki süreçte de dijital platformların kimliğine bağlı olmayarak kullanıcıları engelleyebileceği anlaşılmaktadır. Dijital teknolojileri üreten ülkeler ve şirketler muazzam bir hegemonik güce sahiptirler (Ünsal, 2020). Sosyal medya üzerinden elde edilen hegemonik güç hegemonik devletlerin ve şirketlerin sahip oldukları muazzam gücün küçük bir parçasını teşkil etmektedir.

Birçok ülkede hükümetlerin kitle iletişim araçlarını çeşitli yollarla sansürlendiği bilinmektedir, ama Trump engellendikten sonra sosyal medya

platformlarının da üst düzey siyasetçileri veya hükümetleri sansürleme potansiyeline sahip olduğu ortaya çıkmıştı. Olaydan sonra BM Genel Sekreteri Antonio Guterres, "sosyal medya şirketlerinin gücü ve insanlar hakkında toplanan bilgilerin hacmi, kişisel veriler üzerinde kontrol eksikliği ve verilerin siyasi amaçlarla kullanılması" riski gibi sorunlardan dolayı endişe duyduğunu söylemişti (Business Standard, 2021). ABD'de Temsilciler Meclisi'nin Adalet Komisyonu tarafından duyurulan açıklama metninde, belirleyici niteliğe sahip az sayıdaki internet platformunun, çevrimiçi ticaret, iletişim ve bilgi akışı üzerinde inanılmaz bir güce sahip olduğu ifade edilmişti (Candeub, 2021; Oh, 2021; Mueller & Farhat, 2022). 2020 yılı temmuz ayında Amazon, Apple, Google ve Facebook'un CEO'ları Temsilciler Meclisi'nin Adalet Komisyonu bünyesinde düzenlenen video konferansa katılarak ifade vermişti. ABD'nin en büyük dört teknoloji şirketinin üst düzey yöneticileri, Kongre'de yaptıkları savunmalarında, tekelleşme konusunda haklarındaki suçlamaları reddetmişti (Oh, 2021). ABD merkezli sosyal medya ve teknoloji şirketlerinin sahip oldukları güç gerçekten anlatıldığı gibi topluluk kuralarına uygun olarak değil de Çin'de olduğu gibi farklı amaçlarla da kullanılmıştır. Bundan sonraki süreçte de daha agresif bir şekilde kullanılmaya müsaittir. Otoriter rejimlerde, sosyal medya bir bilgi kontrol aracı olarak temel insan haklarını bastırmak, siyasi muhalifleri itibarsızlaştırmak ve muhalif görüşleri bastırmak amacıyla da kullanılmaktadır (Bradshaw & Howard, 2019).

İnternet özgürlüğünü en çok suiistimal eden Çin rejimi, ülkeye gelen tüm trafiğin kapsamlı bir şekilde izlenmesi ve filtrelenmesi amacıyla popüler yabancı hizmetleri ve merkezi teknik altyapıyı engellemektedir (Freedom House, 2020:2-3). Bu modeli takiben, Rus yetkililer ulusal acil durumlarda ülkeyi uluslararası internetten izole etmek için yasa çıkartmışlar, İran hükümeti de benzer şekilde 2019'un sonlarında kitlesel protestolara polisin şiddetli tepkisini gizlemek için internet bağlantısını kesmişti. Bununla birlikte diğer otoriter rejimler tarafından yönetilen ülkelerde de durum farklı değildir. Ulusal düzeyde hükümetler toplumu baskı altında tutmak için interneti ve dijital teknolojileri istedikleri gibi kullanmaktadırlar. Öte yandan uluslararası düzeyde ABD, Çin ve büyük teknoloji şirketleri dünya düzenine yön vermek ve güç mücadelesini kazanmak amacıyla dijital olanakları açık veya gizli bir şekilde kullanmaktadır. Egemen sınıf,

hükümetler ve büyük teknoloji şirketleri internet bağlantılı teknolojileri daha etkili ve bilinçli kullanma imkânlarına sahip olduğu için internet toplum için bir özgürleştirme aracı olarak değil bir hayatı kolaylaştırma aracı olarak nitelendirilmektedir.

Dünya genelinde en çok kullanıcısı olan Facebook, YouTube, WhatsApp, Messenger, Instagram gibi sosyal medya platformlarına bakıldığı zaman "WeChat" hariç hepsi ABD'de kurulan ve yönetilen platformlardır. ABD dijital dünya genelinde hegemonik güç olmaya devam ederken Çin'de dijital dünyada dengeleri değiştirebilecek konumdadır. Ayrıca Apple, Microsoft, Amazon gibi veri tabanlı şirketler de ABD'den yönetilmektedir. ABD hükümeti, Amazon ve diğer beş baskın teknoloji tekel şirketleri ekonomik kurtarıcılar olarak görmektedir (Vincent, 2017: 185). Teknoloji tekeli oluşturan büyük şirketler ABD için ekonomik kurtarıcılardır. Bu tür şirketlerin ekonomi politiğine bakıldığı zaman sömürüye dayalı bir düzenle dünyanın çeşitli ülkelerinden ABD'ye para akıtmakta olduğu görülmektedir (Fuchs, 2016). Gelişmiş veya gelişmekte olan ülkelerin bu duruma sonsuza kadar sesiz kalmaları mümkün olmayacaktır.

Teknolojik bağımsızlık ve bilgi kontrolünün ABD merkezli teknoloji şirketlerinin tekelide olması dünya kamuoyunu endişelendiren bir sorun olarak devam etmektedir. Diğer dünya ülkelerinden farklı olarak Rusya ve Çin ABD'nin dijital dünyadaki hegemonyasına karşı çıkmak için mücadele etmektedirler. Hükümetler çeşitli yollarla dijital dünyadaki hegemonyaya karşı çıkmaya çalışmakla birlikte kendileri de yönettikleri toplum üzerinde hegemonik olmak amacıyla dijital teknolojileri etkin bir şekilde kullanmaktadır. Mevcut durumda dünya ülkelerinin büyük çoğunluğunun dijital egemenliği kritik dijital altyapı sağlayıcılarının, güncel teknoloji üreticilerinin ve ABD'nin baskısı altındadır. Bu durumun ne kadar devam edeceği kullanıcıların bilinçlenmesinden ve toplu protesto eylemleri başlatma kapasitelerine bağlı olacaktır.

### 2.2.1. Egemenlik Mücadelesi Bağlamında Yapay Zekânın Geleceği

Yapay zekanın tanımı değişen ve gelişen önemine göre zamanla farklılık göstermektedir. Yeni teknolojik gelişmeler eski tanımları geçersiz kılmaktadır (Yakacak & Gümrükçüoğlu, 2024). Yapay zekâ, akıllı makinelerin kendi kendini izleme, yorumlama, teşhis ve analiz gibi görevleri otonom olarak yürütmesini

sağlayan endüstriyel dönüşümün öncü bileşeni olarak düşünülebilir (Ahmed vd., 2022: 5031).

Yapay zekâ ile ilgili gelecek senaryolarına bakıldığında kullanım amacına bağlı olarak olumlu ve yıkıcı etkilerinin kaçınılmaz olduğu anlatılmaktadır. Olumlu anlatılarda yaşamı kolaylaştırması, olumsuz anlatılarda ise teknolojik silahlanma yarışlarını, küresel liderlik mücadelelerini ve hükümetlerle kurumsal aktörler arasında ekonomik çıkar mücadelelerini hızlandıracağı anlatılmaktadır. Yapay zekâ, yönetimlerin yükselişini ve düşüşünü geri dönülmez bir şekilde etkileyecektir (Pavel vd., 2023). En önemli soru ise insan kontrolünü aşan yapay zekâ teknolojilerinin yaratacağı dönüşümün kime hizmet edeceğidir (Csernatoni, 2024). Son yıllarda yapay zekâ teknolojilerinin güvenlik ve savunma alanında daha da geliştirmek amacıyla test edildiği bilinmektedir. ABD ve AB destekli teknoloji şirketleri (Google, OpenAI, Microsoft, Palantir, Amazon, Clearview AI) Ukrayna'nın savaş alanlarını en son askeri teknolojileri denemek için adeta bir laboratuvar gibi kullanıyorlar (Bergengruen, 2024). 2020 Karabağ Savaşı zamanı da Türkiye ve İsrail yapımı olan İHA ve SİHA'ları kullanarak savaş alanında üstünlük sağlayan Azerbaycan topraklarını Ermenistan'ın işgalinden kurtarmayı başarmıştı. Bundan sonraki süreçte ABD'nin ve AB ülkelerinin müdahil olduğu savaşlarda yapay zekâ, insansız hava araçları ve yüz tanıma yazılımları da dahil olmak üzere askeri teknolojileri kullanma ihtimali çok yüksektir. Son zamanlarda çıkan savaşlarda gelişmiş teknolojilerin kullanımına ilişkin endişelerin ve etik kaygıların arttığı haberlere ve bilimsel çalışmalara yansımaktadır.

Yapay zekânın mevcut askerî teknolojilerle entegre olmaya başladığı, yeni askerî teknolojilere öncülük ettiği, gelecekte de yapay zekânın savaş sahasına askerî teknolojilerle daha yoğun bir şekilde entegre olacağı ve stratejik değerinin daha da artacağı beklenmektedir (Bilgin, 2023: 163). Artık askeri kararların yapay zekâ teknolojilerine devredilmesi muhtemeldir. Aynı zamanda savaş alanında komuta ve kontrol işlemlerinin yapay zekaya devredilmesi ulusal güvenlik açısından olumsuz sonuçlar da doğurabilir. Şimdiden yapay zekâ tabanlı otonom silah sistemlerinin ciddi tahribatlara yol açabileceği anlaşılmaktadır. Ayrıca diğer zararlı bir etki ise yapay zekâ destekli sosyal botların, sosyal medya platformlarını gerçek insan gibi algılayabilmesi, paylaşımlar yapabilmesi, insanlara yanlış bilgi vererek tartışmaları

tırmandırabilmesi, dolandırıcılık yapmak ve borsayı istismar etmek gibi birçok zararlı eylemi gerçekleştirebilmesidir (Hajli vd., 2022).

2022 yılında yapay zekâ teknolojilerine toplam 47,4 milyar dolar yatırım yapan ABD yapay zekâ teknolojilerinin geliştirilmesi için yaptığı yatırıma göre dünya genelinde lider konumdadır. ABD'nin en büyük rakibi Çin yaklaşık 3,5 kat az (13,4 milyar dolar) yapay zekâ teknolojilerine yatırım yapmıştır (Maslej vd., 2023:189). Önemli teknolojilerin geliştirilmesine yönelik ekonomik güç oyunları geleceğe dair algıları şekillendirerek sivil ve askeri ilişkilerde radikal değişimlere yol açmaktadır. Yapay zekâ, küresel güç dinamiklerini, güvenlik hususlarını ve ekonomik paradigmaları şekillendiren dönüştürücü bir güç olarak öne çıkmaktadır (Csernatoni, 2024). ABD merkezli yapay zekâ araştırma şirketi OpenAI'ın kurucusu Sam Altman'ın 7 trilyon dolar kaynak arayışı yapay zekâ teknolojileriyle ilgili beklentilerin ne kadar büyük olduğuna işaret etmektedir. Dijital dünyada lider konumda olan ülkeler teknolojik egemenliklerini güçlendirmeye ve stratejik bağımlılıklarını azaltmak için çabalamaktadırlar.

AB ve ABD Ticaret ve Teknoloji Konseyi (TTK) ve Yapay Zekâ Küresel Ortaklığı (YZKO) gibi oluşumlar yapay zekanın insan hakları, temel özgürlükler ve ortak demokratik değerlerle tutarlı olarak sorumlu bir şekilde geliştirilmesine ve kullanılmasına rehberlik eden uluslararası, çok paydaşlı bir girişim için çalışmaktadırlar (European Commission, 2021). İnternet Özgürlüğü Raporunda (2023) yapay zekâ araçlarını geliştirirken ve kullanırken hem devlet hem de devlet dışı aktörler için insan haklarına dayalı güçlü standartlar talep edilmiştir (Benedek, 2023).

Yapay zekanın jeopolitiğini kendi lehine şekillendirmeye çalışan ABD, Çin ve AB arasındaki ciddi bir rekabet gözlemlenmektedir. Çin'in dijital dünyadaki dengeleri yeniden şekillendirme potansiyeline sahip olması ABD'yi rahatsız etmektedir. AB nispeten kısıtlı yatırımlarıyla yapay zekanın yasal çerçevesini oluşturmaya ağırlık vermektedir (Csernatoni, 2024). Fakat AB'nin yapay zekâ yasasının daha geniş toplumsal kaygılar ve değerlerle uyumlu hale getirilmesi yapay zekanın yol açabileceği sorunlar için etkili bir çözüm olamayabilir. Günümüz dünyasında güçlü devletler diğer teknolojik olanakları kendi egemenliklerini korumak için tereddüt etmeden kullandıkları gibi yapay zekâ teknolojilerini de

yasaları ihlal ederek kullanabilecektir. Dünya genelinde yasal düzenlemeler gelişmiş ülkelerde kısmen etkili olabilir, ancak gelişmemiş ülkülerde mahkeme sistemleri hantal veya işlevsiz olduğuna göre hiçbir fayda sağlamayacaktır. Örneğin nükleer silah kullanımının yasaklanması ile ilgili kanun 22 Ocak 2021'de yürürlüğe girmiş olsa da Rusya devlet başkanı Vladimir Putin ABD ve AB ülkeleriyle güç veya çıkar mücadelesinde sıkışınca nükleer silah kullanacağına dair tehditler savurmaktadır. Özetle yasal düzenlemelerin (Council of Europe, 2023) siyasi arenada sıkışan otoriter liderlerin veya hükümetlerin sahip oldukları yasaklanmış silahları kullanmalarına engel olabileceği inandırıcı değildir. Gelişmiş ordular, savaş alanında ve siber-fiziksel alanda giderek artan otonom işlevleri denerken, prototipler oluştururken ve dağıtırken karmaşık ve çift kullanımlı yapay zekâ teknolojilerini de aktif olarak takip ediyor (Csernatoni, 2024).

Yapay zekâ ve blockchain gibi son teknolojiler, çevre yönetiminde karar alma süreçlerine, şeffaflığa ve yanıt verebilirliğe daha fazla ince ayar yaparak sürdürülebilir girişimleri hızlandırıyor (Tapias vd., 2024). Akıllı şehirler, akıllı fabrikalar, akıllı ulaşım, akıllı yardım, akıllı ürünler, akıllı sağlık hizmetleri, akıllı insan ve bilgisayar etkileşimi, akıllı öngörücü bakım, akıllı endüstriyel robotlar, (Duman, 2022) siber güvenlik ve gizlilik, otonom araçlar, sohbet robotları, otonom kaynak keşfi, artırılmış gerçeklik gibi sistemlerde veya alanlarında yapay zekâ büyük ilgi görmektedir (Ahmed vd., 2022). Bu teknolojiler geliştirildikçe gelecekte dünya düzenini ve yaşam kalitesini büyük oranda etkileyecekler. Yapay zekanın güvenli bir şekilde geliştirilmesini ve kullanılmasını güvence altına almak için yapay zekâ geliştiricilerini, araştırmacılarını, hükümet yetkililerini, sektör uzmanlarını ve sivil toplum temsilcilerini bir araya getirecek kilit ortaklarla stratejik ittifaklar geliştirmek etkili bir adım olabilir (Biden, 2023). Yapay zekâ ve büyük veri analitiği araçlarının iyi niyetli aktörler tarafından daha etkin kullanılabileceği mekanizmaların kurulması ve işletilmesi demokrasinin geleceği açısından hayati önem arz etmektedir (Kurnaz, 2022: 20).

### 2.2.2. Dijital Diktatörlüğün Çin Modeli ve Büyük Güvenlik Duvarı

İnternet özgürlüğü söz konusu olduğunda Çin'in dünyanın en baskıcı ülkelerinden biri olduğu bilinmektedir. Hassas konularda eleştirel görüşler ifade

edenler sindirme, taciz ve hatta gözaltına alınma riskiyle karşı karşıya kalmaktadırlar. Çin'in en kötü şöhretli sansür buluşu olan "Büyük Güvenlik Duvarı"nın, içerik kaldırma, web sitesi yasaklama ve vatandaşların gözetlenmesi gibi işlevleri vardır. "Büyük Güvenlik Duvarı" ulusal güvenliği korumak için 1998 yılında geliştirilen Altın Kalkan Projesi'nin bir alt sistemidir. Böyle rejimlerde her zaman siyasi ideolojinin muhalifleri sert cezalarla karşı karşıya kalmaktalar. Yasaklananların listesi sürekli artıyor ve insanların ifade özgürlüğü hakkı önemli ölçüde kısıtlanıyor. "Büyük Güvenlik Duvarı" kapsamlı sansür mekanizması olarak ün kazanmıştır. Mevcut rejime karşı tehdit olarak kabul edilen dijital platformular, web siteleri veya uygulamalar engellenir ve hükümet aleyhinde konuşanlar veya hükümetin zararlı olarak algıladığı herhangi bir bilgiyi paylaşanlar yasal yaptırımlarla karşı karşıya kalmaktadırlar. Örneğin COVID-19 salgını boyunca, salgınla ilgili çevrimiçi tartışmalar engellenmiştir (Reuters, 2020).

Gelecekte sosyal medya ve teknoloji şirketlerinin neler yapabileceklerini anlamak için Çin örneğini detaylı bir şekilde irdelemek yararlı olacaktır. Silikon vadisindeki sosyal medya ve teknoloji şirketlerinin neredeyse tamamı ve aynı zamanda yerel mikroblogların çoğu Çin'de yasaklanmıştır (Bamman vd., 2012; Qin vd., 2017; Xu & Albert, 2014). Diğer taraftan Çin'in kendine özgü bir dijital ekosistem oluşturması ABD'nin dijital diktatörlüğüne karşı bir seçenek olması iyi anlamda da yorumlanmaktadır. Çin hükümeti kullanıcı bilgilerine erişim sağlayamadığı için başta Facebook, X (Twitter), Snapchat, Instagram, Telegram ve Signal olmak üzere birçok sosyal medya uygulaması devlet güvenlik duvarları tarafından engellenmiştir ve normalde erişilemez (Davison vd., 2018).

Şubat 2021'de, binlerce kişinin Clubhouse uygulamasında Sincan gözaltı kamplarını tartışmasının ardından Clubhouse uygulaması Çin'de yasaklanmıştır. YouTube, Twitch ve Netflix gibi video platformları da Çin'in sansür düzenlemelerine uymadığı için yasaklanmıştır. Aynı zamanda hükümetin gözetimi altında TikTok, QQ (bir anlık mesajlaşma), Sina Weibo (bir mikroblog), Youku (bir video paylaşım platformu), Kaixin (bir sosyal medya platformu) ve Wechat gibi yerli sosyal medya uygulamaları ve çeşitli teknoloji şirketleri piyasaya sürülmüştür. Ayrıca Çin'de otomatik sistemler, dünyanın en büyük güvenlik kamera ağını kullanarak internette ve halka açık sokaklarda şüpheli davranışları işaretlemektedir.

Son yıllarda tüm gelişmekte olan ülkelerde olduğu gibi Çin'de de artan akıllı telefon kullanımının yaygınlaşmasıyla özgürce iletişim kurmak daha da tehlikeli hale gelmiştir. Çünkü yetkililer, insanların kişisel verilerine doğrudan erişim sağlamak için gelişmiş gözetim teknolojilerini kullanıyorlar.

Çin'de tüm kitle iletişim araçları Xi Jinping ve Çin Komünist Partisinin (ÇKP) iradesine boyun eğmek zorunda kalmıştır. Bağımsız basın ağır biçimde kısıtlanmış ve gaddar sansür kurallarına tabi tutulmuştur. Medya kuruluşlarının partinin (ÇKP) taleplerine uyum sağlamasını kontrol etmek amacıyla çeşitli devlet kurumları oluşturulmuştur. İlk olarak, ÇKP'nin Tanıtım Departmanı, konuların tam olarak nasıl ele alınabileceğine dair yönergeler sunmaktadır. Ayrıca Merkezi Propaganda Departmanı, tüm medya kanallarının aynı çizgide kalmasını sağlamak için ulusal telekomünikasyon sektörünü denetlemektedir. Siyasi meseleleri veya genel olarak ÇKP'nin politikalarını eleştirmek hapse atılmakla sonuçlanabilir.

New York Times, Wall Street Journal ve BBC dahil olmak üzere önemli sayıda uluslararası haber kaynağı ve bağımsız web siteleri Çin'de engellenmiştir. Ayrıca Çin'in bu kadar gaddar politikalar izlediğini anlatırken ABD'nin de masum olmadığını belirtmek gerekir. Freedom House'a göre Çin, internet özgürlüğünün kısıtlanması konusunda dünyanın en kötü suistimalcisidir. Google ve Yahoo dahil olmak üzere küresel arama motorları Çin'de yasaklanmıştır. Dolayısıyla Google'nin çatısı altında hizmete sunulan Google Haritaları, Google Çeviri ve Google Akademik gibi ek hizmetler ve VPN web sitelerinin yanı sıra Google Play mağazası ve App Store da Çin'de engellenmiştir. Google arama motorunun yerine Baidu kullanılmaktadır. Wikipedia ve Reddit tartışma forumu gibi platformlar da Çin'de yasaklanmıştır.

Çin hükümeti yetkilileri sansürü sözde ulusal güvenliği korumak, nüfusu üzerinde sıkı kontrol sağlamak ve kamuoyunu şekillendirmek için bir araç olarak kullanıyorlar. Siyasi propagandanın halka ulaşmasını sağlamak için ÇKP'nin Tanıtım Departmanı hem çevrimiçi hem de çevrimdışı olarak kamuoyunu şekillendirmek için milyonlarca "kamu duyarlılığı analisti" istihdam etmektedir. Forumlara ve web sitelerine gelince, "50 Cent Partisi" olarak bilinen gayri resmi bir internet yorumcuları grubu, hükümeti eleştirenlere karşı mesaj panolarını dolduruyor ve karalama kampanyalarını koordine ediyorlar (Batke & Ohlberg, 2020). Dünya

genelinde hükümetlerin görevlendirdiği gayri resmi internet yorumcuları grubu maaşlı troller olarak tanımlanmıştır. Yaptıkları işi trolleme faaliyetidir.

Genel olarak her bir ürünün veya hizmetin telif haklarını ihlal ederek benzerini üretmek konusunda Çinliler çok yeteneklidirler. Yerli şirketleri yasalaştırmak ve kontrol etmek daha kolay olduğundan dolayı Çinli sosyal medya endüstrileri, popüler platformlara alternatifler geliştirmekte çok hızlı davranıyorlar. Çin'in sosyal medya ve teknoloji alanında ABD ile rekabet halinde olduğunu ve başarılı olduğunu söylemek yanlış olmaz. Ama Çin'in, dünyadaki en sofistike sansür rejimi ile yönetildiği de bilinmektedir. Çin'de hükümet tarafından "Büyük Güvenlik Duvarı" olarak adlandırılan, çevrimiçi ifadeyi kontrol etmek için web sitesi engelleme ve anahtar kelime filtreleme, sosyal medyayı sansürleme ve hassas politik konulara değinen içerikleri engellemek amacıyla bir dizi yöntem uygulanmaktadır. Çin hükümeti internet ortamındaki içerikleri kontrol eder ve rejimin çıkarlarına aykırı olduğu düşünülen içerikleri kısıtlar, siler veya yasaklar.

Çin'in sansür stratejisinin temel amacı, hükümeti eleştiren siyasi içerikleri engellemektir. 2021'de hükümet, vatandaşların uygunsuz siyasi veya kültürel içerikleri fark etmeleri durumunda birbirlerini ihbar etmeleri için bir telefon ihbar hattı başlatmıştır (China 2021 human rights report). Bu bağlamda Çin Komünist Partisinin (ÇKP) itibarına zarar veren içerikler, dışişleri ile ilgili yorumlar, sağlık ve güvenlik ile ilgili tartışmalar, ekonomi veya insanların mali refahı hakkında yapılan tartışmalar, ülke içinde insan haklarının ihlali ile ilgili konular sansürlenmektedir.

Facebook, X(Twitter) ve YouTube gibi platformların Çin'de yasaklanmasına karşın Çin hükümeti dolaylı yollarla propaganda ve dezenformasyon yaymak amacıyla bu platformları agresif bir şekilde kullanan ülkeler listesinde ilk sıralarda yer almaktadır (Bradshaw & Howard, 2019). Küreselleşmiş bir dünyada, ulusal devletlerin dijital sınırları üzerinde bu kadar acımasız bir kontrol uygulaması samimiyetsiz görünüyor, ancak internet, düşünmek isteyebileceğiniz kadar ulusal etkiden yoksun değildir (Bradbury, 2011).

Botlar rejime sivil desteğin olduğunu gösteren içeriklerle sosyal medya gündemini doldurabiliyorlar. Çin'de hem maaşlı troller hem de botlar rejimi öven içerik üretmekle meşguller (King vd., 2017: 489). Her geçen gün merkezi ve yerel ÇKP propaganda departmanları tarafından yerli ve yabancı gazeteciler üzerindeki

kısıtlamalar önemli ölçüde artmaya devam etmektedir (China 2021 human rights report). İnternet sağlayıcı firmalar da ÇKP ve hükümetin sansür direktiflerini uygulamak için bağımsız olarak binlerce ilave çalışan istihdam etmektedir.

Otoriter hükümetler iktidarları için tehlike arz eden grupları veya kişileri etkisiz hale getirebilmek için kolay bir şekilde yapay krizler yaratabilmektedir. Krizleri sahip oldukları medya kanallarında ve trolleri aracılığıyla uluslararası sosyal medya platformlarında gerçekmiş gibi göstererek propaganda yapıyorlar. Şeffaf yönetim ve yargı sistemi olmayan ülkelerin sınırları dahilinde fikir azatlığının olmadığı bilinen bir gerçektir. Hatta baskıcı rejimler yönettikleri ülkelerdeki yolsuzlukları, zulmü, işkenceleri başka ülkelerin sınırlarında dile getiren youtuberların, gazetecilerin ve blog yazarlarının seslerini kısmak amacıyla her türlü yolu denemektedir. Söz konusu yollardan bazıları hükümetin yolsuzluklarını dile getirenlerin ailelerini ve yakınlarını hapsetmek, vatan haini ilan etmek, dış güçler için çalışmakla suçlamak, ekonomik imkânlarını kısıtlamak, yapılan yayınlara erişimi engeli koymaktır (Zhao, 2020).

Ayrıca gelişmemiş ülkeler muhaliflerin kaçırılması, ülkelerine teslim edilmesi, aktivistlere, gazetecilere karşı taciz, takibe alma ve baskı yapmak gibi konularda karşılıklı olarak alenen iş birliği/pazarlık yapıyorlar. Otoriter rejimle idare olunan diğer ülkelerde olduğu gibi Çin'de de anayasada, vatandaşların konuşma, ifade özgürlüğü, toplanma, dernek kurma, yürüyüş ve gösteri yapmak gibi özgürlüklerinin olduğu belirtilse de vatandaşların anayasal hakları hükümet tarafından çeşitli şekillerde kısıtlanmaktadır. Yetkililer tüm kitle iletişim araçları üzerinde daha sıkı kontrol uygulamaya, bunları düzenli olarak hükümet görüşlerini ve ÇKP ideolojisini yaymak için kullanmaya, özellikle hassas yıldönümleri ve halk sağlığı gibi konularda basını, sosyal medyayı ve interneti sansürlemeye ve manipüle etmeye devam etmektedirler (China 2021 human rights report). Örneğin Çinli yetkililer, haber kuruluşlarına, COVID-19'la ilgili haberlerin yayınlanmaması konusunda katı talimatlar vermiş ve uzun süre sosyal medyayı sansürlemiştir (İnceoğlu, 2020).

Çinli yetkililer ayrıca devlete ait telekomünikasyon şirketlerini ve özel teknoloji şirketlerini kamu güvenlik kurumlarıyla veri paylaşmaya zorlamaktadır (Freedom House, 2020: 20). Çin'de vatandaşların hareketleri ve konumları ile ilgili

hızlı bir şekilde bilgi toplamak için tren istasyonlarına, otellere ve trafiğin yoğun olduğu diğer yerlere veri terminalleri kurulmuştur. Ülkenin karmaşık internet ekosistemini oluşturan şirketler, farklı hükümet yetkililerine bağlı olabilir veya aynı kuralları farklı şekillerde yorumlama özgürlüğüne sahip olabilir (Matsakis, 2020). Çin'de teknoloji şirketlerinden yalnızca içeriği kısıtlayan yasalara uymaları değil, aynı zamanda hükümet yanlısı kaynaklardan gelen haberleri tanıtmaları da doğal bir zorunluluktur. Merkezi bir hükümet direktifine ve iki Çin üniversitesi tarafından yayınlanan çevrimiçi bildirimlerle korona virüs hastalığının kökenleri hakkında akademik araştırmaların yayınlanmasına kısıtlamalar getirilmiştir (Gan vd., 2020). Çinli yetkililer, virüsle ilgili olan akademik araştırmaların yayınlanmasının önceden devlet onayına tabi tutulmasının tamamen dahili bir mesele olduğunu düşünerek uluslararası alanda doğacak sonuçlarını görmezden gelmiştir. Citizen Lab'ın paylaştığı bilgilere göre, WeChat platformunda kullanıcıların sohbetleri otomatik olarak filtrelenmektedir (China 2021 human rights report, 46). Otoriter rejimler internetteki sansür sistemini kapsamlı bir şekilde sürdürmek için mevzuatı ve yeni teknolojileri mümkün olduğu kadar etkin bir şekilde kullanmaktadırlar (Li, 2023).

ÇKP üyeliği, kadrolu bir fakülte pozisyonu elde etmek için her zaman bir gereklilik olmasa da ÇKP üyeliği olmayan akademisyenlerin terfi için genellikle daha az şansı vardır (China 2021 human rights report, 49). Medeni haklar, elit kayırmacılık ve sivil toplumla ilgili yapılan akademik araştırmalar politik olarak hassas kabul edildiği için yasaklanmıştır. Tüm bölümlerde lisans öğrencileri için Marksizm, Maoizm ve Deng Xiaoping düşüncesi gibi konularda siyasi ideoloji derslerini almaları zorunluluktur. ÇKP sansür konusunda ülkenin fiziksel sınırlarının ötesine de geçerek yurtdışında okuyan öğrencilerin sınıflarında bile izletilmesi ve rejim yetkililerine rapor edildiği bilinmektedir. Eğitim sektörü gibi diğer sektörler de kapsamlı bir şekilde hükümetin kontrolü altındadır. Çin'de olduğu gibi dünyanın diğer tek parti rejimi tarafından yönetilen ülkelerinde de durum aynıdır. İş dünyası hükümetin kontrolü ve baskısı altındadır ve muhalif sesleri susturmak için kullanılan en etkili araçlardan biridir. Bu tür rejimler kendilerine karşı çıkabilecek yabancı uyruklulara da vize vermeyerek ülkeye girişleri engellemektedirler. Genel olarak diktatörlerin elindeki en büyük imkân ülkenin ekonomik kaynaklarını istedikleri gibi yönetmeleridir. Otoriter hükümetlerin devletin bütçesini ve tabi servetlerini kimseye

hesap vermeden istedikleri gibi harcama fırsatı çok ciddi sorunların ortaya çıkmasına neden olmaktadır. Özellikle her türlü maddi imkânlara sahip oldukları için onlara karşı çıkabilmek aşırı derecede zordur.

Çin gibi yönetilen ülkelerde sansürden sorumlu kuruluşlar bütçe raporlarını paylaşmadıkları için yaptıkları harcamaları tahmin etmek kolay değildir. 12 Ocak'ta Jamestown Vakfı, ÇHC'nin 2020'de internet sansürü için 6,6 milyar dolar harcadığını tahmin eden resmî belgelere dayanan bir rapor yayınlamıştır (Fedasiuk, 12 Ocak 2020). Hükümetlerin rejimlerini korumak amacıyla sansür ve propaganda yapmak için harcadıkları büyük miktarda paraların bir kısmı da başka ülkelerde iş birliği yaptıkları kişilere veya kuruluşlara ödenmektedir. Örneğin yönettikleri ülkelerde iyi gelişmelerin olduğunu yazan yabancı gazetecilerle veya yayın organlarıyla para karşılığında iş birliği yapabiliyorlar. Ayrıca otoriter hükümetler sansür ve propaganda için harcanan paraların yanı sıra insan hakları aktivistlerini, hak savunucularını, yurt içi ve yurt dışındaki muhalifleri, çıkarlarına karşı çıkan netizenleri susturmak için ve hassas konuların dijital platformlarda tartışılmasını engellemek için de büyük miktarda kaynak ve efor harcamaktadır. Ülke sınırları içinde bu tür rejimlere karşı çıkmak kolay olmadığı için ulusüstü bir kuruluşun temel insan haklarının korunması bağlamında müdahale etmesi anlamlı bir eylem olabilir. Söz konusu ulusüstü kuruluş etkili olabilmek için tarafsız olmalı ve bencil kararlar vermemelidir.

# ÜÇÜNCÜ BÖLÜM

# DİJİTAL DÜNYA DÜZENİNDE HAK İHLALLERİ İLE İLGİLİ ÇÖZÜM ÖNERİLERİNE YÖNELİK NİTEL BİR ARAŞTIRMA

## 3.1. Çalışmanın Amacı

Bu tez çalışmasının temel amacı dijital hak ve sorumlulukların irdelenmesi ve hak ihlallerine yönelik çözüm önerilerinin ortaya konulmasıdır. Bilindiği gibi dünyada klasik vatandaşlık biçimi yerini dijital dünyada vatandaşlık modeline bırakmaktadır. Dijital dünyada vatandaşlık modelinin bazı dezavantajlarına rağmen avantajları da insanların yaşam kalitesinin iyileştirilmesi hususunda mühim rol oynamaktadır.

Dijital dünyada gereken disiplin ve düzen kurulursa, maliyet, zaman ve emek tasarrufunun sağlanması ve vatandaşlarla yöneticilerin karşılıklı etkileşimine dayalı olan "yönetişim" modelinin de uygulanması mümkün olacaktır. Şeffaflığın sağlanmasıyla insanların yaşam kalitesinin yükselmesi orantılı olarak artacaktır.

Daha iyi bir dünya düzeni kurmak için hak ve sorumluluklarının farkında olan, aktif, dinamik, sorumlu ve katılımcı bireylerden oluşan bir toplumun ortaya çıkması gerekiyor. Ancak dezavantajlı kesimlerin internet bağlantılı teknolojilerden faydalanamaması, eski yönetim sistemiyle ülkelerin yönetilmesi, vatandaşların dijital dünyadaki hak ve sorumluluklarının farkında olmaması, dijital dünyada belirli bir disiplin ve düzenin olmaması önemli bir çalışma alanı olarak kalmaktadır. Ağırlıklı olarak yapılan çalışmalar genel düzeyde belirli konulara odaklanmakla yetinmektedirler. Oysa vatandaşların dijital dünyada aktif, dinamik, bilinçli, katılımcı bireyler olabilmeleri için hak ve sorumluluklarını kapsamlı bir şekilde bilmeleri büyük önem arz etmektedir. Bu alanda kapsamlı bir çalışmanın ortaya konulması gerektiği düşünülmüştür.

## 3.2. Çalışmanın Önemi

Dijital dünyadaki gelişmelere paralel olarak dijital hakların ve sorumlulukların farkında olmak ve hak ihlallerine karşı bilinçlenmek önem arz

etmektedir. Şimdilik dijital ortamdaki temel sorunların çözümüne yönelik evrensel ölçekte bir ekosistemin olmaması tehditlere karşı bireysel savunmaları gerektirmektedir. Çözüm bekleyen sorunlarla ilgili büyük teknoloji şirketlerini, hükümetleri ve sivil toplum kuruluşlarını adım atmak için mecbur bırakmak bireylerin bu alandaki farkındalık düzeyine bağlıdır. Bu tez çalışması dijital haklar, sorumluluklar ve hak ihlallerine yönelik betimsel durum anlatımı yapıldıktan sonra evrensel düzeyde dijital dünyadaki temel sorunların çözümüne yönelik önerilerin sunulmasıyla benzerlerinden farklı olduğu varsayılmaktadır. Başka bir ifadeyle literatür incelemesinde dijital vatandaşlıkla ilgili hakların ve sorumlulukların farklı başlıklar altında tanımlamalarına ve mevcut temel sorunlara yönelik çözüm önerilerinin ortaya konulduğu tez çalışmasına rastlanılmamıştır.

Literatürde dijital vatandaşlıkla ilgili doktora tez çalışmalarına bakıldığında büyük ekseriyetinin eğitim alanına yönelik olduğu tespit edilmiştir. Eğitim alanında olduğu kadar toplumsal anlamda da dijital vatandaşlık dikkatle ele alınması gereken konulardan biridir (Karakuyu, 2023: 7). Literatür taramasında dijital vatandaşlık haklarının ve sorumlulukların öğretilmesine ve alt boyutlarına yönelik yapılan ilişkisel çalışmaların ön plana çıktığı görülmüştür. Türkiye'de dijital vatandaşlık alanı ile ilgili çalışmalar yok denecek kadar az olup, var olanlar da spesifik araştırmalar olarak özellikle eğitim alanına yönelik yapılmıştır (Eser Akkuş, 2017). Uluslararası alan yazında dijital vatandaşlıkla ilgili yapılan çalışmalar incelendiğinde, ilkokul, ortaokul, lise, üniversite ve öğretmenler gibi birçok farklı katılımcı grubuna yönelik çalışmaların yapıldığı söylenebilir (Karakuyu, 2023: 88). Öğretmen rolleri, teknoloji liderliği, öğrenci etkinlikleri ve internet güvenliği gibi başlıklar bağlamında dijital vatandaşlığı ele alan çalışmaların yoğunlukta olduğu değerlendirilmektedir (Som Vural, 2016: 30).

Karakuyu (2023) doktora çalışmasında üniversite öğrencilerine yönelik dijital vatandaşlık öğretim programının tasarlanması, uygulanması ve değerlendirilmesini amaçlamıştır. Karma yöntemle yapılan çalışmada "Günümüz dijital toplumlarına bilinçli dijital vatandaşlar yetiştirebilmek için dijital vatandaşlık eğitiminin hem toplumsal hem de bireysel anlamda bir ihtiyaç" olduğu belirtilmiştir.

New Zealand Human Rights Commission (2018) tarafından yayımlanan çalışmada dijital teknolojilerin hızlı ilerlemesine yanıt vermede yasal ve politik

çerçevelere rehberlik edebilecek temel uluslararası ve yerel insan hakları standartlarının ve ilkelerinin üst düzey bir özeti sunulmuştur. Çalışmanın birinci ve beşinci bölümünde mahremiyet hakkı bağlamında gözetim ve kişisel veriler için geçerli olan uluslararası insan hakları çerçevesi ve ihlalleri ortaya konulmuştur. İkinci bölümde Yeni Zelanda'da geçerli olan yasal çerçeveye ve politika çerçevesine genel bir bakış sağlanmış ve üçüncü bölümde gizlilik hakkına ilişkin izin verilen sınırlamaların ana hatları çizilmiştir. Dördüncü bölümde insan hakları üzerindeki olumsuz etkileri önlemek için devletlerin uygulamaya koyması gereken önlemler tartışılmıştır. Bununla birlikte, işletmelerin ve diğer özel sektör ile sivil toplum kuruluşlarının kişisel verilerin kullanımı ve korunmasına ilişkin politikaların geniş kapsamlı sonuçlarının değerlendirilmesi önerilmiştir.

Som Vural (2016) tarafından yapılan doktora tezi çalışmasında üniversite öğrencilerinin dijital vatandaşlık düzeylerini ortaya çıkarmak amacıyla özgün bir ölçek geliştirilmiştir. Veri toplamak için 23 madde ve beş boyuttan oluşan ölçekle dijital vatandaşlığa ve alt faktörlere ilişkin ortalamalar arasındaki ilişkiler ortaya çıkartılmıştır. Öğrencilerin sınıf düzeylerine yönelik yapılan karşılaştırmada dijital vatandaşlık ortalamalarının sınıf düzeyi arttıkça arttığı, internet kullanım sıklıkları ve aylık gelirleriyle genel ortalamaları arasındaki bağıntıların anlamlı olduğu tespit edilmiştir.

Kaur (2021) tarafından yapılan çalışmada Scopus'tan alınan 544 araştırma makalesine dayanan bibliyometrik analiz yapılarak en etkili çalışmalara tablo şeklinde yer verilmiştir. Dijital vatandaşlığın boyutlarına da (8) yer verilen çalışmada son on yılda (2002-2021) dijital vatandaşlık konusuna ilişkin araştırmaların doğasına ve gidişatına ışık tutulmuştur. Bunun yanı sıra, çalışmada dijital vatandaşlık alanındaki en önemli yazarlar, dergiler, kuruluşlar ve ulusların yanı sıra bu alanda gelecekteki potansiyel araştırma alanları da tanımlanmıştır.

Andrew ve Bernard (2021) tarafından yayımlanan çalışmada dijital çağda devletlerin, şirketlerin ve bireylerin insan haklarıyla ilgili karmaşık sorumluluklarının incelendiği araştırmalara yer verilmiştir. Hukuk, uluslararası ilişkiler ve gazetecilik de dahil olmak üzere çeşitli disiplinlerden uzmanlar tarafından dijital teknolojilerin insan hakları üzerindeki etkisinin ayrıntılı bir analizi sunulmuştur.

Henry vd. (2022) tarafından yapılan çalışmada dijital vatandaşlık bir statü (vatandaş olmanın ne anlama geldiği), bir pratik (vatandaş olarak hareket etmenin ne anlama geldiği) ve özneler arası bir deneyim (dışarıda, içeride veya dışarıda işgal etmenin ne anlama geldiği) olarak kavramsallaştırılmıştır. Yazarlar günümüze kadar dijital vatandaşlık söylemlerinde, teorilerinde veya uygulamalarında toplumsal cinsiyete dayalı güç ilişkilerinin rolüne sınırlı bilimsel ilgi gösterildiğini belirtmiştir. Çalışmada dijital vatandaşlığa yönelik çok katmanlı, feminist bir yaklaşımın öncelikle dijital toplumlardaki cinsiyete dayalı tahakküm ve dışlayıcı uygulamaları analiz etmek ve bunun yanı sıra feminist demokratik dönüşüm ve güçlendirme projesini destekleyen eyleme rehberlik etmek için değerli bir yol sundukları savunulmuştur.

Miller & Vaccari (2020) tarafından hazırlanan çalışmada dezenformasyondan nefret söylemine ve çevrimiçi özgürlüklere devlet müdahalesine kadar demokrasi ile ilgili çeşitli dijital tehditlere yönelik kaynaklar, vatandaşlar üzerindeki etki ve olası çözümler hakkında sekiz makaleyi bir araya getiren özel bir sayı sunulmuştur. Araştırmalar yirmi üç ülke ve dört kıtada yapılmıştır. Çalışmada internetin dünya çapında demokrasinin uygulanabilirliğini ve iyi işleyişini nasıl engelleyebileceğine ilişkin en acil soruların bazılarını ele almak için, genellikle farklı ülkeleri karşılaştıran çeşitli disiplin yaklaşımları ve yöntemleri kullanılmıştır. Dijital medya ve siyaset üzerine gelecekteki araştırmalar için önemli zorluklar belirtilmiştir.

Custers (2022) tarafından yapılan çalışmada mevcut temel haklara bağlı kalmaya ek olarak dijital çağda ortaya çıkan yeni haklarla ilgili sorunlar ele alınmıştır. Bu konuda daha geniş bir hukuki tartışma başlatmak amacıyla vatandaşlara dijital alanda çeşitli yeni haklar önerilmiştir.

Hyliaka (2021) tarafından yapılan çalışmada dijitalleşme bağlamında insan haklarının ve özgürlüklerinin karşı karşıya kaldığı temel tehditleri ve zorlukları analiz etmek ve bu tehditlere karşı korunmanın yolları üzerine önerilerin geliştirilmesi hedeflenmiştir. Çalışmada, sorunlu konulara ilişkin teorik ve hukuki araştırmalar yapılmıştır. Dijital çağın hak ve özgürlükler bağlamında tamamen yeni ve niteliksel olarak farklı fırsatlar sunduğu ancak aynı zamanda, bu hak ve özgürlüklerin güvence altına alınması için yeni zorlukları ve tehditleri de beraberinde getirdiği tartışılmıştır.

Yapılan benzer çalışmalar incelendiğinde dijital dünyada vatandaşlık haklarına, sorumluluklarına ve mevcut sorunların çözümüne yönelik birebir benzer şekilde ve geniş kapsamlı bir çalışmanın ortaya konulmadığı görülmüştür. Başka bir ifadeyle bu çalışmada tartışılan temel sorunlar amacına ve konusuna göre benzer çalışmalarda yeterince tartışılmamıştır. Aynı zamanda bu araştırma bu alanda bilgi edinmek isteyenler için pratik anlamda ve araştırma yapmak isteyenler için teorik anlamda kaynak bırakma konusunda önem taşımaktadır. Diğer çalışmalardan farklı olarak ilk aşamada vatandaşlık mekanizmasının nasıl ortaya çıktığı ve nasıl çalıştığı çalışmanın amacına uygun olarak tanımlanmıştır. Daha sonra vatandaşlık mekanizmasının nasıl dijital vatandaşlık mekanizmasına evrildiği, dijital hakların ve sorumlulukların neler olduğu, evrensel ölçekte hak ihlallerinin etkilerinin ve sonuçlarının neler olduğu anlatılmıştır. Sonuncu aşamada ise dünya toplumunu ilgilendiren beş temel sorunun çözümüne yönelik bilim insanlarının ve uzmanların görüşleri/önerileri derinlemesine görüşme yöntemiyle toplanarak değerlendirilmiştir. Özetle bu çalışmanın önemi dijital hak ve sorumlulukların tanımlanması ve tehlikelere/tehditlere dikkat çekerek hak ihlallerine yönelik temel anlamda çözüm önerilerinin yeterli düzeyde ortaya konulduğu doktora tezi çalışmasının bulunmamasından kaynaklanmaktadır.

### 3.3. Çalışmanın Sınırlılıkları

1990'lardan sonra internet bağlantılı teknolojilerin yaygınlaşmasıyla dünya düzeninde akışkan bir değişim yaşanmaya başlamıştır. Yaşanan gelişmeler sonucunda sosyal, kültürel, politik, ekonomik yapıların ve uygulamaların dönüşümü zorunlu hale gelmiştir. Söz konusu dönüşümlere paralel olarak dijital dünyada vatandaşların hak ve sorumluluklarının tanımlanması da zaruri hale gelmiştir.

Araştırma kapsamında dijital dünyada vatandaşların hak ve sorumluklarının neler olduğu irdelenerek, gerçek hayattaki hak ve sorumluluklarının dijital ortama evrimi, bireysel, ulusal ve uluslararası alanda ortaya çıkan sorunların neler olduğu ve sorunların çözümüne yönelik neler yapılabileceği araştırılmıştır. Fakat dijital dünyadaki sorunların kapsamı oldukça geniş olduğu için yalnız güncel sorunların ele alınması araştırmanın sınırlılıkları arasında ilk sırada yer almaktadır. Ayrıca bu araştırma 01 Ocak 2023-30 Mart 2023 tarihleri arasında Türkiye'de ve ABD'de

dijital vatandaşlıkla ilgili akademik çalışmalar yapmış 15 katılımcının (2'si kadın, 13'ü erkek) görüşleriyle sınırlıdır.

Her araştırmada olduğu gibi bu araştırmada da bazı sınırlamalar vardır. Araştırma sınırlamaları, bir çalışmanın genellikle araştırmacının kontrolü dışında olan pratik veya teorik eksiklikleridir (Viera, 2023). Titiz bir şekilde yürütülün araştırma süreçlerinde dahi sınırlamalar araştırma sürecinin ayrılmaz bir parçasıdır. Yazarlar tarafından potansiyel olarak önemli sınırlamaların kabul edilmesi ve tartışılması, bilimsel söylemin ve ilerlemenin önemli bir bölümünü temsil eder (Zhou & Jiang, 2023: 44). Sınırlamalar yaygın olarak metodoloji ve araştırma süreci olmak üzere iki kategoride gruplandırılır. Araştırmacılar, araştırdıkları çalışmanın sınırlarını mümkün olduğu kadar kapsamlı bir şekilde açıklayarak gelecekte daha etkili araştırmaların yapılması için yol gösterici olabilirler (Özkan & Kaya, 2015).

Bu çalışmanın evreni Türkiye'de ve ABD'de ikamet eden dijital haklar, sorumluluklar ve hak ihlallerine yönelik çalışmalar yapmış bilim insanları ve uzmanlarla sınırlandırılmıştır. Dijital dünyada vatandaşları ilgilendiren konuların ve sorunların hepsinin bir tez çalışmasında incelenmesi mümkün olmadığı için, dijital dünyadaki haklar, sorumluluklar ve temel sorunlarla ilgili farkındalık yaratmak ve çözüm önerileri sunmak amacıyla yalnız güncel konulara ve sorunlara yer verilmiştir. Çalışmanın amacına uygun olarak dijital dünyadaki en etkin konularla ve sorunlarla ilgili önemli bilgiler sunulmuştur. Derinlemesine görüşme kısmında ise spesifik olarak beş temel ve güncel sorunun seçilmesi çalışmanın sınırlılıkları arasındadır.

Araştırma sorularının büyük teknoloji şirketlerinin sahipleri olan Mark Zuckerberg, Bill Gates, Jeff Bezos gibi dijital dünyaya yön veren kişilere sorulması daha etkili sonuçlar doğurabilirdi. Fakat çalışmanın sorularına cevap almak için Mark Zuckerberg, Bill Gates, Jeff Bezos'a ulaşmak için çaba harcansa da sonuç almak mümkün olmamıştır. Mark Zuckerberg, Jeff Bezos'a gönderilen mailler cevaplandırılmamıştır. Bill Gates'e gönderilen mail ise Bill Gates'in özel ofisi olarak bilinen Gates Ventures'ta çalışan Vidhu Pasricha tarafından cevaplandırılmıştır. Cevap olarak yazılan mailde "tahmin edebileceğiniz gibi, her ay yüksek miktarda materyal alıyor ve ne yazık ki hepsine bakamıyor" diye belirtilmiştir.

Ayrıca "Çalışmanın Bulguları ve Yorumları" kısmında da belirtildiği gibi kadın akademisyenlerin ve uzmanların çalışmaya katılmak talebine ağırlıklı olarak

olumsuz yanıt vermeleri de sınırlılıklar arasındadır. Bununla birlikte Türkiye'de Kişisel Verileri Koruma Kurumu tarafından da araştırma sorularının yanıtlanmasına olumsuz yanıt verilmiştir. Araştırmaya katılma taleplerine verilen olumsuz yanıtlardan bazıları örnek olarak aşağıda gösterilmiştir;

> *Üzülerek, mevcuttaki yoğun gündemimiz nedeniyle talebinize olumsuz dönüş yapmak durumundayız.*
> *İlettiğiniz soruların büyük bir kısmı alanım dışı olduğu için cevaplamam etik olmaz.*
> *Araştırmanıza katılamayacağım, iyi çalışmalar dilerim.*
> *Ulaştığınız için teşekkür ederiz. Zaman kısıtlaması nedeniyle kibarca reddetmek zorundayım, en iyi dileklerimle (İngilizceden çevri).*

Katılımcıların katkılarına bağlı olan çalışmalarda araştırmaya katılım talebine olumlu cevap almak biraz yorucu bir süreçtir. Buna ilaveten araştırma örnekleminin bilim insanları ve uzmanlardan ibaret olması veri toplama sürecini daha da zorlaştırmaktadır. Çünkü bilim insanları ve uzmanlarının mevcut politik şartlardan dolayı soruları cevaplamak istememeleri veya hükümeti sürekli överek sorulara samimi cevaplar vermemeleri, zamanlarının kısıtlı olması, karşılıksız katkı sağlamaya hevesli olmamaları gibi durumlarla karşılaşmak muhtemeldir. Bu tür olumsuzluklar araştırmacının moralini kötü etkileyerek araştırmanın ilerlemesini yavaşlatmaktadır. Aynı zamanda çalışmanın örneklemine uygun bilim insanları ve uzmanların bulunması ve iletişim kurmak için de çok zaman ve çaba harcanmaktadır. Tüm zorluklara rağmen iyi niyetli, yardım sever ve bilime katkı sunmak isteyen alanında uzman kişilerin katkılarıyla veri toplama süreci bir şekilde tamamlanmış oluyor. Son olarak gelecekte yapılacak çalışmalarda örneklemin tamamının başka ülkelerde yaşayan alanında uzman kişilerden seçilmesi ve yapay zekâ teknolojilerinin dijital dünyada vatandaşlık mekanizmasını nasıl etkilediğine ayrıntılarıyla yer verilmesi önerilmektedir.

### 3.4. Araştırma Soruları

Tez çalışmasında ana hatlarıyla aşağıda yer alan beş (5) temel soruya cevap aranmıştır. Derinlemesine görüşme yöntemiyle toplanan veriler kategorilere ayrılmış, incelenmiş ve yorumlanmıştır. Araştırma sonucunda dijital dünyada farkındalığı artırmak amacıyla hak ve sorumluluklarla ilgili önemli bilgilere yer verilmiş, mevcut

hak ihlallerine dikkat çekilmiş ve beş temel soruna yönelik çözüm önerileri ortaya konulmuştur.

**Araştırma Sorusu 1 (S1):** Dijital dünyada endişe duyulan sorunlardan biri veri tekelciliği ve olumsuz etkileridir, bu konuda dezavantajlı ülkeleri de kapsayacak çözüm önerileri neler olabilir?

**Araştırma Sorusu 2 (S2):** Dijital dünyada siber suçları ve savaşları önlemek amacıyla ne tür tedbirler alınmalıdır, siber suçlara yönelik ülkeler arasında yapılan anlaşmalar ne kadar güvenilir olabilir?

**Araştırma Sorusu 3 (S3):** Egemen sınıf dijital dünyada toplumsal ilişkileri manipüle etmek amacıyla dijital eşitsizlikleri görmezden gelir ve aktif katılımı çeşitli yöntemlerle engellemeye çalışır. Bu sorunları en azından azaltabilmek amacıyla ne tür önlemler alınabilir?

**Araştırma Sorusu 4 (S4):** Dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların çözülmesine yönelik hangi adımlar atılmalıdır?

**Araştırma Sorusu 5 (S5):** Gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketler, dijital platformlar ve teknolojiler neden rekabet esasları üzerine kurulan serbest piyasada ABD merkezli büyük teknoloji şirketleriyle (Alphabet, Apple, Amazon, Meta, Microsoft, ...) küresel ölçekte rekabet edemezler?

Bu soruların her birinin kolay anlaşılmasını sağlamak amacıyla aşağıda açıklamalara yer verilmiştir. Bu bağlamda birinci soruya ilişkin olarak dijital dünyada veri tekelciliğinin ve olumsuz etkilerinin incelenmesi hedeflenmiştir. ABD merkezli büyük teknoloji şirketlerin tüm dünya nüfusunun verilerine sahip olması, dünya nüfusunun verilerini kullanarak çok yüksek oranda servetler elde etmesi ve gelecekte güç paylaşımı konusunda ciddi sorunların ortaya çıkma olasılığına dikkat çekilmiştir. Gelinen noktada bazı ülkeler veri tekelcisi olan şirketlerin gelirlerine dolaylı yollarla ortak olmak istemektedir. Ayrıca bu veri tekelciliği sadece parasal anlamda değil, sosyal, politik, kültürel, ekonomik yapıların ve uygulamaların dönüşümü için itici güç niteliğindedir. Değişimin belirtileri olarak gelişmekte olan ülkelerde para birimlerinin dolar karşısında sürekli değer kaybetmesi, işsizlik, dijital çağa uygun teknolojilerin üretilmemesi ve ithal olunan teknolojilerin çok fahiş fiyatlar ve vergilerle vatandaşlara satılması örnek olarak gösterilebilir.

Bazı ülkeler vatandaşlarının verilerini kendi ülkelerinde tutmaya yönelik dolaylı yollarla çalışmalar yapmaktadır, Çin hükümeti çağa uygun teknolojiler üreterek, arama motorları ve sosyal ağ platformlarını oluşturarak tekel teknoloji şirketlerinin ürünlerini ve hizmetlerini ülkelerinde yasaklamıştır. Gelişmekte olan ülkelerdeki hükümetler söz konusu değişime uygun politikalar sergilemek niyetinde ve kapasitesinde olmadıkları için devletin kolluk güçlerini kullanarak eski düzenin devam etmesinde ısrar etmektedirler. Sonuç olarak vatandaşlar ciddi sorunlarla karşılaşmaktadırlar.

İkinci soruda dijital dünyada siber suçları ve savaşları önlemek amacıyla ne tür tedbirlerin alınabileceği esas alınmıştır. Dünya genlinde internet bağlantılı teknolojilerin yaygınlaşmasıyla savaş yöntemleri ve araçları da değişmeye başlamıştır. İlk defa bilgisayarların askeri amaçlar için üretilmesi ve kullanılması, 1960'ların başında ağ çalışmalarının ABD Savunma Bakanlığı tarafından desteklenmesi de savaş biçimlerinin dönüşümünün habercisi olmuştur.

Dijital çağda İnsansız Hava Araçları (İHA) gibi gelişmiş silahlar eski silahlarla kıyaslandığında daha az maliyetli ve daha çok etkili hale getirilmiştir. Fakat ortada ciddi bir sorun var; tüm gelişmiş teknolojilerin büyük çoğunluğuna internet bağlantılarıyla müdahale edilebildiği için siber saldırılara her zaman açıktırlar. Yani internet bağlantısı olan tüm teknolojik cihazların veya platformların siber saldırı riskiyle karşılaşması mümkündür. Bunun yanı sıra dolaylı yollarla, yani internet bağlantısı olmasa dahi teknolojik sistemlere çeşitli yöntemlerle saldırı gerçekleştirilmiştir. Her ne kadar ülkeler arasında siber suçlarla ilgili anlaşmalar yapılsa da tam olarak güvenli bir dijital ekosistemin tesis olunması henüz mümkün olmamıştır. Ayrıca kurum ve kuruluşlar da siber saldırı tehditleri ile karşı karşıyadır. Medyada da fidye yazılımları ve farklı amaçlarla gerçekleşmiş olan siber saldırılarla ilgili haberlere sık sık rastlanmaktadır. Genel olarak dijital dünyada siber güvenlikle ilgili kapsamlı düzenlemelere ihtiyaç vardır.

Araştırmada üçüncü soruyla bağlantılı olarak dijital uçurumun nedenleri ve etkileri analiz edilmiştir. Özellikle gelişmekte olan ülkelerde dijital uçurumun çok büyük olumsuz etkileri olduğu bilinmektedir. Toplumun büyük çoğunluğu sesini duyurabilecek teknolojik araçlara ve aynı zamanda o araçları kullanabilecek düzeyde bilgiye sahip değildir. Dünya ülkelerinin yaklaşık üçte ikisinde internetin alt yapısı o

kadar kötü durumdadır ki yüksek ücretler karşılığında bile yeterli düzeyde internet hizmeti almak mümkün değildir. Kullanıcılar sürekli hükümetin kısıtlamaları, düşük internet hızı ve altyapıyla ilgili sorunlarla karşılaşmaktadır.

Eğitim ve iletişim başta olmak üzere her türlü hizmet ve imkâna online olarak erişilen bir dünyada dijital olarak dışarıda kalmış kişiler giderek daha fazla toplumun dışına itiliyorlar (Politikyol, 2021). Bugün yaş, cinsiyet, etnik köken, meslek, eğitim, milliyet ve bölge, dijital eşitsizliklerin belirleyicisi olan ana faktörler olarak karşımıza çıkıyor (Yurdakul, 2021).

Söz konusu durumu yaratan ve yöneten yöneticiler sorunları çözmek için asla çaba göstermezler. Sonuç olarak vatandaşlar fiziksel dünyada olduğu gibi dijital dünyada da temel insan haklarından mahrum bırakılmaktadırlar. Dijital dünyada medya okuryazarlığı için gereken yeterliliklere sahip olmayan vatandaşların sosyal ilişkileri geleneksel medya aracılığıyla kolaylıkla şekillendirilmekte, manipüle edilmekte ve huzur bozucu olaylara karşı çıkmaya çalışan herkes çeşitli yöntemlerle susturulmaktadır. Vatandaşların refah düzeyleri yüksek olursa bu tür olumsuz olaylara karşı mücadele etme fırsatları aratacaktır.

Tez çalışmasında dördüncü soru bağlamında dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin hakların nasıl ihlal edildiği incelenmiştir. Genel olarak insanlar kendilerini güvende hissetmedikleri ortamlardan uzaklaşmaya çalıştıkları gibi, güvenli olduğunu düşünmedikleri dijital platformları da kullanmamayı tercih ederler. Her türlü ortamda ve tüm sosyal ilişkilerde belirleyici bir etmen olarak güven her zaman ilk sırada gelmektedir. Dijital dünyada vatandaşların kişisel verilerinin hedefli reklamcılık, gözetim, ayrımcılık gibi etik olmayan amaçlarla kullanılması vatandaşları ciddi anlamda rahatsız etmektedir. Bu gibi sorunların azaltılması için yasal düzenlemelerin ve yaptırımların yeterli olmadığı bilinmektedir.

Son soruda gelişmekte olan ülkeler tarafından altyapısı hazırlanan dijital platformların ve teknolojilerin neden ulusal veya uluslararası düzeyde kabul görmediği araştırıldı. Bu soruda güven kavramı iki farklı anlamda ele alınmıştır; birincisi gelişmekte olan ülkelerde kişisel verilerin güvende olmaması, ikincisinde ise gelişmekte olan ülkelerin hukukun üstünlüğü ilkesine uygun olarak yönetilmemesinden kaynaklanan güven eksikliği olarak ele alınmıştır.

Gelişmekte olan ülkelerin bilinçli vatandaşları kendi ülkelerinde kişisel verilerinin hangi amaçlarla kullanılabileceğini az çok tahmin edebiliyorlar. Çünkü gerçek dünyada ne kadar güvendelerse dijital dünyada da o kadar güvendedirler. Aynı şekilde gelişmiş ülkelerin vatandaşları da durumun farkında olduğu için kısmen de olsa en güvenli dijital platformları ve ürünleri tercih ederler. Facebook, Instagram, X (Twitter) gibi sosyal medya şirketleri gelişmekte olan ülkelere temsilciler atarsa kullanıcıların güveninin azalacağı tahmin edilmektedir. İnsanlar gizli kullanıcı adıyla doğru hesap ettikleri fikirlerini yazıp paylaşmaktan daha çok korkacaklar. Günümüzde dijital dünyadaki belirsizlik ve güvencesizliğin hâkim olması sürekli huzursuzluğa neden olmaktadır.

### 3.5. Çalışmanın Yöntemi

Bu çalışmada araştırmanın amacına ve sorularına uygun olduğu için nitel araştırma yöntemlerinden biri olan derinlemesine görüşme yöntemi seçilmiştir. Nitel araştırma, gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konması süreci olarak tanımlanabilir (Yıldırım ve Şimşek 2021: 37).

Nitel araştırmanın geçerliliği ve güvenilirliği, araştırılan deneyimin anlaşılmasının derinleştirilmesini teşvik eden geçerli kaynakların seçilmesiyle ilgilidir (Polkinghorne, 2005: 141). Aynı zamanda nitel araştırma bir olgunun anlamını katılımcıların bakış açılarından anlamaya çalıştığı için, en önemli bilgilerin öğrenilebileceği ve amaçlı bir örneklemin seçilmesi gerekmektedir (Merriam & Grenier, 2019). Veri kaynaklarının amaçlı seçimi, araştırmacının fenomen veya deneyim hakkında önemli ölçüde bilgi edinebileceği kişi veya belgelerin seçilmesidir. Çalışmanın merkezinde yer alan araştırmacı, durumu detaylı bir şeklide tanımlar, mevcut durumu incelerken bağlantılı konulardan bahseder veya ele aldığı tek bir konuya odaklanır.

Başkalarını anlamak için derinlemesine görüşme yöntemi çok kullanılan ve en iyi veri toplama yöntemlerinden birdir. İnsanların gerçekliğe ilişkin algılarına, anlamlarına, tanımlamalarına ve gerçeği inşa edişlerine vakıf olmanın en iyi yolu derinlemesine görüşme yapmaktır (Punch & Etöz, 2005). Seçtiğimiz görüşme türü, görüşmenin yapılış biçimini ve görüşmeyi nasıl yönettiğimizi etkileyecektir (Punch,

2014:167). Görüşme türleri amacına, şekline, uzun süreli veya kısa süreli olmasına göre farklılık göstermektedir. Maxwell'e (2013) göre görüşmenin amacı araştırmacının çalıştığı konu ile ilgili bilgi birikimine sahip olan kişilere sorular sorarak onların düşüncelerinin öğrenilmesidir. Araştırma sürecinde araştırmacının da konuyla ilgili yeterli bilgi birikimine sahip olması önemlidir. Çünkü temel anlamda derinlemesine görüşme soru sorup cevap almak gibi görünse de aslında daha fazla anlam taşımaktadır. Bazı etnometodolojistlere göre görüşme verileri, dışsal gerçekliğin bir izdüşümü değil, görüşme gerçekleştirilirken iki tarafın birlikte inşa ettiği bir gerçekliktir ve böyle de incelenebilir (Punch, 2014:173).

Derinlemesine görüşme yöntemiyle yapılan nitel araştırma birden çok sayıda kaynaktan alınan verilerin bir araya getirilmesi, incelenmesi, kategorileştirilmesi ve yorumlanmasıyla gerçekleştirilmektedir. Açık uçlu soruların sorulması, dinlenmesi, cevapların kaydedilmesi ve incelenmesini gerçekleştirmek amacıyla derinlemesine görüşme yöntemi yaygın bir şekilde kullanılmaktadır (Tokmak, 2016: 83-98). İnternet bağlantılı teknolojilerin yaygınlaşmasıyla dijital ortamda yapılan derinlemesine görüşme yöntemi de literatürde yerini almıştır. Önceleri yüz yüze derinlemesine görüşme tekniğine kıyasla dezavantajları öne çıkarılan bu veri toplama tekniği pandemi ile birlikte pratik hale gelmiş ve araştırmacılar tarafından kullanımı daha da yaygınlaşmıştır (Ardahanlıoğlu, 2022). Görüşme yoluyla, deneyimler, tutumlar, düşünceler, niyetler, yorumlar ve zihinsel algılar ve tepkiler gibi gözlemlenemeyeni anlamaya çalışırız (Yıldırım ve Şimşek, 2021: 128). Derinlemesine görüşme sürecinde görüşmeci katılımcının düşüncelerini rahat ve samimi bir şekilde ifade etmesi için gereken güveni sağlamalıdır.

Görüşme sırasında alınan yanıtların nasıl yorumlanacağı da çok önemli bir konudur. Punch'a (2014:173) göre bu mesele teknik anlamda sorulara verilen yanıtların geçerliliği, görüşmecinin taraflılığı ve görüşmeyi etkileme olasılığı, soruları yanıtlayanların hafızasının güçlü olup olmaması, yanıt verme eğilimleri, dürüst olmaları ve sosyal isteklilik ile ilgilidir. Nitel araştırmacılar, katılımcıları bizzat ziyaret ederek, alanda uzun süre harcayarak ve ayrıntılı anlamlar elde etmek için derinlemesine araştırma yaparak elde edilen derin bilgi yapısını "anlamak" için çaba gösterirler (Creswell & Poth, 2016: 253).

Bu çalışmada Türkiye'de ve ABD'de dijital iletişim, veri görselleştirme, bulut veri, yazılım, siber güvenlik ve uluslararası politikalar alanında akademik çalışmalar yapmış olan bilim insanları ve uzmanlarla yarı yapılandırılmış derinlemesine görüşme gerçekleştirilmiştir. Derinlemesine görüşme, araştırılan konunun bütün boyutlarını kapsayan, daha çok açık uçlu soruların sorulduğu ve detaylı cevapların alınmasına ve görüşme esnasında duruma göre ilave soruların da sorulmasına imkân veren, fiziksel ve online ortamda birebir görüşülerek bilgi toplanmasına imkân veren bir veri toplama yöntemidir. Karşıdaki kişinin duygu, bilgi, tecrübe ve gözlemlerine görüşme yoluyla ulaşılır (Tekin, 2006: 101). Kiminle neden görüşülmesi gerektiği, kaç kişi ile görüşme yapılması gerektiği, görüşmelerin zamanı ve süresi, görüşmelerin başlatılması ve sonlandırılması araştırma sürecinde göz önünde bulundurulması gereken temel konulardır (Punch, 2014:171).

Görüşme sırasında yüz yüze ve online derinlemesine görüşme yöntemleri kullanılmıştır. Çalışmada ön test yapılarak düzenlenen beş temel soru katılımcılara sorulmuştur. Ancak beş temel sorunun yanı sıra görüşme sırasında daha detaylı bilgi edinmek amacıyla katılımcılara ilave sorular da sorulmuştur. Sorulara verilen yanıtlar uygun kategoriler altında toplanmış ve değerlendirilmiştir.

### 3.6. Çalışmanın Örneklemi

Çalışmanın evrenini, Türkiye'de ve ABD'de dijital dünyada vatandaşlık konusuyla bağlantılı çalışmalar yapmış bilim insanları ve uzmanlar, örneklemini ise, dijital iletişim, veri görselleştirme, bulut veri, yazılım, siber güvenlik ve uluslararası politikalar alanında akademik çalışmalar yapmış bilim insanları ve uzmanlar oluşturmaktadır. Çalışma evrenin büyüklüğü göz önünde bulundurularak amaçlı örnekleme (Patton, 2002) yöntemi ile seçilen 15 kişiye ulaşılmıştır. Amaçlı örnekleme, ilgilenilen özellik hakkında en fazla bilgiye sahip olan popülasyon segmenti içindeki örnekleme birimlerinin rastgele seçimi olarak tanımlanır (Guarte & Barrios, 2006: 277). Amaçlı örnekleme yöntemi, araştırma sorununun çözümüne yönelik bilgi birikimi olduğu düşünülen kişilerin seçilmesi işlemidir. Bu örnekleme türüne uygun olarak Türkiye'de ve ABD'de mail ve WhatsApp üzerinden bilim insanlarına ve uzmanlara ulaşılmış, görüşme talebini kabul eden kişilerle görüşme gerçekleştirilmiştir, veriler toplanmıştır, temalar, kategoriler ve alt kategoriler

şeklinde değerlendirilmiştir. Çalışmanın soruları 01.01.2023-30.03.2023 tarihleri arasında 15 katılımcı tarafından yanıtlanmıştır. Soru formuna (EK-1) sayfa 245'te yer verilmiştir.

Katılımcıların sayısının belirlenmesinde akademik çalışma alanları ve deneyimlerinin yanı sıra, ulaşılabilir olmaları, görüşmenin yapılacağı tarihlerde uygun olmaları ve görüşmeyi kabul etmeleri etkili olmuştur.

### 3.7. Çalışmanın Bulguları ve Yorumları

Araştırmaya katılan katılımcıların demografik özellikleri ve görüşme sorularına verdikleri yanıtların bazıları aşağıda tablolar ve yorumlar hâlinde sunulmuştur;

**Tablo 1.** Görüşme yapılan kişilerin demografik özellikleri.

| Katılımcılar | Cinsiyet | Eğitim Durumu | Mesleği | Yaş Bilgileri | İş Deneyimi (yıl) |
|---|---|---|---|---|---|
| **K1** | Erkek | Doktora | Akademisyen | 46 | 20 |
| **K2** | Erkek | Doktora | Akademisyen | 68 | 34 |
| **K3** | Erkek | Doktora | Akademisyen | 42 | 19 |
| **K4** | Kadın | Doktora | Akademisyen | 46 | 23 |
| **K5** | Erkek | Doktora | Akademisyen | 54 | 20 |
| **K6** | Erkek | Doktora | Akademisyen | 35 | 11 |
| **K7** | Erkek | Doktora | İletişim uzmanı | 41 | 15 |
| **K8** | Erkek | Doktora | İletişim uzmanı | 32 | 3 |
| **K9** | Erkek | Doktora | Uluslararası ilişikliler ve siber güvenlik uzmanı | 36 | 13 |
| **K10** | Kadın | Y/Lisans | İletişim uzmanı | 27 | -- |
| **K11** | Erkek | Lisans | Sistem uzmanı | 47 | 25 |
| **K12** | Erkek | Y/Lisans | İT uzmanı | 47 | 20 |
| **K13** | Erkek | Y/Lisans | Bulut veri mühendisi | 32 | 10 |
| **K14** | Erkek | Doktora | Veri görselleştirme uzmanı | 29 | 5 |
| **K15** | Erkek | Doktora | Siber Güvenlik Uzmanı | 33 | 6 |

Tablo 1'de görüldüğü üzere, bu çalışmada 2 kadın 13 erkek olmakla toplamda 15 katılımcıyla derinlemesine görüşme yapılmıştır. Kadınların sayının az olmasının nedeni çalışmaya katılmak talebine ağırlıklı olarak olumsuz yanıt vermeleri olmuştur.

Dijital iletişim, veri görselleştirme, bulut veri, yazılım, siber güvenlik ve uluslararası politikalar alanında çalışmalar yapmış olan bilim insanları ve uzmanlardan oluşan katılımcıların eğitim durumu dikkate alındığında Doktora derecesine sahip olanların sayısının (11 kişi) çoğunluğu oluşturduğu görünmektedir. Katılımcılardan 3'ü Yüksek Lisans programı mezunu, 1'i lisans programı mezunudur. Katılımcıların mesleği incelendiğinde 6 katılımcının Akademisyen, 3 katılımcının İletişim uzmanı, 1 katılımcının Uluslararası İlişkiler ve Siber Güvenlik uzmanı, 1 katılımcının Bulut Veri mühendisi, 1 katılımcının Sistem uzmanı, 1 katılımcının İT uzmanı, 1 katılımcının Siber Güvenlik uzmanı, 1 katılımcının Veri Görselleştirme uzmanı olduğu görülmektedir. Katılımcıların yaş durumları incelendiğinde 27-68 yaş aralığında bulundukları, deneyim durumlarına bakıldığında ise 3-34 yıl aralığında olduğu görülmektedir. Fakat Yüksek Lisans Programı mezunu ve İletişim uzmanı olan bir kişinin henüz iş deneyimi olmadığı belirtilmiştir.

Tablo 2,3,4,5,6 da görüşmeler sonucunda ortaya çıkan bulgular belirlenen temalar, kategoriler ve alt kategoriler çerçevesinde değerlendirilmiştir. Analiz yapılırken katılımcıların isimleri kullanılmamıştır, isimlerin yerine Katılımc-1, Katılımcı-2, …, Katılımc-15 şeklinde kodlama yapılmıştır. Cinsiyet bilgileri erkek (E), kadın (K) biçiminde belirtilmiştir.

**Tablo 2.** Katılımcıların dijital dünyada veri tekelciliğinden kaynaklanan sorunların çözümüne yönelik düşünceleri (**TEMA 1**).

| TEMA | KATEGORİ | ALT KATEGORİ | F |
|---|---|---|---|
| **1** | Kanunların ve yaptırımların | - Rekabet yasalarının uygulanması **(K14), (K15)** | **2** |
| | | - Tekelciliği önleyecek yasa ve politikalar izlenmeli **(K4)** | **1** |
| | | - Ancak devlet bazında uygulanacak ağır yaptırımlar ve kontroller kayda değer bir fark yaratabilir **(K7)** | **1** |

| | | | |
|---|---|---|---|
| | uygulanması | - Veri koruma yasalarının geliştirilmesi **(K14), (K15)**<br><br>- Verilerin uluslararası şirketlere pazarlanmasının önüne geçilmesi ve uluslararası hukuka yönelik düzenlemelerin yeniden yapılması **(K8)** | **2**<br><br>**1** |
| | Uluslararası düzeyde iş birliği yapmak | - Daha iyi veri erişimini sağlamak **(K14), (K15)**<br><br>- Uluslararası düzeyde iş birliği yapmak **(K15)**<br><br>- Düzenleyici kurumların yetkilerini açıklık ve netlikle belirlemek gerekiyor **(K1)**<br><br>- Çevrimiçi hizmet sağlayanların veriler üzerindeki etkisini azaltmak ve veri sağlayanlara daha fazla kontrol yetkisi vermek **(K6)**<br><br>- Veri etiği ilkelerini uygulamak **(K1)**<br><br>-Verilerin işlenmesi konusunda global düzeyde bir standardizasyon hazırlanmalı ve yasalar ülkeler tarafından kabul edilmelidir **(K12)**<br><br>- Dezavantajlı ülkeler, daha gelişmiş ülkelerle aynı veri ve araçlara erişim elde ederek dijital ekonomiye daha fazla katılmalarını sağlayabilir **(K13)**<br><br>- Verilerin ve dijital araçların ücretsiz olarak paylaşılmasına ve dağıtılmasına izin veren açık veri politikaları ve açık kaynaklı yazılımlar gibi girişimlerle başarılabilir **(K13)**<br><br>- Dezavantajlı ülkelerdeki kişi ve kuruluşlara kendi dijital platformlarını ve yeteneklerini geliştirmeleri için eğitim vermek ve kaynak sağlamak **(K13)**<br><br>- Gelişmiş ve dezavantajlı ülkeler arasında ortaklıkların teşvik edilmesi **(K13)**<br><br>- Dijital dünyadaki faydaların daha adil bir | **2**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**1**<br><br>**2** |

| | | | |
|---|---|---|---|
| | | şekilde paylaşılmasını sağlamak için hükümetleri, şirketleri ve sivil toplumu içeren çok paydaşlı bir yaklaşım gerekiyor **(K13) (K5)** | |
| | Ulusal düzeyde çözüm üretmek | - Her ülke kendi vatandaşlarının uluslararası platformlar kadar, ulusal platformlara da dahil olmasına etki edebilir **(K3)** | **1** |
| | | - Yerel ekosistemin geliştirilmesi ve çözümlerin desteklenmesi gerekiyor **(K15), (K5), (K8)** | **3** |
| | | - Sorunun çözüm için kültürel, ekonomik ve politik olarak çok boyutlu ve kapsamlı çalışmalar yapılmalıdır **(K5)** | **1** |
| | | - Devlet müdahalesinin ve kontrolünün iyimser amaçlarla artırılması gerekiyor **(K6)** | **1** |
| | | - Eğer ülkeler bu dezavantajlı konumdan kurtulmak istiyorlarsa kendi dijital sistemini modernleştirmek ve standartlarının üzerine çıkartmak zorundadırlar **(K2)** | **1** |
| | | - Teknolojik tüm araç, cihaz, yazılım ve donanımda millileşmenin gerçekleştirilmesi şarttır **(K9)** | **1** |
| | | - Teknoloji konusunda daha iyi eğitim vermek bütçeden eğitime ve ARGE çalışmalarına daha fazla olanak sağlamak **(K11)** | **1** |
| | Açık veri kullanımını ve erişimini yaygınlaştırmak | - Verilere ve dijital platformlara açık erişimi teşvik etmek (K7), (K13) | **2** |
| | | - Verileri üreten kurum ve kuruluşlara açık veri konusunda eğitim vermek **(K7)** | **1** |
| | | - Veri akışının dengeli olarak paylaşılmasını olanaklı hale getirmek **(K10)** | **1** |

Tablo 2'ye göre, katılımcıların büyük bir kısmı (12 kişi) veri tekelciliğinden kaynaklanan sorunların çözülmesi için uluslararası düzeyde iş birliğinin önemli olduğunu bildirmiştir. Bu yaklaşımlar veri tekelciliğinden kaynaklanan sorunların uluslararası düzeyde kapsamlı ve çok boyutlu çözüm gerektirdiğini ortaya koymaktadır. Aynı zamanda katılımcılar (9 kişi) veri tekelciliğinden kaynaklanan

sorunların çözümüne yönelik ulusal düzeyde de tedbirlerin alınması gerektiğini belirtmiştir.

Katılımcıların yaklaşık yarısı (7 kişi) dijital dünyada veri tekelciliğinden kaynaklanan sorunların gereken kanunların ve yaptırımların uygulanması yoluyla çözülebileceğini vurgulamıştır. Katılımcıların küçük bir kısmı (4 kişi) açık veri yaklaşımının da olumlu etki yapabileceğini bildirmiştir.

Kanunların ve yaptırımların uygulanması kategorisindeki yanıtların bir kısmında ulusal, bir kısmı ise uluslararası düzeyde faydalı olabileceği belirtilmiştir. Dijital demokrasiyi sağlayabilmek için 2 kişi rekabet yasalarının uygulanması gerektiğini, 1 kişi veri tekelciliğini önleyecek yasa ve politikaların izlenmesi gerektiğini, 2 kişi veri koruma yasalarının geliştirilmesi gerektiğini bildirmiştir. Yanı sıra 1 kişi verilerin uluslararası şirketlere pazarlanmasının önüne geçilmesi ve uluslararası hukuka yönelik düzenlemelerin yeniden yapılması gerektiğini, 1 kişi ise devlet bazında uygulanacak ağır yaptırımların ve kontrollerin kayda değer bir fark yaratabileceğini vurgulanmıştır.

Uluslararası düzeyde iş birliği kategorisinde 2 kişi daha iyi veri erişiminin sağlanması gerektiğini, 1 kişi uluslararası düzeyde iş birliği yapılması gerektiğini, 1 kişi hükümetlerin ve özel sektörün düzenleyici kurumların yetkilerini açıklık ve netlikle belirlemeleri gerektiğini, 1 kişi çevrimiçi hizmet sağlayanların veriler üzerindeki etkisini azaltmak ve veri sağlayanlara daha fazla kontrol yetkisinin verilmesi gerektiğini, 1 kişi veri etiği ilkelerinin uygulanması gerektiğini, 1 kişi verilerin işlenmesi konusunda global düzeyde bir standardizasyonun hazırlanması ve yasaların dünya ülkeleri tarafından kabul edilmesi gerektiğini, 1 kişi dezavantajlı ülkelerin gelişmiş ülkelerle aynı veri ve araçlara erişimi konusunda iş birliği yaparak dijital ekonomiye daha fazla katılım sağlayabileceklerini, 1 kişi verilerin ve dijital araçların ücretsiz olarak paylaşılmasına ve dağıtılmasına izin veren açık veri politikaları ve açık kaynaklı yazılımlar gibi girişimlerin gerçekleştirilmesi gerektiğini, 1 kişi dezavantajlı ülkelerdeki kişi ve kuruluşlara kendi dijital platformlarını ve yeteneklerini geliştirmeleri için eğitim vermek ve gereken kaynakların sağlanmasının faydalı olabileceğini, 1 kişi gelişmiş ve dezavantajlı ülkeler arasında ortaklıkların teşvik edilmesi gerektiğini, 2 kişi dijital dünyanın faydalarının daha adil bir şekilde paylaşılmasını sağlamak için hükümetleri, şirketleri

ve sivil toplumu içeren çok paydaşlı bir yaklaşımın uygulanması gerektiğini önermiştir.

Katılımcıların ulusal düzeyde önerdiği tedbirlere değerlendirildiğinde hükümetlerin daha fazla sorumluluk üstlenmesi gerektiği belirtilmiştir. Katılımcılardan 1 kişi her ülkenin kendi vatandaşlarının uluslararası platformlar kadar, ulusal platformlara da dahil olmasına etki etmesini, 3 kişi yerel ekosistemin geliştirilmesi ve çözümlerin desteklenmesini, 1 kişi sorunun çözüm için kültürel, ekonomik ve politik olarak çok boyutlu ve kapsamlı çalışmaların yapılmasını, 1 kişi devlet müdahalesinin ve kontrolünün iyimser amaçlarla artırılmasını, 1 kişi ülkelerin dezavantajlı konumdan kurtulmak istemeleri durumunda kendi dijital sistemini modernleştirmeleri ve standartların üzerine çıkartmak zorunda olduklarını, 1 kişi tüm teknolojik araç, cihaz, yazılım ve donanımda millileşme politikalarının gerçekleştirilmesi gerektiğini, 1 kişi teknoloji konusunda daha iyi eğitim vermek, bütçeden eğitim ve ARGE çalışmaları için daha fazla olanak sağlamanın dijital dünyadaki dengeleri değiştirebileceğini belirtmiştir.

Açık veri kullanımının ve erişiminin yaygınlaştırılması kategorisinde katılımcılardan 2 kişi verilere ve dijital platformlara açık erişimin teşvik edilmesi gerektiğini, 1 kişi verileri üreten kurum ve kuruluşlara açık veri konusunda eğitim verilmesi gerektiğini, 1 kişi ise veri akışının dengeli olarak paylaşılmasının olanaklı hale getirilmesi gerektiğini belirtmektedir.

Katılımcıların dijital dünyada veri tekelciliğinden kaynaklanan sorunların çözümüne yönelik verdiği yanıtlardan bazıları aşağıda yer almaktadır;

**K1 (E, 46):** *Hükümetlerin mevzuatının karmaşık ve bölük pörçük bir yapıya sahip olduğu, yetkilerin çakıştığı ve çeşitli kurumların aynı alanda sorumluluğu olduğu belirtilmektedir. Bu nedenle, hükümetlerin ve özel sektörün veri tekelciliğine karşı mücadele etmek için düzenleyici kurumların yetkilerini açıklık ve netlikle belirlemeleri gerekmektedir.*

*Veri etiği, verinin nasıl toplanması, saklanması, kullanılması ve paylaşılması gerektiği konusunda kuralları içermektedir. Bu ilkelerin uygulanması, veri tekelciliğinin önüne geçecek ve dezavantajlı ülkelerin veri haklarının korunmasını sağlayacaktır.*

**K2 (E,68):** *Eğer ülkeler bu dezavantajlı konumdan kurtulmak istiyorlarsa kendi dijital sistemini modernleştirmek, yenileştirmek ve standartlarının üzerine çıkartmak zorundadırlar. Dünyada gelir düzeyi düşük ama dijitalleşme konusunda son derece başarılı olan ülkeler de var. Ve dolayısı ile bu konuda oldukça güzel yatırım yapan güzel çalışan ülkeler var. Özetle mutlaka dijital alt yapı için yatırım yapmak ve saldırılara karşı önlem almak lazım.*

**K3 (E,42):** *Kullandığımız şirketler büyük ölçüde, belki yüzde 95'i ABD merkezli şirketlerdir. Ruslar ve Çinliler kendi şirketlerini geliştirmeye çalışıyorlar, biraz da ulusallaşmaya gidiyorlar. Böyle bir şey olabilir. Yani her ülke kendi vatandaşlarına uluslararası platformlarda olduğu gibi, biraz ulusal platformlara da dahil olmalarına etki edebilir.*

**K4 (K, 46):** *Tekelciliği önleyecek yasa ve politikalar izlenmeli. Ayrıca yönetimleri bu önlemleri almaya zorlayabilecek bilinçli vatandaşlara da çok ihtiyaç var.*

**K5 (E, 54):** *Bu işin teknolojisini ve altyapısını üreten büyük teknoloji şirketleri ister istemez bu verileri toplayacaklar. Dolayısıyla bu alanda bir rekabet oluşuyorsa bu teknolojileri üretenler ön planda olacaklar. Bu teknolojilerin üretiminde az gelişmiş veya gelişmekte olan ülkeler zaten geriden bir noktada başladıklarından dolayı, doğal olarak böyle bir süreç var. Sorunun çözümü için kültürel, ekonomik ve politik olarak çok boyutlu ve kapsamlı çalışmalar yapılmalıdır. Çözüm olarak, yönetimler avantajlı konuma gelebilmek için gelişmiş ülkelerde olduğu gibi gereken koşulları ve ortamı oluşturabilirler.*

**K6 (E, 35):** *Dijital dünyada veri tekelciliği ve olumsuz etkilerini azaltmak amacıyla aşağıdaki önlemler alınabilir:* ***a.*** *Çevrimiçi hizmet sağlayanların veri üzerindeki etkisini azaltmak ve veri sağlayanlara daha fazla kontrol yetkisi vermek.* ***b.*** *Devlet müdahalesinin ve kontrolünün iyimser amaçlarla artırılması.*

**K7 (E, 41):** *Büyük verilerin büyük teknolojik firmaların elinde bulunması veri tekelciliğinin oluşmasını sağlamaktadır. Veri tekelciliğini önlemenin en önemli adımlarından biri açık veri kullanımını yaygınlaştırmaktır. Açık veri yaklaşımı tüm verilerin açık ve şeffaf olması gerektiğini savunmaktadır. Verilerin herkes tarafından kullanılabilmesi açısından açık olması önem taşımaktadır. Verilerin açık olması sayesinde veri tekelciliğinin önüne geçilebilir.*

*İkinci adım ise verileri üreten kurum ve kuruluşlara açık veri konusunda eğitim verilmesidir. Eğitim ile veriden enformasyon ve bilgi üretme yeteneği sadece veriye sahip olan kamu kurum ve kuruluşlarıyla sınırlı kalmayarak daha şeffaf bir hale gelecek ve böylelikle veri tekelciliği ortadan kalmış olacaktır.*

*Artık büyük teknoloji şirketleri, kullanıcıların hayatıyla ilgili en temel noktalara bile nüfuz etti ve kullanıcılar veri aktaran donanımlarından vazgeçmek niyetinde değil (telefon, bilgisayar destekli arabalar, saat, kredi kartları vb.), üstelik dezavantajlı ülkelerin yaşadığı sorunlar da kullanıcıları rahatsız etmiyor. Bu yüzden kişisel girişimlerin ya da STK'ların veya "darkweb" gibi illegal yapıların üreteceği çözümlerin kalıcı ya da fark yaratacak boyutta olamayacağı hem deneyimlerimiz hem de çıkarımlarımız yoluyla sabit.*

*Kâr amaçlı oluşumlarla (veri şirketleri) ancak kâr amaçlı olmayan yapılar mücadele edebilir. Bu yüzden devlet bazında uygulanacak ağır yaptırımlar ve devlet eliyle yapılacak kontroller ancak kayda değer bir fark yaratabilir. Devletten kastım kapitalizm öncelikli, neoliberal olmayan devletlerdir. Zira kapitalizm tabanlı devletlerin zaten veri tekelcileri tarafından desteklendiği bir gerçektir. Üstelik bunlar uluslararası yapılarda önemli bir oya da sahip. Sonuç olarak; ciddi ve istikrarlı devlet politikaları ve yasalar yolu ile yapılacak mücadele en etkin yol gibi görünse de veri tekelciliği ile mücadele; yüzyılın başlarında petrol tekelciliği ile yapılan mücadele kadar başarılı olabilecek gibi, bütüncül bir çözümden ziyade, ülkesinin çıkarlarını öncelikli gören devletlerin ülkesinde sınırlı alanda başarılı olabilecek bir mücadele olacak.*

**K8 (E, 32):** *Veri tekelciliği veriye yönelik kişisel hakların tehdit edilmesi ve ülkeler arasında emperyal sürecin yaratılmasına neden olmaktadır. Bu anlamda her ülkenin kendilerine yönelik veri depolarının oluşturulması, açık veri paylaşımının*

*uluslararası şirketlere pazarlanmasının önüne geçilmesi ve uluslararası hukuka yönelik düzenlemelerin yeniden yapılması çözüm önerileri arasında yer almaktadır.*

**K9 (E, 36):** *Veriler yapay zekâyı besleyen en önemli madendir. Dolayısıyla veri, stratejik bir iş varlığıdır. Yapay zekâ devriminde herkes veriyi etkin ve etik şekilde koruyup kullanmaktan sorumludur. Böylece ülkeler stratejilerini, bilgi işlem yetenekleri ve veri paylaşımı gibi çeşitli boyutları temel alarak belirlemeye başlamıştır. Bazı ülkelerin güçlü siyasi ve ekonomik bir dijital alt yapısı mevcutken, çoğunun siber saldırı veya savunma gücü zayıftır. Bu noktada veri tekelciliğinin ortaya çıkardığı olumsuz etkilerden en az şekilde etkilenmek için özellikle tüm teknolojik araç, cihaz, yazılım ve donanımda millileşmenin gerçekleştirilmesi şarttır. Siber uzayın mevcut koşullarında veri tekelciliği sorununun önüne geçilememesi halinde siber ortamın gizlilik, bilinmezlik ve inkâr edilebilirlik gibi özelliklerinden faydalanılması kolaylaşacaktır. Bu durum risk ve tehditleri artıracaktır.*

**K10 (K, 27):** *Veri tekelciliğinin ortaya çıkmasındaki en önemli unsur ekonomik güçtür. Ekonomisi güçlü ülkeler verileri de elinde bulundururlar. Dezavantajlı ya da ekonomik olarak gelişmemiş ülkeler ise verilere ulaşmakta güçlük çekmektedir. Çözüm olarak ise veri kontrolünün dezavantajlı ülkelerde bulunamayacağı ya da tekelleşmenin önüne geçilemeyeceği için veri akışının dengeli olarak paylaşılmasını olanaklı hale getiren adımların atılması gerekmektedir.*

**K11 (E, 47):** *İlk etapta teknoloji alanında daha iyi eğitim vermek, bütçeden eğitim, altyapı ve ARGE çalışmaları için daha fazla olanak sağlamak gerekiyor.*

**K12 (E, 47):** *Öncelikle toplanan verinin niteliği, hangi amaçla ve hangi hizmet sebebiyle toplandığı çok net ifade edilmelidir. Son yıllarda çıkan GDPR/KVKK gibi yasalarla toplanacak veriler regüle edilmeye çalışılsa da diğer ülkeler için henüz bu tür yasalar çıkmadığı için global olarak geçerli değil. İlk etapta global düzeyde bir standardizasyon gerekli olmakla birlikte toplanan verinin işlenmesi ile ilgili de çeşitli yasalar ülkelerin katılımıyla ortak mutabakat olarak çıkartılmalıdır.*

**K13 (E, 32):** *Dezavantajlı ülkeleri dijital dünyaya dahil etmek için olası bir çözüm önerisi, verilere ve dijital platformlara açık erişimini teşvik etmektir. Bu, verilerin ve dijital araçların ücretsiz olarak paylaşılmasına ve dağıtılmasına izin veren açık veri politikaları ve açık kaynaklı yazılımlar gibi girişimlerle başarılabilir. Dezavantajlı ülkeler, açık erişimi teşvik ederek, daha gelişmiş ülkelerle aynı veri ve araçlara erişim elde ederek dijital ekonomiye daha fazla katılım sağlayabilir.*

*Diğer bir olası çözüm önerisi ise dezavantajlı ülkelerdeki kişi ve kuruluşlara kendi dijital platformlarını ve veri yeteneklerini geliştirmeleri için eğitim ve kaynak sağlamaktır. Bu, bireylerin ve kuruluşların kendi dijital çözümlerini geliştirmelerine yardımcı olmak için fon, mentorluk ve uzmanlığa erişim sağlayabilen teknoloji inkübatörleri ve eğitim programları gibi girişimlerle etkili olabilir.*

*Ayrıca gelişmiş ve dezavantajlı ülkeler arasında ortaklıkların teşvik edilmesi de olası bir çözüm önerisi olabilir. Bu ortaklıklar, dezavantajlı ülkelerde kapasite oluşturmaya, verilere ve dijital platformlara erişimi iyileştirmeye yardımcı olabilecek teknoloji transferini sağlamak, bilgi ve kaynakların paylaşımını, ortak araştırma ve geliştirme girişimlerini içerebilir.*

*Genel olarak, açık erişimi teşvik etmek, eğitim ve kaynak sağlamak, ortaklıkları teşvik etmek, dezavantajlı ülkeleri dijital dünyaya dahil etmek ve veri tekelinin olumsuz etkilerini azaltmak için olası çözüm önerileridir.*

*Bunlar, veri tekelciliğini ele almak ve dezavantajlı ülkelerin dijital dünyaya daha fazla dahil edilmesini teşvik etmek için olası çözümlerden sadece birkaçıdır. Nihayetinde, dijital dünyanın faydalarının daha adil bir şekilde paylaşılmasını sağlamak için hükümetleri, şirketleri ve sivil toplumu içeren çok paydaşlı bir yaklaşım gerekiyor.*

**K14 (E, 29):** *Dezavantajlı ülkeler, veri koruma yasalarını geliştirerek, kullanıcıların verilerinin kötüye kullanılmasını önleyebilirler. Bu yasalar, veri tekelciliği ile mücadele etmek için önemli bir araç olabilir.*

*Veri tekelcileri, pazar hakimiyetlerini kötüye kullanarak rekabeti engellemektedirler. Dezavantajlı ülkeler, bu sorunu çözmek için mevcut rekabet yasalarını uygulayabilirler.*

*Dezavantajlı ülkeler, veri tekelciliği ile mücadele etmek için daha iyi veri erişimi sağlayarak, kendi veri kaynaklarını geliştirebilirler. Bu, ülkelerin dijital ekonomide daha fazla söz sahibi olmasına yardımcı olabilir.*
*Dezavantajlı ülkeler, diğer ülkelerle iş birliği yaparak veri tekelciliği sorununu çözebilirler. Uluslararası iş birliği, veri tekelciliği sorununun çözümünde önemli bir faktördür.*

**K15 (E, 33):** *Veri tekelciliğinin ekonomik, toplumsal ve bireysel açıdan olumsuz etkilerini azaltmak için özel ya da kamu kurumları ve kuruluşları arasında veri paylaşımını teşvik etmek, verilerini paylaşan kurum ve kuruluşları teşvik etmek, yerel ekosistemi ve çözümleri desteklemek, verilerin güvenilir bir şekilde işlenebilmesi için inşa edilecek mevzuat altyapısı, rekabet ve uluslararası iş birliği gibi etkili adımlar atılabilir.*

**Tablo 3.** Katılımcıların dijital dünyada siber suçların ve savaşların önlenmesine yönelik alınabilecek tedbirler ve siber saldırılarla ilgili ülkeler arasında yapılan anlaşmaların güvenirliliğine ilişkin düşünceleri (**TEMA 2**).

| TEMA | KATEGORİ | ALT KATEGORİ | F |
|---|---|---|---|
| **2** | Teknik tedbirler | -Güçlü güvenlik önlemleri uygulamak **(K1)**, **(K2)**, **(K5), (K7), (K13)** | **5** |
| | | -Daha iyi teknolojik altyapı hazırlamak **(K1)**, **(K4)**, **(K14)** | **3** |
| | | -Siber saldırıları ve savaşları önleyici tedbirleri en başta işletim sistemi üreticilerinin alması gerekmektedir **(K12)** | **1** |
| | | - CEH ve CISSP gibi yüksek güvenlik sertifikalarına sahip uzmanlar çalıştırmak veya onlardan destek almak **(K11)** | **1** |
| | Hukuki düzenlemeler | -Dijital güvenlik yasalarının geliştirilmesi **(K9), (K14)** | **2** |
| | | -Uluslararası normlar ve standartlar geliştirmek **(K3)**, **(K9), (K13)** | **3** |
| | | -Uluslararası kurumlar tarafından | **2** |

| | | | |
|---|---|---|---|
| | | uluslararası standartların hazırlanması ve uygulanması **(K3)**, **(K9)** | |
| | Diplomatik tedbirler | -Uluslararası iş birliğinin güçlendirilmesi **(K4)**, **(K9), (K13), (K14)** | **4** |
| | | -Kullanıcıların haklarını güvence altına almak amacıyla uluslararası düzeyde bir yaptırım mekanizması geliştirilebilir **(K8)** | **1** |
| | Eğitim ve farkındalık | -Daha iyi eğitim vermek ve farkındalık yaratmak **(K13), (K14)** | **2** |
| | | -Siber savunma yeteneklerinin geliştirilmesi **(K6), (K7), (K8), (K13)** | **4** |
| | Çeşitli önlemleri içeren çok yönlü bir yaklaşım | -Savunmanın her alanında nasıl bir yaklaşım sergileniyorsa aynı şekilde tedbir alınmalıdır **(K7), (K10), (K13), (K14), (K15)** | **5** |
| | | -Kapsamlı önleyici tedbirlerin alınması gerekiyor **(K3)**, **(K5), (K9), (K13)** | **4** |
| | Siber suçlara karşı ülkeler arasındaki anlaşmaların güvenilirliği | -Belirli anlaşmalara ve katılımcı ülkelerin taahhüt düzeyine bağlıdır **(K6), (K7), (K13)** | **3** |
| | | -Ülkeler arasında yapılan anlaşmalar kısmen işe yarar **(K8), (K3)** | **2** |
| | | -Ülkeler arasında yapılan anlaşmalar güvenilir olmayacak **(K4)**, **(K5), (K10), (K11), (K12)**, **(K14)** | **6** |

Çalışma kapsamında katılımcılara sorulan ikinci soru aslında iki kısımdan ibarettir. Birinci kısımda siber suçların ve savaşların önlenmesine yönelik alınabilecek tedbirlerin neler olabileceği, ikinci kısımda ise siber saldırılarla ilgili ülkeler arasında yapılan anlaşmaların güvenilir olup olmayacağı sorulmuştur.

Tablo 3'e bakıldığında, katılımcılar siber suçların ve savaşların önlenmesine yönelik alınabilecek tedbirlere ilişkin ağırlıklı olarak teknik tedbirlerin alınması ve hukuki düzenlemelerin geliştirilerek uygulanmasına dikkat çekmiştir. Bu önerilerden yola çıkarak günümüzde dijital evrende uluslararası düzeyde dezavantajlı ülkeleri de kapsayan teknik ve hukuki standardizasyonun henüz oluşturulmadığı

anlaşılmaktadır. Tablo 3'te göründüğü gibi teknik tedbirlerin alınması konusunda 10 kişi, hukuki düzenlemeler yapılması konusunda 9 kişi, çeşitli önlemleri içeren çok yönlü bir yaklaşımın önemli olduğunu 9 kişi, eğitimin önemi ve farkındalık yaratmak konusunda 6 kişi, diplomatik tedbirler görülmesi konusunda 5 kişi benzer düşünceleri paylaşmıştır.

Katılımcıların yaklaşık yarısı (6 kişi) siber saldırılara karşı ülkeler arasında yapılan anlaşmaların güvenilir olmayacağını belirtmiştir, 3 kişi anlaşmaların katılımcı ülkelerin taahhüt düzeyine bağlı olduğunu, 2 kişi ise ülkeler arasında yapılan anlaşmaların kısmen işe yarayacağını belirtmiştir.

Teknik tedbirler kategorisinde 5 kişi daha güçlü güvenlik önlemlerinin alınması gerektiğini, 3 kişi daha iyi teknolojik altyapının hazırlanması gerektiğini, 1 kişi siber saldırıları ve savaşları önleyici tedbirlerin en başta işletim sistemlerini üretenler tarafından alması gerektiğini, 1 kişi CEH ve CISSP gibi yüksek güvenlik sertifikalarına sahip uzmanların çalıştırılması veya onlardan destek alınması gerektiğini önermiştir.

Hukuki düzenlemeler kategorisindeki yanıtlara bakıldığında 2 kişi dijital güvenlik yasalarının geliştirilmesini, 3 kişi uluslararası normlar ve standartların geliştirilmesini, 2 kişi uluslararası kurumlar tarafından uluslararası standartların hazırlanmasını ve uygulanmasının mühim olduğunu dile getirmiştir.

En etkili çözümlerden biri olabilecek diplomatik tedbirler kategorisinde 4 kişi uluslararası iş birliğinin güçlendirilmesi gerektiğini, 1 kişi kullanıcıların haklarını güvence altına almak amacıyla uluslararası düzeyde bir yaptırım mekanizmasının geliştirilmesi gerektiğini vurgulamıştır.

Eğitim ve farkındalık kategorisindeki öneriler kısmında daha iyi eğitim vermek ve farkındalık yaratmak 2 kişi, siber savunma yeteneklerinin geliştirilmesi, savunmanın her alanında nasıl bir yaklaşım sergileniyorsa aynı şekilde tedbirin alınması, kapsamlı önleyici tedbirlerin alınması gerektiğini 1 kişi ifade etmiştir.

Çeşitli önlemleri içeren çok yönlü bir yaklaşım gerektiği konusunda 9 kişi fikirlerini paylaşmıştır. 5 kişi tarafından savunmanın her alanında nasıl bir savunma yaklaşımı sergileniyorsa aynı şekilde tedbirin alınması, 4 kişiye göre ise kapsamlı önleyici tedbirlerin alınması gerektiği ifade edilmektedir.

Dijital dünyada veri tekelciliğinden kaynaklanan sorunların çözümüne yönelik verilen yanıtlardan bazıları aşağıda yer almaktadır;

**K1 (E, 46):** *Siber suçlar e-posta ve internet dolandırıcılığı, kimlik dolandırıcılığı, finans veya kart bilgilerinin çalınması, kurumsal verilerin çalınması ve satılması, siber gasp ve fidye yazılımı saldırıları gibi farklı türlerde olabilir. Bu nedenle, siber suçların türlerinin bilinmesi ve güvenlik önlemlerinin alınması önemlidir.*

*Güncel siber güvenlik trendlerini takip etmek ve yatırım yapmak gerekiyor. 2023'de farklı türlerdeki siber saldırıların hayatımıza gireceği ve güvenlik altyapısına yeterli yatırım yapmamış pek çok şirketin zor durumda kalabileceği görülmektedir. Bu nedenle, kuruluşların güncel siber güvenlik trendlerini takip etmeleri ve yatırım yapmaları önemlidir.*

*"Siber Savaş" ise artık bireyi aşan bir meseledir ve devlet ve kurumlar düzeyinde savunma hazırlıkları gerekir. Bu tip savaşlar için daha hazırlı olunacak bir döneme girildiğini düşünüyorum.*

**K2 (E,68):** *Yaşadığımız çağda Siber savaş, Siber saldırı, Siber güvenlik ve Siber casusluk konuları son derece önemlidir. 21 yılda hareket sırasında 4 boyut var; kara, deniz, hava ve siber boyut. Siber boyut en önemlisidir. Bugünkü dünyada devletler birine siber saldırı yaptığı zaman bu saldırının mutlaka kareden yapılması gerekmiyor, mesela denizdeki bir gemiden de yapabiliyorlar. Hatta Siber saldırının yapıldığı kaynağı da tespit etmek zor oluyor.*

*Siber saldırı ve Siber savaşa karşı devletlerin mutlaka kendilerinin dijital altyapılarını güçlendirmesi için milli bir politika izlemesi lazım. Siber saldırılara karşı sadece jandarmanın, polisin, istihbarat teşkilatları gibi güvenlik kuvvetlerinin önlem alması yeterli olmaz, bütün kurum ve kuruluşların bu konuda hazırlıklı olması gerekiyor. Çünkü Siber saldırı olduğunda örneğin ülkenin bütün hava ve kare trafiği engellenebilir, iletişim sistemi etkisiz hale getirilebilir, Bütün ulaşım sistemleri çalışmayabilir, bankacılık sistemi çalışmayabilir ve ülkenin enterkonnekte elektrik sistemi devre dışı bırakılabilir. Bunlar ister istemez ülkede hayatı zor duruma sokar. Siber saldırılarda herhangi bir nükleer veya konvansiyonel silah kullanılmasa da çok fazla zarar vermesi mümkündür.*

*Meselen Rusya-Ukrayna Savaşı'nda bile Rusya Ukrayna'ya havadan ve karadan saldırmadan önce Siber saldırılar uyguladı. Ülkenin elektronik altyapısını ve iletişim sistemlerini nötr hale getirmeyi hedefledi. Ondan sonra havadan ve karadan operasyonu başlattı.*

*Her zaman Siber saldırıların gerçekleşme ihtimali vardır. Aslında Sibel Savaş şu anda hem ulusal bazda hem de uluslararası bazda devamlı devam ediyor, yani siber savaş bitmedi ve bitmeyecektir de artan hızıyla devam edecektir. Her ülke bu ortamda siber savaşın aralıksız devam ettiğini kabul ederek kendi sistemlerini modernleştirerek bu konuda önlem almak zorundadır.*

**K3 (E,42):** *Bir ülkenin siber güvenliğini koruyan kişi, o ülkenin hava sahasını koruyan pilotu gibi önemlidir. Bu nedenle Siber güvenliği sağlamak için yatırım yapılması gerekiyor.*

*Örneğin BM tarafından internette kişi haklarının korunmasına ilişkin uluslararası sözleşme hazırlayıp tüm ülkelere imzalatılabilir ve caydırıcı yaptırımlar düşünülebilir. Özellikle agresif yöntemlerle siber saldırılar yapan devletlere karşı yaptırımlar uygulanmalıdır.*

*Uluslararası bir kurumun çatısı altında uluslararası anlaşmalar yapılmalıdır. Peki bu imzalama işe yarayacak mı? Kısmen yarar, tabii ki bitirmez. Amma hiçbir önlem almamaktan iyidir. Saldıranlara karşı sıkı yaptırımlar getirerek çağa uygun hale getirilebilir.*

**K4 (K,46):** *Her devletin kendi sistemlerine dair güvenlik duvarları ve ekipleri olmalı, uluslararası platformda da bunu geliştirmek için iş birliğine ihtiyaç var. Siber saldırılarla ilgili anlaşmaların güvenilir olduğunu düşünmüyorum.*

**K5 (E,54):** *Sanal ortamda illegal eylemlerin aşırı derecede yapıldığı darknet denilen bir yer var. Bu alanın kontrol altına alınabileceği tek bir yer o işlemlerin yapıldığı fiziksel olarak sunucuların bulunduğu yerdir. Onun dışında kimse kontrol altına alamaz. Sunucularda dünyanın her tarafındadır. Bu tek merkezden kontrol edilebilir bir olay değil. Zaten internetin güzelliği de o, ama kimine göre kötülük olarak da yorumlanabilir. Bu durum internetin hangi amaçla kullanıldığına bağlıdır. Güzellik*

*dediğim kontrol edilemez olmasıdır. Verilerin korunması için oluşturulan güvenlik duvarları yüksek maliyet talep eden teknolojilerdir. Verilerin üretilmesinden korunması daha zordur.*

*Bazen de siber saldırıların uluslararası yasaların geçerli olmadığı ülkelerde gerçekleştiği bilinmektedir. Siber saldırıların gerçekleşme süreciyle ilgili bir belirsizlik de vardır. Kimin nereden siber saldırı düzenlediğini tespit etmek günümüz koşullarında kolay değildir. Çünkü ileri düzeyde hacking yapanlar kendilerine gizlemenin yollarını da bulabiliyorlar. Onları takip ederek tespit etmek mümkündür. VPN üzerinden adres değiştirmek saklanmak için çözüm değil. Yani VPN kullansalar dahi bulunmaları mümkündür.*

*İki ülkenin masa başında bir kâğıt üzerinde imza atarak birbirimize siber ortamda saldırmayacağız demesi saldırıları engellemez.*

**K6 (E, 35):** *Dijital dünyada siber suçları önlemek amacıyla aşağıda sıralanan önlemler alınabilir; Yönetici girişi gibi önemli bölümlere girişlerde iki aşamalı kimlik doğrulama yöntemi mutlaka kullanılmalıdır, reklam virüslerine karşı dikkatli olunmalıdır ve internetteki eski veri girdileri temizlenmelidir, arama motoru optimizasyonu konusunda HTTPS kullanılmalıdır ve güvensiz eklentiler kabul edilmemelidir.*

*Siber suçlara yönelik ülkeler arasında yapılan anlaşmalar güvenli olabilir, fakat bu anlaşmaların seyrini devletlerarası siyasi ilişkiler belirler.*

**K7 (E, 41):** *Siber saldırıların ve savaşların, herhangi bir saldırı ve savaş gibi değerlendirilmesi gerektiği kanaatindeyim. "Barışı korumanın en iyi yolu düşmanı saldırmaya korkacak kadar yıldırmaktır" düsturundan hareketle, siber savaş konusunda en bilgili ve yetenekli siber orduya sahip olmak saldırılardan korunma ya da savaşlardan kaçınma (başka seçenek kalmazsa savaşa girip kazanma) için tek seçenek. Ancak "siber saldırı ve savaşları önlemek için ne tedbirler alınmalıdır? sorusunun yanıtı: önlemek mümkün değildir. "Si vis pacem para bellum" olacaktır.*

*Ülkeler arasında yapılan anlaşmaların güvenilirliği ise tamamen hangi ülke ile yapıldığı, ile ilgilidir. Bazı ülkelerle yapılan anlaşmalar güvenilir olabilir, bazıları olmaz.*

**K8 (E, 32):** *Çözüm olarak dijital dünyada kullanıcıların haklarını güvence altına almak amacıyla uluslararası düzeyde bir yaptırım mekanizması geliştirilebilir. Aynı zamanda tüm kullanıcıları siber tehlikelerin farkında olmaları konusunda bilgilendirmek faydalı olacaktır.*
*Siber saldırıları önlemek için tabii ki uluslararası anlaşmalar önemlidir, ama sorunları azaltmak ya da önlemek için yeterli değildir.*

**K9 (E, 36):** *Siber güvenlik alanında tüm aktörlerin özgürlüklerini, eşitliklerini, haklarını korumak amacıyla bir iş birliği modelinin geliştirilmesine yönelik siber uzaydaki faaliyetlerin kolay ölçülebilen kuralları hazırlayan ve bu kuralları denetleyen bir üst otorite kurumun oluşturulması zorunluluktur.*
*Bu kurumun kontrol mekanizması ulusal ve uluslararası ortak hukuk prensipleriyle var olabilir. Bu prensip siber uzayın ağ bütünlüğü içinde ele alınmasını ve ağ yöneticisinin astın eylemlerinden sorumlu olmasını gerekli kılacaktır.*
*Avrupa Siber Suçlar Sözleşmesinden ve evrensel siber hukuk kurallarından yararlanılarak tarafların yükümlülükleri belirlenebilir. Uluslararası toplum ile birlikte uluslararası hukuk kuralları ortaya konur ve böylece ülkelerin kendini savunma esasları belirlenebilir. Böyle bir hukuki çerçeve ile saldırganlığın hangi koşullarda oluşacağı tarif edilebilir. Dolayısıyla her devletin sorumluluklarını yerine getirmesi mecburiyeti ortaya çıkar ve uluslararası toplumun bu konuda zorlayıcı tedbirler alması mümkün hale gelecek.*
*BM Sözleşmesi, Lahey ve Cenevre Sözleşmeleri ve ilgili antlaşmalar devletler arasındaki "kuvvet kullanımının hukuki sonucu", "güç kullanımı", saldırganlık ve savaş eylemlerini değerlendirmenin tek temelidir. BM tarafından ortaya konacak yaptırımlar veya cezai eylemler siber saldırganlar için güçlü bir caydırıcılık yaratmalıdır.*
*Enformasyon teknolojisinin tüm araçları donanım, yazılım, yeni uydular, fiber kablolar, bilgisayar ağları vb. siber metalaşmayı doğurmuştur. Siber metalaşmaysa siber mülkiyet ihtiyacını tetiklemiştir. Siber uzay kimindir? Kim kontrol etmelidir? Kim ne kadar yetkiye sahiptir? Gibi birçok sorunun konuşulmasıyla bu alanda hakkını aramak veya bu alandaki fırsatlardan yararlanmak isteyen tüm aktörler de siber saldırılara yoğunlaşmıştır.*

**K10 (K, 27):** *Siber saldırıların önüne geçmek zor olsa da bu doğrultuda dijital ortamda bulunan kurum ve kuruluşlar veya şirketler siber saldırıların önüne geçebilmek için her geçen gün güncellenen uygulamalar geliştirmelidir. Siber saldırılardan önce davranmakta yarar var. Mesela siber saldırıları esnasında güvenlik duvarının aşılmaya çalışılması esnasında uyarı veren ya da kendini kilitleyen sistemler gibi.*
*Siber suçlara yönelik uluslararası anlaşmalar güvenilir olmayacak.*

**K11 (E, 47):** *Devletin ve özel sektörün sistem ve network altyapıları konusunda daha bilinçli olmaları, bünyelerinde sistem ve network uzmanlarının yanı sıra CEH ve CISSP gibi yüksek güvenlik sertifikalarına sahip uzman bulundurmaları ya da bunu sağlayacak danışmanlık firmalarıyla çalışmaları siber saldırıların önlenmesi konusunda etkili olabilir.*
*Devletler arası anlaşmalar uygulamaya geçemediğinden gerekli şartları sağlayamaz.*

**K12 (E, 47):** *Siber suçluların iadesi vb. anlaşmalar yapılsa da genellikle siber suçlar işlemin yapıldığı ülke yasalarına tabi olmaktadır. Doğal olarak eylemi gerçekleştiren suçlular yaşadıkları ülkelerde yasalarda karşılığı varsa cezaya tabii tutulmaktadır. Bu durum karşısında saldırganlar kendi önlemlerini almaktadır. Örneğin Conficker isimli virüs ilk çıktığında klavyesi ya da sistem dili Ukrayna olan hiçbir cihaza ceza almamak için saldırmamış, ancak ülke dışındaki milyonlarca cihaza zarar vermiştir. Başka bir ülke tarafından suçlu tespit edilse dahi kendi ülkesinde herhangi bir suça karışmadığı için iadesi yapılmamaktadır. Maalesef bu durumda ülkeler arasında anlaşmalar da güvenli olmaktan çıkmıştır. Siber saldırıları ve savaşları önleyici tedbirleri en başta işletim sistemi üreticilerinin alması gerekmektedir. Ancak kapalı kaynak kodu sebebiyle özellikle Windows işletim sistemi özelinde hali hazırda tespit edilmemiş "zero-day" diye tabir edilen keşfedilmemiş açıklar mutlaka mevcuttur. Bu sorunlar çözülürse bu tarz saldırılar büyük ölçüde azaltacak.*

**K13 (E, 32):** *Dijital dünyada siber saldırıların ve savaşların önlenmesi, teknik, hukuki ve diplomatik tedbirler dahil olmak üzere çeşitli önlemleri içeren çok yönlü bir yaklaşımı gerektirmektedir. Alınabilecek önlemlerden bazıları şunlardır:*
*Kuruluşlar ve bireyler, güvenlik duvarları, antivirüs yazılımı ve şifreleme gibi güçlü güvenlik önlemleri uygulayarak kendilerini siber saldırılara karşı koruyabilirler.*
*Bireyleri ve kuruluşları siber saldırıların riskleri hakkında eğitmek, riskleri nasıl önleyecekleri veya nasıl müdahale edecekleri konusunda eğitmek etkili bir önlem olabilir.*
*Ülkeler, siber uzayda sorumlu davranış için uluslararası normlar ve standartlar geliştirmek üzere birlikte çalışabilir.*
*Hükümetler, siber suçlara karşı kolluk kuvvetlerinin çabalarını güçlendirmekle ve siber suçluların soruşturulması ve kovuşturulmasında uluslararası iş birliğini geliştirmek için birlikte çalışabilirler.*
*Hükümetler, siber saldırıları izleme ve bunlara karşı savunma dahil olmak üzere kendi siber savunma yeteneklerini geliştirmeye yatırım yapabilir.*
*Siber suçlara karşı ülkeler arasındaki anlaşmaların güvenilirliği, belirli anlaşmalara ve katılımcı ülkelerin taahhüt düzeyine bağlıdır. Bazı anlaşmalar diğerlerinden daha güçlü uygulama mekanizmalarına sahip olabilir ve ülkeler arasındaki güven ve iş birliği düzeyi de anlaşmaların etkinliğini etkileyebilir. Siber saldırıları ve siber savaşı etkili bir şekilde önlemek ve bunlara yanıt vermek için uluslararası iş birliğini ve iş birliğini geliştirmeye yönelik çalışmalara devam etmek önemlidir.*

**K14 (E, 29):** *Dijital dünyanın önemli sorunlarından biri olan Siber saldırıları ve savaşları, önlemek için alınabilecek bazı tedbirler şunlar olabilir:*
*Ülkeler, dijital güvenlik yasalarını geliştirerek, siber saldırılara ve savaşlara karşı önlemler alabilirler. Bu yasalar, siber suçların önlenmesine yardımcı olabilir ve ülkeler arasında iş birliğini teşvik edebilir.*
*Dijital dünyadaki siber saldırıların ve savaşların önlenmesi için, insanların daha iyi eğitilmesi ve farkındalığının artırılması gerekmektedir. Bu, insanların dijital dünyada nasıl güvende kalacakları hakkında daha fazla bilgi sahibi olmalarına yardımcı olabilir.*

*Dijital dünyada siber saldırıların ve savaşların önlenmesi için uluslararası iş birliği önemlidir. Ülkeler, birbirleriyle iş birliği yaparak, siber suçluların tespit edilmesi ve cezalandırılması için adımlar atabilirler.*
*Dijital dünyadaki siber saldırıları ve savaşları önlemek için daha iyi teknolojik altyapıya ihtiyaç vardır. Bu, ülkelerin güvenlik sistemlerini güçlendirmelerine ve siber saldırılara karşı daha iyi korunmalarına yardımcı olabilir.*
*Siber suçlara yönelik ülkeler arasında yapılan anlaşmaların güvenilirliği konusu ise karmaşık bir konudur. Bu tür anlaşmaların etkili olabilmesi için, ülkelerin bu anlaşmalara tamamen uymaları ve anlaşmaları ihlal edenlerin etkili bir şekilde cezalandırılması gerekir. Ancak, bazı ülkeler anlaşmalara uyacaklarını söyleyip, sözlerini tutmazlar. Bu nedenle, uluslararası iş birliği ve güvenlik protokolleri gibi daha kapsamlı tedbirlere ihtiyaç var.*

**K15 (E, 33):** *Siber saldırılar ve savaşlar mevcut fiziksel koşullardan ayrı düşünülmemelidir. Savunmanın her alanında nasıl bir yaklaşım sergileniyorsa, siber saldırılara karşı savunma konusunda da aynı nitelikte yaklaşım sergilenmektedir.*
*Anlaşmalar her ne kadar hazırlık seviyesinin artırılması ve ölçülmesi gibi alanlarda fayda sağlasa da her ülkenin yerel siber savunma kapasitesi bağımlılık olmaksızın geliştirilebilir ve idame edilebilir olmalıdır.*

**Tablo 4.** Katılımcıların egemen sınıfın dijital dünyada toplumsal ilişkileri manipüle etmek amacıyla dijital eşitsizlikleri görmezden gelmesine ve aktif katılımı çeşitli yöntemlerle engellemesine yönelik düşünceleri (**TEMA 3**).

| TEMA | KATEGORİ | ALT KATEGORİ | F |
|---|---|---|---|
| **3** | | Her türlü tedbirleri, önlemleri almak gerekiyor **(K2)** | **1** |
| | | Dijital platformlarda örgütlenen dijital topluluklar bu tarz manipülasyonların önüne geçmede en etkin yol olabilir **(K4)** | **1** |
| | | Maddi durumu iyi olmayan vatandaşlar için de internet olanaklarından faydalanma imkânı sağlanmalıdır. Elon Musk'ın Afrika'da, İran'da, Ukrayna'da uydu aracılığıyla internet erişimi sağlaması gibi çözümler sunulabilir **(K3) (K5)** | **2** |

| | | | |
|---|---|---|---|
| | Toplumsal ilişkilerin çeşitli yöntemlerle şekillendirilmesi sorununa yönelik çözüm önerileri | Devletler, dijital dünyada etkin olmalı ve sahayı egemen sınıflara bırakmamalıdır. Vatandaşlarını bu konuda bilgilendirmesi gerekmektedir **(K6), (K7)** | **2** |
| | | Dijital eşitsizliğe yönelik zararları minimize edebilmek için öncelikle toplumun farklı kesimleri arasındaki sosyoekonomik eşitsizliğin giderilmesi gerekmektedir **(K7), (K8), (K10)** | **3** |
| | | Toplumu düşünen kesimin bilinçlendirme amaçlı videolar yayınlaması ve videoları kitlelere ulaştırmakla başlanabilir **(K11)** | **1** |
| | | Bu tür sorunları azaltmak için daha fazla açık kaynak, kâr amacı gütmeyen sivil toplum kuruluşlarının ön planı çıkması gerekmektedir **(K12)** | **1** |
| | | Dijital kapsayıcılık **(K13), (K14)** | **2** |
| | | Gizliliğin koruması **(K13)** | **1** |
| | | Dijital okuryazarlık ve eleştirel düşünme **(K13), (K14), (K15)** | **3** |
| | | Çeşitliliği ve katılımı teşvik etmek **(K13), (K14)** | **2** |
| | | Halkın farkındalığı ve katılımı **(K5), (K13), (K14), (K15)** | **4** |
| | | Daha fazla şeffaflık ve hesap verebilirlik **(K14), (K15)** | **2** |
| | | Medya çeşitliliğini artırmak **(K14)** | **1** |
| | Aktif katılım teşvik edilmektedir | Kullanıcılar hakkında veri toplamak için aktif katılım genellikle teşvik edilmektedir **(K1)** | **1** |

Egemen sınıfın dijital dünyada toplumsal ilişkileri çeşitli yöntemlerle şekillendirmesi sorununa yönelik düşünceler iki kategoride değerlendirilmiştir. Birinci kategoride sorunun çözümüne yönelik hem ulusal hem de uluslararası

düzeyde çözüm olabilecek öneriler sunulmuş. İkinci kategoride ise aktif katılımın egemen sınıf tarafından genellikle teşvik edildiği belirtilmiştir.

Toplumsal ilişkilerin çeşitli yöntemlerle şekillendirilmesi sorununun çözümüne ilişkin 26 farklı öneri sunulmuştur. Tablo 4'te belirtildiği üzere dijital dünyada toplumsal ilişkilerin çeşitli yöntemlerle şekillendirilmesi sorununa yönelik 1 kişi her türlü tedbirlerin ve önlemlerin alınması gerektiğini, 1 kişi dijital platformlarda örgütlenen dijital toplulukların bu tarz manipülasyonların önüne geçmede en etkin yol olabileceğini, 2 kişi maddi durumu iyi olmayan vatandaşlar için de internet olanaklarından faydalanma imkânı sağlanması gerektiğini, 3 kişi dijital eşitsizliğe yönelik zararları minimize edebilmek için öncelikle toplumun farklı kesimleri arasındaki sosyoekonomik eşitsizliğin giderilmesi gerektiğini**,** 1 kişi toplumu düşünen kesimin bilinçlendirme amaçlı videolar yayınlaması ve paylaşılması gerektiğini**,** 1 kişi bu tür sorunları azaltmak için daha fazla açık kaynak, kâr amacı gütmeyen sivil toplum kuruluşlarının ön plana çıkması gerektiğini, 2 kişi dijital kapsayıcılık yaklaşımının uygulanması gerektiğini, 2 kişi çeşitliliğin ve katılımın teşvik edilmesi gerektiğini, 4 kişi farkındalığın ve katılımın sağlanması gerektiğini, 1 kişi medya çeşitliliğinin sağlanması gerektiğini, 3 kişi de dijital okuryazarlık ve eleştirel düşünmenin yaygınlaştırılması gerektiğini ifade etmektedir.

Devletlerin üstlenmesi gereken sorumluluklar açısından bulgular değerlendirildiğinde 2 kişi şeffaflık ve hesap verebilirliğin sağlanması gerektiğini, 1 kişi gizliliğin koruması gerektiğini, 2 kişi devletlerin dijital dünyada etkin olması ve sahayı egemen sınıflara bırakmamaları gerektiğini dile getirmiştir. Fakat gelişmekte olan ülkelerde zaten devletin egemen güçler tarafından yönetildiği bilinen bir gerçektir.

İkinci kategoride ise diğer önerilerle zıt anlama gelen bir yanıt verilmiştir. 1 katılımcı kullanıcılar hakkında veri toplamak amacıyla genelde aktif katılımın teşvik edildiğini vurgulamıştır. Bu yanıt kısmen doğrudur. Ama dünya genelinde, özellikle gelişmekte olan ülkelerde, kırsal alanlarda hale internet erişimi olmayan ve açlık sınırının altında yaşadıkları için son model teknolojik aletleri satın alamayan çok sayıda insanların olduğu da bilinen bir gerçektir.

Görüşme gerçekleştirilen katılımcıların egemen sınıfın dijital dünyada toplumsal ilişkileri çeşitli yöntemlerle şekillendirmesi sorununa yönelik verdikleri yanıtların bazılarına aşağıda yer verilmiştir;

**K1 (E, 46):** *Aktif katılım genellikle teşvik ediliyor, çünkü bu sayede kullanıcılar hakkında veri toplanıyor. Kişisel veri konusunda daha hassas olmak ve Big Tech dışındaki girişimlerin, özgür yazılım gibi yazılımların ve araçların kullanılması tavsiye olunur.*

**K2 (E, 68):** *Dijital çağın taleplerine göre yapılanmak zorundasınız, başka hiçbir şansımız yoktur. Yani teknolojik açıdan yapılanmadığımız takdirde, kendimizi geliştiremediğimiz takdirde manipülasyonların hedefi olmaktan kaçınmak mümkün değildir. Modern teknolojinin ön gördüğü her türlü tedbirleri, önlemleri almak gerçek kişide olsak görevimiz tüzel kişide olsak görevimizdir, devlet de olsak görevimizdir.*

**K3 (E,42):** *Sadece dijital dünyada veya sosyal platformlarda sahip oldukları güç değil, hukuk sistemi de egemen sınıflara hizmet eder. Sistem büyük hırsızı değil küçük hırsızı yakalar ya da sistem zayıf olanı ezmek üzere kurgulanmıştır diyebiliriz. Özetle sitemin yapısı gereği egemen sınıfın sahip olduğu imkânlarla hem dijital dünyada hem de gerçek dünyada toplumu şekillendirmeye çalışması kaçınılmazdır.*
*Dijital dünyada egemen sınıfın etkisini azaltmak için mümkün olduğu kadar çok sayıda ve çok ülke menşeli farklı platformlar yaratmak gerekiyor. Maddi durumu iyi olmayan vatandaşlar için de internet olanaklarından faydalanmaları için imkânlar sağlanmalıdır.*

**K4 (K,46):** *Dijital platformlarda örgütlenen dijital topluluklar bu tarz manipülasyonların önüne geçmede en etkin yol olabilir.*

**K5 (E,54):** *Olayın iki boyutu var. Birincisi maddi boyutudur, ekonomiye dayalıdır. Çözüm olarak Elon Musk'ın Afrika'da, İran'da, Ukrayna'da uydu aracılığıyla internet erişimi sağlaması gibi çözümler sunulabilir. Diğer boyut ise vatandaşların bilinçlendirilmesidir.*

**K6 (E, 35):** *Devletler, dijital dünyada etkin olmalı ve sahayı egemen sınıflara bırakmamalıdır. Devletlerin kendi siber güvenlik önlemlerini oluşturması, vatandaşlarını bu konuda bilgilendirmesi ve toplumları dış manipülasyonlara karşı koruması gerekiyor. Ulusal düzeyde ise dezavantajlı kesimi de bilinçlendirilmesi ve dijital olanaklardan faydalanmaları için gereken koşullar sağlanmalıdır.*

**K7 (E, 41):** *Bütüncül bir iyileştirme süreci başlatmak gerekiyor. Özellikle toplumun alım gücünü ve eğitim düzeyini yükseltmek etkili bir çözüm olabilir.*

**K8 (E, 32):** *Dijital eşitsizliğe yönelik zararları minimize edebilmek amacıyla öncelikle sosyoekonomik refahın yükseltilmesi, toplumun farklı kesimleri arasındaki eşitsizliğin giderilmesi gerekmektedir. Bu farklılığın giderilmesinin ardından bu kesimlere yönelik dijital medya okuryazarlığının artırılması ve farkındalıklarının üst seviyeye çıkartılması sorunun çözümü noktasında faydalı olabilmektedir.*

**K9 (E, 36):** *Siber uzay hem fiziksel hem de sanal ağı etkisi altına almıştır. Çok yönlü ilişkileri ve tüm ulusların evrensel olarak karşılıklı bağımlılığını yaratan siber uzay hem sömürücü ve kısıtlayıcı hem de özgürleştirici ve eşitlikçi bir yapı sunmuştur. İçinde bulunulan bu durum kaos haliyle tanımlanan yeni dünya düzenini simgelemektedir.*

**K10 (K, 27):** *Fırsat eşitliği sağlanabilir. Dijital eşitsizlikler de ekonomik nedenlere bağlıdır hal böyleyken dijital eşitlik için de genel eşitlik sağlanıp erişim hizmeti sunulabilir.*

**K11 (E, 47):** *Toplumu düşünen kesimin bilinçlendirme amaçlı videolar yayınlaması ve bunu o kitlelere ulaştırmasıyla başlanabilir. Eğer onların sahip olduğu platformlarda engellemeler olursa kendi platformlarını oluşturmaları ve buralardan yayın yapmaları gerekecektir. Ama bu hem eğitim olarak hem teknolojik olarak altyapı gerektirir. Ülkede ki ISP ve benzeri kuruluşlar yeterli altyapı güçlendirmek ve teknolojik imkânları erişilebilir hale getirmezlerse bu da mümkün olmayacaktır.*

**K12 (E, 47):** *Organizasyonlar kâr amacı güden kurumlar olduğu için genellikle sermaye yolunu takip eder. Dolayısıyla bir eşitsizlik çıkması kaçınılmazdır, bu tür sorunları azaltmak için daha fazla açık kaynak, kâr amacı gütmeye sivil toplum kuruluşlarının ön planı çıkması gerekmektedir.*

**K13 (E, 32):** *Dijital eşitsizliği azaltmak ve dijital dünyada toplumun manipülasyonunu önlemek, teknolojik, politika ve sosyal önlemleri içeren çok yönlü bir yaklaşımı gerektirir. İşte alınabilecek bazı önlemler:*

*Hükümetler ve özel sektör kuruluşları, özellikle dezavantajlı topluluklarda teknolojiye ve dijital okuryazarlık programlarına erişimi artırmak için çalışabilir. Bu, geniş bant erişimini artırmaya, teknolojiye uygun fiyatlı erişim sağlamaya ve insanların dijital becerilerini geliştirmelerine yardımcı olacak eğitim ve öğretim programları sunmaya yönelik girişimleri içerir.*

*Hükümetler ve özel sektör kuruluşları, kişisel verilerin kötüye kullanılmasını ve bireylerin hedefli reklam veya sahte haberler yoluyla manipüle edilmesini önlemek için daha güçlü gizlilik korumaları uygulayabilir. Bu, kişisel verileri koruyan ve veri toplama ve kullanımında şeffaflığı destekleyen yasa ve yönetmeliklerin çıkarılmasını içerir.*

*Eğitim programları, bireylerin dijital dünyada daha iyi gezinmesi ve yanlış bilgi ve manipülasyonu tespit etmesi için dijital okuryazarlık becerilerini ve eleştirel düşünme becerilerini geliştirmesine yardımcı olabilir.*

*Çeşitliliği ve katılımı teşvik etme çabaları, dijital eşitsizliğin azaltılmasına ve toplumun manipüle edilmesinin önlenmesine yardımcı olabilir. Bu, teknoloji endüstrisindeki çeşitliliği teşvik etme ve teknolojinin farklı bakış açıları göz önünde bulundurularak geliştirilmesini sağlama çabalarını içerir.*

*Halkın farkındalığını ve katılımını teşvik etmek, iktidardakilerin hesap vermesini sağlamaya ve toplumun manipüle edilmesini önlemeye yardımcı olabilir. Bu, teknoloji politikalarının ve düzenlemelerinin geliştirilmesinde halkın katılımını teşvik etmeye ve teknolojinin potansiyel riskleri ve faydaları konusunda halkın farkındalığını artırmaya yönelik girişimleri içerir.*

*Genel olarak, dijital eşitsizliği azaltmak ve dijital dünyada toplumun manipülasyonunu önlemek, hükümetler, özel sektör kuruluşları, eğitimciler ve sivil toplum grupları dahil olmak üzere bir dizi paydaşı içeren kapsamlı bir yaklaşım gerektirir.*

**K14 (E, 29):** *Egemen sınıfın dijital dünyada toplumsal ilişkileri şekillendirmek amacıyla dijital eşitsizliği artırması ve toplumun aktif katılımını engellemesi, dijital demokrasi için büyük bir problemdir. Çözüm için şunlar yapılabilir:*
*Dijital eşitsizliği azaltmak için, herkesin dijital dünyaya erişiminin sağlanması gerekmektedir. Bu, özellikle toplumun dezavantajlı kesimleri için önemlidir. İnternet erişiminin sağlanması, toplumsal katılımı artırabilir ve insanların dijital dünyada aktif olarak yer almalarına yardımcı olabilir.*
*Dijital dünyanın işleyişi hakkında daha fazla bilgi sahibi olmak, insanların dijital dünyada aktif katılımını artırabilir. Dijital okuryazarlık programları, insanların dijital dünyadaki hakları, özgürlükleri ve sorumlulukları hakkında bilgi sahibi olmalarına yardımcı olabilir.*
*Egemen sınıfın dijital dünyada toplumsal ilişkileri şekillendirmesi ve toplumu manipüle etmesi konusunda daha fazla şeffaflık sağlanması gerekmektedir. Bu, özellikle sosyal medya platformları için geçerlidir. Şeffaflık, insanların dijital dünyadaki bilgilere erişimlerini artırabilir ve toplumun daha aktif bir şekilde katılımını teşvik edebilir.*
*Medya çeşitliliği, egemen sınıfın toplumsal ilişkileri şekillendirmesi konusunda büyük rol oynamaktadır. Daha fazla medya çeşitliliği, insanların farklı görüşleri duymasına ve dijital dünyada daha geniş bir perspektife sahip olmalarına yardımcı olabilir.*

**K15 (E, 33):** *Dijital ilişkiler çoğunlukla dijital veri üzerinden gerçekleştiği için verinin doğrulanması büyük öneme sahiptir. Doğruluğu tespit edilemeyen verilere dayalı karar verme içgüdüsünün önüne geçmek, ilk etapta kullanıcıların bilinçlendirmesi ile en aza indirilebilir. Uzman görüşüne dayanan sistemler ya da hesaplamalı yöntemler ile yapılacak çalışmalar da destekleyici nitelikte kullanılabilir. Lakin problemin çözümünde şeffaflık, hesap verebilirlik, değişmezlik*

*ve merkezi olmama gibi kriterlerin de sağlanması gerekmektedir. Dünyada henüz bunun üzerine kesin ve kalıcı bir çözüm geliştirilememiştir.*

**Tablo 5.** Katılımcıların dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların çözümüne yönelik görüşleri (**TEMA 4**).

| TEMA | KATEGORİ | ALT KATEGORİ | F |
|---|---|---|---|
| **4** | Kapsamlı yasal düzenlemeler hazırlamak ve uygulamak | Açık veri gizliliği ile ilgili yasaları oluşturmak **(K13)** | **1** |
| | | Daha sıkı kanunlar çıkarmak, kontrol mekanizmalarını artırmak ve yaptırımlar uygulamak **(K3), (K6), (K7), (K8), (K9), (K10), (K11), (K12), (K13), (K14), (K15)** | **11** |
| | | Şeffaflığı artırmak **(K9), (K13), (K14)** | **3** |
| | | Uluslararası iş birliği ve anlaşmalar yapmak **(K2), (K3), (K10), (K13)** | **4** |
| | | Kurumsal ve devlet düzeyinde de tedbirler gerekiyor, bu konuda AB'nin düzenlemeleri başarılıdır **(K1)** | **1** |
| | Diğer öneriler | Vatandaşların bilinçlendirilmesi **(K4), (K6), (K12), (K13)** | **4** |
| | | Veri etiğini teşvik etmek **(K1), (K11), (K13)** | **3** |
| | | İnternet üzerinden alışverişlere yönelik düzenlemelerin yeniden gözden geçirilmesi, şirketlere bazı kısıtlamaların getirilmesi **(K6)** | **1** |
| | | Kişisel veri ihlallerinin bildirilmesi **(K14)** | **1** |
| | | Yüzde 100 güvenlikten bahsedilemez. Sadece bilinçli olursak rastgele erişilebilirlikten verilerimizi koruyabiliriz **(K6)** | **1** |
| | | Genel olarak, dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve kullanılması ile ilgili sorunların ele alınması, | **2** |

| | | | |
|---|---|---|---|
| | | yasal, teknolojik ve etik önlemlerin bir kombinasyonunu gerektirmektedir **(K13), (K14)** | |

Katılımcıların dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların çözümüne yönelik verdiği yanıtlar iki kategoride değerlendirilmiştir. Birinci kategoride katılımcıların büyük bir kısmı sorunların çözümü konusunda kapsamlı yasal düzenlemelerin hazırlanması, kontrol mekanizmalarının artırılması ve yaptırımların uygulanması gerektiğini belirtmiştir. İkinci kategoride ise kullanıcıların bilinçlendirilmesi ve kişisel verilerin korunmasına yönelik önleyici tedbirlerin alınması gerektiği ifade edilmiştir.

Birinci kategori kapsamında 1 kişi açık veri gizliliği ile ilgili yasaların oluşturulmasını, 11 kişi daha sıkı kanunların çıkarılmasını, kontrol mekanizmalarının artırılmasını ve yaptırımların uygulanasını, 3 kişi şeffaflığın artırılmasını, 4 kişi uluslararası iş birliği ve anlaşmaların yapılmasını, 1 kişi kurumsal ve devlet düzeyinde de tedbirlerin alınması gerektiğini önermiştir.

İkinci kategoride ise 4 kişi vatandaşların bilinçlendirilmesi gerektiğini, 3 kişi veri etiğinin teşvik edilmesi gerektiğini, 1 kişi internet üzerinden alışverişlere yönelik düzenlemelerin yeniden gözden geçirilmesi ve şirketlere bazı kısıtlamaların getirilmesi gerektiğini, 1 kişi kişisel veri ihlallerinin kullanıcılara bildirilmesi gerektiğini, 2 kişi genel olarak, dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve kullanılması ile ilgili sorunların ele alınması gerektiğini, yasal, teknolojik ve etik önlemlerin bir kombinasyonuyla sorunların çözülmesi gerektiğini belirtmiştir. 1 kişi ise yüzde 100 veri güvenlinin mümkün olmayacağını, sadece bilinçli olanların verilerini rastgele erişilebilirlikten koruyabileceğini dile getirmiştir.

Katılımcıların sorunun çözümüne yönelik verdikleri yanıtlardan bazılarına aşağıda yer verilmiştir;

**K1 (E, 46):** "*Kişisel veri hassasiyetinin artması gerek. Ama kurumsal ve devlet düzeyinde de tedbirler gerekiyor ki bu konuda AB'nin düzenlemeleri daha başarılı".*

**K2 (E, 68):** *Maalesef dijital dünyada bu verilerin toplanması saklanması ve korunması konusunda uluslararası düzeyde henüz net bir konsensüs sağlanmadı, yani Uluslararası Hukuk bu konuda Henüz Arzu ettiğimiz düzeyde değil. Özellikle gelişmekte olan ülkeler henüz kendi sistemlerini üretemediler, mecburen ABD merkezli platformları ve teknolojileri kullanıyorlar.*

**K3 (E, 42):** *Uluslararası ve ulusal sorunları çözmenin tek yöntemi hukuktur. Medeniyetinin temelini sağlayan şey anlaşmadır, hukuktur. Herhangi bir ülkede hukuk sisteminin işleyişi ile paralel öngörülebilirlik de çok önemlidir. Gerçek dünyada olduğu gibi dijital dünyada da kişi haklarının korunması için devletlerin düzenleme yapması ve yaptırımları uygulaması gerekiyor.*

**K4 (K, 46):** *Kaliteli donanım, güçlü altyapı, veri güvenliği ile ilgili güvenilir yazılım ve yazılım uzmanlarına ihtiyaç vardır. Buna paralel olarak kişisel verilerini en azından rastgele erişimden koruyabilecek düzeyde vatandaşları bilinçlendirmek gerekiyor.*

**K5 (E, 54):** *Bilişim sistemlerinde veri güvenliği ile ilgili yüzde 100 güvenlikten bahsedilemez. Sadece bilinçli olursak verilerimizi rastgele erişilebilirlikten koruyabiliriz. Yazılım sistemlerine ve ortamlara hâkim olan birisi kişisel verilere farklı yöntemlerle ulaşabilir.*

*Sosyal medya platformlarını hazırlayan uluslararası şirketler için kullanıcıların kişisel verileri ve davranış alışkanlıkları başkalarına ticari amaçla satılabilecek verilerdir. Kullanıcılar uygulamaları kullanmak için para ödemiyorlar, o yüzden onların verileri para kazanmak amacıyla kullanılmaktadır. Kullanıcılar uygulamaları kullanmak için para ödeseler dahi yine de kişisel verileri toplayan büyük teknoloji şirketleri, kurum ve kuruluşlar tarafından kâr amacıyla kullanılmayacağına inanmıyorum.*

*Ben bilişim işleriyle uğraşan ve işin yazılım/kodlama kısmını da bilen biri olarak verilerimizin güvende olabileceğine inanmıyorum. Kodlama sisteminde her zaman açık olabileceğini kabul etmek gerekiyor. Bu açıkları kapatmanın önemli yolu ileri düzeyde kodlama ve sistem bilgisine sahip olmaktır.*

*Sosyal medya platformlarını geliştirip hizmete sunanlar işlerine geldiği gibi sözleşmeler düzenlenmiş, eğer geliştirdiğim platformu kullanmak istiyorsan koşullarımı da kabul edeceksin diyorlar. Eğer kabul etmek istemiyorsan o zaman kullanma, kullanmak zorunda değilsin. O yüzden de insanlar o sözleşmeleri okumadan kabul ederler. Aslında zora dayalı değil insanlar kendi rızasıyla o sözleşmeleri kabul ediyorlar.*

**K6 (E, 35):** *Kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılması ile ilgili sorunların azaltılması için kanunların sıklaştırılması ve yaptırımların daha da caydırıcı olması büyük önem arz etmektedir. Diğer olası bir çözüm ise vatandaşların bu konuda bilinçlendirilmesi için kamu spotlarının yaygınlaştırılması olabilir. Ayrıca internet üzerinden alışverişlere yönelik düzenlemelerin yeniden gözden geçirilmesi, şirketlere bazı kısıtlamaların getirilmesi ve kullanıcıların bilgilendirilmesi gerekmektedir.*

**K7 (E, 41):** "*KVKK ve benzeri yasaların titizlikle ve tavizsiz uygulanması, dönemsel gerekliliklere göre yeni yasa, mevzuatların ivedilikle çıkarılması gerekir. Zira dijital platformlar çok hızlı bir gelişme gösteriyor ve gereklikler her gün hatta her an yenileniyor".*

**K8 (E, 32):** *İlk önce kişisel verilerin korunmasına yönelik yasal düzenlemelerin kapsamı genişletilmelidir. Aynı zamanda kontrol mekanizmalarının artırılması ve yaptırımların keskin bir şekilde uygulanması gerekmektedir.*

**K9 (E, 36):** *Teknolojik gücü elinde tutan her türlü yaşamsal kolaylığı elinde tutarken diğerleri toplumsal huzursuzlukla yaşamak zorunda kalmaktadır. Devletler kendi içlerinde siber ağların mülkiyetini elinde bulundururken tüm birey ve kurumların bu ağa erişim ve kullanımında eşitliğini sağlayamamaktadır. Siber uzayın mülkiyetinin olmamasından kaynaklı devletler arasında tamamen bir eşitsizlik bulunmaktadır. Yani gücü elinde bulunduran diğerleri üzerindeki tahakkümünü artırmaktadır.*

*Bu sebeple kişisel verilerin ikincil işlenmesini düzenleme, yasal bir bildirimin sunulmasını sağlama ve tüm araştırma alanları için açık bir onay mekanizması sağlama gibi noktalarda uygulamalar geliştirilmelidir. Ayrıca yeni nesil*

*teknolojilerin getirdiği siber güvenlik gereksinimlerine cevap vermesi maksadıyla Kişisel Verilerin Korunması Kanunu sürekli güncellenmelidir.*

**K10 (K, 27):** *Kişisel verilere ilişkin sorunların etkili bir şekilde çözümü pek kolay olmayacaktır. Ama en azından kişisel verilerin korunmasına yönelik daha sıkı kanunlar çıkarılabilir, daha sıkı yaptırımlar uygulanabilir ve özellikle de uluslararası anlaşmalar yapılabilir.*

**K11 (E, 47):** *Bununla ilgili öncelikle kanunlar uygulanmalıdır. Güvenilir güvenlik ve şifreleme program ve araçları kullanılabilir. Ama önemli olan insanların bu konuya saygı göstermeleridir. Mutlaka kanunları ihlal etmeye ve kendini gizlemeye çalışan kötü amaçlı hackerler ortaya çıkacaktır.*

**K12 (E, 47):** *İlgili yasaların yürürlükte olması bu sorunların çözülmesi ya da azaltılmasına yardımcı olacaktır ancak tek başına yaptırımlar maalesef yeterli olmamaktadır. Sadece şikâyet üzerine açılan davalar sonucu cezai yaptırım uygulanmakta, ancak proaktif olarak özellikle büyük şirketlerin daha sık denetlenmesi gerekmektedir. Cezalar olay gerçekleştikten sonra değil, gerçekleşmeden kesilmeli ve çok kullanıcılı kişisel veri barındıran siteler çok sıkı kontrol edilmelidir. Yakın zamanda meydana gelen Yemeksepeti sitesinden hesap bilgilerinin çalınması örneğinde olduğu gibi basit SQL Injection atağına karşı koyamaması ve maalesef büyük bir dizayn hatası yaparak veri tabanında kayıtlarında hash+salt yerine sadece hash koduyla tuttukları için çok sayıda kullanıcının giriş bilgileri buna bağlı olarak diğer sitelerdeki verileri de saldırıya maruz kalmıştır. Bu tür durumlarda sadece idari para cezası yerine buradan elde edilen verilerle yaşanılacak mağduriyetler için de ceza yaptırımı gerekmekte bunun doğal sonucu olarak da bu tür büyük şirketler gelişen teknolojiye ayak uyduran ve saldırılara cevap verebilecek nitelikli kadro oluşumuna zorlanmış olacaktır.*

**K13 (E, 32):** *Kişisel verilerin dijital dünyada toplanması, saklanması, korunması ve kullanılmasına ilişkin sorunların çözümü kapsamlı bir yaklaşım gerektirmektedir. İşte alınabilecek bazı önlemler:*

*Hükümetler, neyin kişisel veri oluşturduğunu, nasıl toplanıp kullanılması gerektiğini ve bu yasaları ihlal etmenin cezalarını tanımlayan açık veri gizliliği yasaları ve düzenlemeleri oluşturabilir.*

*Kişisel verileri toplayan ve depolayan şirketler ve kuruluşlar, şifreleme, erişim kontrolleri ve izleme gibi güçlü veri koruma önlemleri uygulamalıdır. Ayrıca, kişisel verilerin yalnızca meşru amaçlar için toplanmasını ve kullanılmasını sağlamalıdırlar.*

*Şirketler ve kuruluşlar, veri toplama ve kullanma uygulamaları konusunda şeffaf olmalıdır. Bu, net gizlilik politikaları sağlamayı ve verilerini toplamadan önce bireylerden izin almayı içerir.*

*Bireyler, kişisel verileri üzerinde daha fazla kontrole sahip olmalıdır. Bu, verilerine erişme, istedikleri zaman verileri silme yetkisinin ve yeteneğinin yanı sıra verilerini kimin topladığını ve nasıl kullanılacağını bilme hakkını içerir.*

*Veri etiği dijital dünyada teşvik edilmelidir. Şirketler ve kuruluşlar, kişisel verileri kullanımlarından sorumlu tutulmalı ve verileri bir bütün olarak toplumun yararına olacak şekilde kullanmaya çalışmalıdır.*

*Sınır ötesi veri gizliliği konularını ele almak için uluslararası iş birliği şarttır. Hükümetler, ortak veri gizliliği standartları oluşturmak ve veri gizliliği ihlallerinin soruşturulması ve kovuşturulmasında iş birliğini geliştirmek için birlikte çalışabilir.*

*Genel olarak, dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve kullanılması ile ilgili sorunların ele alınması, yasal, teknolojik ve etik önlemlerin bir kombinasyonunu gerektirmektedir. Bu adımları atarak daha güvenli ve etik bir dijital dünya yaratmak için çalışabiliriz.*

**K14 (E, 29):** *Dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılması, kişisel gizlilik ve veri güvenliği konularında ciddi sorunlar oluşturmaktadır. Daha iyi yasalar, prensipler, prosedürler bu sorunun üstesinden gelmek için kullanılabilir.*

*Veri koruma yasalarının daha sıkı hale getirilmesi, kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılması konusunda daha sıkı kuralların uygulanmasını sağlayabilir.*
*Şeffaflık ilkesi, kişisel verilerin toplanması, saklanması ve kullanılması konusunda şeffaf bir politika benimseyerek, kullanıcıların ne tür verilerin toplandığını, neden toplandığını ve ne amaçla kullanıldığını açık bir şekilde belirtmelidir.*
*Kişisel veri ihlallerinin bildirilmesi, kullanıcıların verilerinin kötüye kullanıldığı durumlarda, kullanıcıların etkili bir şekilde korunmasını sağlayabilir.*
*Veri ihlallerine karşı cezalar, şirketlerin kişisel verileri kötüye kullanmaktan kaçınmalarını sağlayabilir. Bu, kullanıcıların verilerinin güvenliği konusunda daha fazla güven duymalarını sağlayabilir.*

**K15 (E, 33):** *Avrupa'da Genel Veri Koruma Yönetmeliği anlamına gelen General Data Protection Regulation (GDPR) başta olmak üzere tüm dünyada bu konuda yürütülmekte olan çeşitli çalışmalar vardır. Türkiye'de de Kişisel Verileri Koruma Kanunu ve Kişisel Verileri Koruma Kurumu bu husus özelinde çalışmalar yürütmektedir. Bu çalışmalar birçok görüş ve sektör göz önüne alınarak hazırlandığından bunların takip edilmesi uygun olur.*

**Tablo 6.** Katılımcıların gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketlerin veya sosyal medya platformların serbest piyasada ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet edebilmesini zorlaştıran faktörlere ilişkin görüşleri (**TEMA 5**).

| TEMA | KATEGORİ | ALT KATEGORİ | F |
|---|---|---|---|
| **5** | | - Kaynakların eksikliği **(K3), (K4), (K5), (K6) (K7), (K9), (K10), (K12), (K13)** | **9** |
| | | - Teknolojik alt yapının yetersizliği **(K4), (K7), (K10), (K12), (K13), (K14)** | **6** |
| | | - Fikri mülkiyet hakları ile ilgili sorunlar **(K13)** | **1** |

| | | | |
|---|---|---|---|
| | ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet etmeyi zorlaştıran faktörler | - İç mevzuatlar ve düzenlemeler **(K1),** (**K2), (K5), (K6), (K13)**<br>- Finansal güç **(K4), (K5), (K11), (K12), (K13), (K14)**<br>- İnovasyon eksikliği **(K1),** (**K2), (K3), (K14)**<br>- Marka bilinirliği **(K3), (K5), (K8), (K9) (K14)**<br>- Beyin göçü **(K7), (K10), (K13), (K14), (K15)**<br>- Coğrafi dağılım **(K15)**<br>- Kümülatif birikim **(K3), (K9), (K15)**<br>- Satın alma modeli **(K5), (K7), (K12)**<br>- Devlet desteğinin olmaması **(K3), (K4), (K12),** (**K13)** | **5**<br>**6**<br>**4**<br>**5**<br>**5**<br>**1**<br>**3**<br>**3**<br>**4** |
| | Aslında serbest piyasa koşulları mevcut değil | - ABD rakiplerini engellemektedir **(K4), (K7), (K8), (K9), (K11)** | **5** |
| | Gelişmekte olan ülkelerde şeffaflık ve güvenlik sorunu var | - Güvenlik endişesi her zaman vardır, her konuda yüzde 100 şeffaf olmak gerekiyor **(K1), (K3)**<br>- Hiçbiri aslında güvenli değil, hepsi dinlenebilir ve kopyalanabilir. Veriler veya bilgiler kimin elindeyse istediği gibi kullanacaklar (**K2)**<br>Gelişmekte olan ülkeler inovasyondan çok güvenliği öne çıkarıp yasaklamayı ya da kısıtlamayı tercih ediyorlar (**K1), (K13)**<br>Gelişmekte olan ülkelerin ABD'de sağlanan ekonomik, teknolojik imkânları ve itibarı, belli seviyenin üzerindeki personele sağlaması güçtür (**K14),** (**K15)**<br>Gelişmekte olan ülkeler, düşük ücretler, | **2**<br>**1**<br>**2**<br>**2**<br>**1** |

| | | | |
|---|---|---|---|
| | | sınırlı kariyer gelişimi fırsatları ve siyasi istikrarsızlık gibi faktörler nedeniyle üst düzey yetenekleri çekmek ve elde tutmakta zorlanabilirler **(K13)** | |
| | Güçlü teknolojileri sadece güçlü ülkeler değil zayıf ülkeler de geliştirebilir | - Bütün mesele "Know-how" üretebilmektir. Bu konuda ülkelerin milli politikaları, milli teknoloji politikaları, teknoloji yaratma ve üretme politikaları önemlidir. Örneğin İsrail'in yüksek milli geliri yok ama yüksek teknolojisi var. Türkiye İHA ve SİHA'ları üretiyor. (**K2), (K3)** | **2** |

Tablo 6'da gelişmekte olan ülkelerin ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet etmesini zorlaştıran faktörler dört kategoride değerlendirilmiştir.

Birinci kategoride görünüşte rekabet yasalarına aykırı olmayan nedenler yer almaktadır. Katılımcıların görüşüne göre gelişmekte olan ülkelerin başarısız olması kaynakların eksikliği, teknolojik alt yapının yetersizliği, fikri mülkiyet haklarıyla ilgili engeller, iç mevzuatların ve düzenlemelerden kaynaklanan sorunlar, finansal güç eksikliği, inovasyon eksikliği, marka bilinirliği, beyin göçü, coğrafi dağılım, kümülatif birikim, satın alma modeli ve devlet desteğinin olmaması gibi nedenlerden kaynaklanmaktadır.

İkinci kategoride, katılımcılar (5 kişi) aslında serbest piyasa koşullarının mevcut olmadığını, gelişmiş ülkelerin kendi şirketlerinin ve firmalarının çıkarlarını korumak için uluslararası boyutta piyasaları etkilediğini dile getirmiştir.

Üçüncü kategoride gelişmekte olan ülkelerde itibar, şeffaflık ve güvenlik sorununun olduğu vurgulanmıştır. Bu kategoride güvenlik sorunu iki alt kategoride değerlendirilmiştir. Birinci alt kategoride gelişmekte olan ülkelerdeki dijital teknoloji şirketlerin kişisel verilerin korunması açısından güvenilmez olduğu, ikinci alt kategoride ise gelişmekte olan ülkelerdeki siyasi istikrarsızlık ve hukuk sisteminin işleyişiyle ilgili sorunlara dikkat çekilmiştir.

Dördüncü kategoride bazı katılımcılar (2 kişi) güçlü teknolojilerin ve sosyal medya platformların sadece finansal olarak güçlü olan ülkeler tarafından değil, finansal olarak zayıf olan ülkeler tarafından da üretilebildiği ifade edilmiştir.

Katılımcıların, gelişmekte olan ülkelerin ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet etmesini zorlaştıran sorunlara yönelik verdiği yanıtlardan bazıları aşağıda sıralanmıştır;

**K1 (E, 46):** *Çünkü gelişmekte olan ülkeler inovasyondan çok güvenliği öne çıkarıp yasaklamayı ya da kısıtlamayı tercih ediyorlar. Bu şartlarda global bir şirketin çıkması epey zor oluyor.*

**K2 (E, 68):** *Örneğin Türkiye İHA ve SİHA'ları daha önce ABD'den satın alıyordu. Ama şimdi Türkiye'de üretiliyor, hatta onlardan daha iyi üretiyorlar. Demek ki istendiği zaman iyi teknolojiler üretmek mümkündür. İşte bütün mesele "Know-how" üretebilmektir. Eğer "Know-how" üretirsiniz Microsoft'tan daha iyi bir teknoloji üretme şansınız da var. Yani bilgiyi üreteceksiniz ve onu uygulama alanına sokacaksınız. Güçlü teknolojiyi sadece güçlü ülkeler değil zayıf ülkeler de geliştirebilir. Bu yetişmiş insan gücüne ve eğitim sitemine bağlıdır. Örneğin İsrail'in yüksek milli geliri yok ama yüksek teknolojisi var.*

*-- Ama İsrail'in arkasında ABD'nin desteği var*

*Her şey destekle olmaz. Örneğin İsrail tarım sektöründe tohum üretiyor, dünyanın pek çok ülkesine tohum satıyor. Bunu ABD'nin desteğiyle yapmıyor, kendi teknolojisiyle yapıyor. Dolayısıyla bu konuda ülkelerin milli politikaları, milli teknoloji politikaları, teknoloji yaratma ve üretme politikaları önemlidir. Yeter ki devletler bu konuda gereken adımları atsın.*

*Güven konusuna gelince tüm bilgilerin hizmet aldığımız operatörler ve büyük teknoloji şirketleri tarafından alınabileceği, kopyalanabileceği endişesi var. Bence de doğru. Biz şimdi WhatsApp'ı, Facebook'u ve Instagram'ı kullanıyoruz. Bunlar bizim veri tabanlarımızın hepsine ulaşabiliyorlar. Hiçbiri aslında güvenli değil, hepsi dinlenebilir ve kopyalanabilir. Bu da bir gerçektir. Maalesef bunları önlememiz mümkün değil, veriler veya bilgiler kimin elindeyse istediği gibi*

*kullanacak. Meselen WhatsApp'tan bütün yazışmalarımızı hepsini kopyalayıp istedikleri gibi değerlendirebilirler.*

*-- Ama insanların onları daha güvenli buluyorlar diye düşünüyorum, gelişmekte olan ülkelerde daha çok ABD merkezli platformları kullanıyorlar.*

*Eğer siz kendi milli sisteminizi kurarsanız, kendi şirketleriniz bu konuda bir yaratıcılık yaparsa durum değişebilir. Ama şu bir gerçek ki bunların hepsi dinlenebilen kopyalanabilen veri tabanlarına müdahale edilebilen sitemlerdir.*

*-- Kimin elinde olursa olsun kullanır mı sizce?*

*-- Kesinlikle*

**K3 (E, 42):** *Çünkü şu an ABD en fazla bilgiyi öğreten ülke durumundadır. ABD merkezli şirketler artık belli bir yol almışlar. Bu süreçte teşvik ve tanıtım da önemlidir. Özellikle serbest piyasa ekonomisinde başarılı bir ürün üretiliyorsa, bence başarılı olma şansı her zaman vardır. Tabii ki güvenlik endişesi de her zaman vardır. Çözüm olarak gizli iş yapmamak, her konuda yüzde 100 şeffaf olmak gerekiyor.*

**K4 (K, 46):** *Gelişmiş ülkeler kendi şirketlerinin ve firmalarının çıkarlarını korumak için uluslararası boyutta piyasaları etkiliyorlar. Gelişmekte olan ülkelerin böyle bir gücü ve altyapısı yoktur.*

**K5 (E, 54):** *Teknolojinin kullanımı konusunda gelişmiş ülkelerle gelişmekte olan ülkeler arasındaki uçurumun nasıl aşılabileceği ile ilgili dünya çapında toplantılar, sempozyumlar yapılıyor, ama durum değişmiyor.*

*Gelişmekte olan ülkelerin de bilişim sistemleri ile ilgili deneyimli kişilerden destek alınması gerekiyor, bu durumda otomatik olarak en başa geri dönmüş oluyoruz. Bir de şöyle bir durum var; yeni teknoloji üretmek konusunda ne kadar geri planda isen ya da arkadan takip ediyorsan bu teknolojileri kullanma konusunda da o kadar geridesin demektir.*

*Diğer taraftan gelişmekte olan ülkeler iyi teknolojiler veya platformlar ürettikleri zaman da gelişmiş ülkelerden yatırımcılar değerinden de fazla para ödeyerek satın alıyorlar. Örneğin Yemeksepeti Almanya merkezli global bir şirket tarafından satın*

*alındı. Diğer bir handikap ise gelişmekte olan ülkelerde üretilen platformlar sermaye birikiminin yetersiz olması nedeniyle bireysel kalır.*
*Gelişmekte olan ülkeler tarafından hazırlanan sosyal medya platformlarının güvenilir olmaması fikri bana mantıklı gelmiyor. ABD merkezli şirketlerin daha güvenilir olduğunu düşünmüyorum. Örneğin kullanıcılar TikTok gibi Çin merkezli platformlara pek güvenmezler. Peki Facebook kullanıcılarının kişisel verilerinin korunması ile ilgili skandallar yaşanmadı mı?*
*O zaman bu güven dediğimiz şey hizmetin veya ürünün kullanıcılara nasıl sunulduğu ile ilgilidir. Bu durumun biraz ülkeler arası politikalar ve ulusal politikalarla ilgili olduğunu ve sadece bir halkla ilişkiler etkinliği olduğunu düşünüyorum.*

**K6 (E, 35):** *Uluslararası şirketlerin ekonomik, hukuki ve siyasi güçleri bazen ulusal devletlerin gücünü aşabilirler. Dolayısıyla iç mevzuatlar, uluslararası mevzuatlarla yarışamayacak hale gelirler. Liberal ve küresel dünya düzeninde Keynesyen ve devlet müdahaleci politikaların yeterince hükmü olmayabilir, bilhassa teknoloji alanında bu yetersizlik daha fazla hissedilir. Sosyal medyanın devletler tarafından kısıtlanamaz, çünkü toplumlar Proxy siteler üzerinden sosyal medya platformlarında bilgi paylaşımı yapabilirler.*

**K7 (E, 41):** *ABD merkezli şirketler, hem gelecek vaat eden teknoloji tabanlı şirketleri hem de alanda çalışan parlak beyinleri hızla ve başarıyla satın alıyorlar. Satın alamadıkları nadir durumlarda ise hem parasal hem de veri kaynaklarını keserek bu şirketlerin kendi kendine ölmesine neden oluyorlar.*

**K8 (E, 32):** *Çünkü Herman Schiller'in belirttiği gibi ABD emperyalizmi ürettiği sinema, dizi gibi içeriklerle sadece gösterim mekanizmasına izin vermemektedir. Bu bağlamda zihinlerin üretimini de gerçekleştirdiği için alternatif düşüncelere yer vermemektedir. Bu durumda ABD merkezli kuruluşlarla küresel ölçekte hareket etseler de küre-yerel ilişkisi bağlamında zihinsel üretimlerini serbest piyasa esasları içerisindeki rakiplerine imkân vermemektedirler.*

**K9 (E, 36):** *ABD bireysel internetin kontrolünden sanayi casusluğuna, siber savaştan tüm iletişim ağlarının kontrolüne kadar siber ortamın hâkimiyetini kazanabilmek için siber saldırılara karşı savunma ve saldırı timleri oluşturarak siber ordu birimlerini devreye sokmuştur. Özellikle liberal değerlerin hâkim olduğu uluslararası sistem içerisinde yarattığı küresel şirketler bu düzende etkin olmasını desteklemektedir.*

*Aynı zamanda ABD hükümeti taşeron hackerler kullanarak gerçekleştirdikleri saldırılarda kimliklerini gizlemektedir. Böylece küresel ölçekte ABD'ye karşı rekabete girecek ülkeler karşılarında direk bir muhatap bulamamaktadır.*

*ABD'nin siber kontrollü sistemlere bağımlılığı, potansiyel rakiplerinin hiçbirinin onun kadar özel şirketler tarafından sahip olunan ve işletilen ulusal sistemlere sahip olmaması, başka hiçbir sanayileşmiş ve teknolojik olarak gelişmiş ulusun onun kadar lobicilik faaliyetleriyle kolayca yönlendirilmemesinden kaynaklanmaktadır.*

**K10 (K, 27):** *Bu durumun da en büyük sebebi sermaye ve alt yapı yetersizliğidir. Büyük teknoloji şirketlerinin sağlam alt yapısı bulunması nedeniyle hızla büyümektedirler. Gelişmekte olan ülkelerin alt yapı oluşturması da bir hayli zaman alabilmektedir ve diğer bir unsur ise alt yapıyı sağlayacak teknik eleman yetersizliğidir.*

**K11 (E, 47):** *Küreselci ya da onları kullanan birtakım çevrelerin, onların amaçlarını engelleyecek ya da durduracak şirketlere, markalara izin verme olasılığı yoktur. Bütün dünya pazarını ekonomik ölçekte de ellerinde bulundurdukları için, bunları kaybetmeyi istemezler. Sadece piyasanın adı rekabet piyasasıdır.*

**K12 (E, 47):** *Bunun arkasındaki en temel neden sermaye, bu tür şirketler altyapı konusunda neredeyse sınırsız kaynak aktarmaktadır. Böyle bir durumda gelişmekte olan ülkeler hem internet altyapısı hem fiziki altyapı yetersizlikleri sebebiyle hiçbir zaman bu firmalarla rekabet edemezler veya edemeyecekler. Zaten bu tür şirketlerin en önemli bir başka özelliği ise kendilerinin çıkartmadığı ancak popüler olabilecek yeni çıkan uygulamaları daha en başında ya melek yatırımcı modeliyle ya da direkt ortak olarak kendi bünyelerine katmalarıdır. Yakın zamanda Türkiye tarihinin en*

*büyük satın alması PEAK games üzerinden olmuştur. Zynga isimli şirket 1,8 milyar dolar vererek yerli oyun üretici firmayı bünyesine katmıştır. Belki de ileride dünya lideri olabilecek bir şirketin önü oldukça hatırı sayılır bir rakam karşılığında piyasadaki hâkim güce geçmiştir. Devlet desteği olmadan maalesef bu tür kurumların, içerik üreticilerinin piyasada tutunma şansı pek yoktur.*

**K13 (E, 32):** *Teknoloji tabanlı şirketlerin veya gelişmekte olan ülkeler tarafından geliştirilen sosyal medya platformlarının, rekabet ilkelerine dayalı serbest piyasada ABD merkezli büyük teknoloji şirketleriyle küresel olarak rekabet etmesini zorlaştıran çeşitli faktörler vardır.*

*ABD merkezli büyük teknoloji şirketleri, araştırma ve geliştirme, pazarlama ve satın almalara yatırım yapmak için kullanabilecekleri risk sermayesi ve halka arz finansmanı dahil olmak üzere önemli finansal kaynaklara erişebilir. Bu onlara, finansmana sınırlı erişimi olabilecek gelişmekte olan ülkelerdeki şirketlere göre önemli bir avantaj sağlıyor.*

*ABD, yüksek hızlı internet ve güvenilir elektrik dahil olmak üzere teknoloji tabanlı şirketleri ve sosyal medya platformlarını desteklemek için iyi geliştirilmiş bir altyapıya sahiptir. Gelişmekte olan ülkeler, teknoloji tabanlı şirketlerinin küresel olarak rekabet etmesini zorlaştırabilecek bu tür bir altyapıya sahip olmayabilir.*

*ABD merkezli büyük teknoloji şirketleri, yeniliklerini korumak ve rakiplerinin pazara girmesini engellemek için kullanabilecekleri önemli fikri mülkiyet portföylerine sahiptir. Bu da gelişmekte olan ülkelerdeki şirketlerin aynı pazarda rekabet etmesini zorlaştırabilir.*

*ABD merkezli teknoloji şirketleri, bilim insanları, mühendisler ve iş profesyonelleri dahil olmak üzere dünyanın dört bir yanından en iyi yetenekleri çekebilir. Gelişmekte olan ülkeler, düşük ücretler, sınırlı kariyer gelişimi fırsatları ve siyasi istikrarsızlık gibi faktörler nedeniyle üst düzey yetenekleri çekmek ve elde tutmakta zorlanabilirler.*

*ABD merkezli teknoloji şirketleri, yenilik ve girişimciliğe nispeten uygun olan bir düzenleyici ortamda faaliyet göstermektedir. Gelişmekte olan ülkeler, teknoloji tabanlı şirketlerin küresel pazarda faaliyet göstermesini ve rekabet etmesini zorlaştırabilecek daha kısıtlayıcı düzenlemelere sahiptir.*

*Özetlemek gerekirse, teknoloji tabanlı şirketlerin veya gelişmekte olan ülkeler tarafından geliştirilen sosyal medya platformlarının, rekabet ilkelerine dayalı serbest piyasada ABD merkezli büyük teknoloji şirketleriyle rekabet ederken karşılaştıkları çeşitli zorluklar vardır. Ancak, kaynakların, altyapının, yeteneğin ve düzenleyici desteğin doğru bileşimi ile gelişmekte olan ülkelerdeki şirketlerin küresel pazarda rekabet etmesi ve başarılı olması mümkündür.*

**K14 (E, 29):** *Gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketler veya sosyal medya platformları, altta belirtilen bazı sebeplerden dolayı ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet etmekte zorlanabilirler.*

*ABD merkezli büyük teknoloji şirketleri, dünya genelinde milyarlarca dolarlık bir bütçeye sahiptir. Bu şirketler, yüksek teknoloji araştırma ve geliştirme projelerine yatırım yapabilirler ve dünya genelinde pazarlama faaliyetleri için büyük bütçeler ayırabilirler.*

*ABD merkezli teknoloji şirketleri, sürekli olarak yeni ürünler ve hizmetler geliştirmekte ve yenilikler yapmaktadır. Bu şirketler, dijital dünyanın trendlerini ve değişen müşteri ihtiyaçlarını takip ederek, inovasyon yoluyla müşterilerine en iyi deneyimi sunmaya çalışıyorlar.*

*ABD merkezli büyük teknoloji şirketleri, dünya genelinde yüksek bir marka bilinirliğine sahiptir. Bu şirketler, reklam kampanyaları ve sponsorluklar gibi faaliyetlerle dünya genelinde markalarını tanıtmaktadırlar.*

*ABD, yıllardır teknoloji geliştirme ve inovasyon konusunda öncü bir ülke olmuştur. Bu nedenle, ABD merkezli teknoloji şirketleri, en iyi teknoloji alt yapılarına erişebilmektedirler.*

*Benzer girişimlerin yaratılmasında ortamın, yatırımların, teşviklerin etkisi kadar, bu girişimleri kuracak uzmanlara ve girişimcilere ihtiyaç vardır. Genelde işinde uzman olarak kabul edilen eğitimli nüfus kendi yaşadıkları ülkeden daha iyi olanak ve koşulların sağlandığı ABD ve Batı Avrupa merkezli ülkelere göç eder. Yani beyin göçü gerçekleşmiş olur. Beyin göçü daha sonrasında gelişmekte olan ülkelerde gerekli şartlar sağlansa da bu gibi girişimlerin oluşturabilmesi için en büyük engellerden biridir.*

**K15 (E, 33):** *Bu tip şirketler tüm dünyadan yetenekli iş gücü toplamakta, insanlar buralarda çalışabilmek için sıraya girmektedir. Gelişmekte olan ülkelerin bu şirketler tarafından sağlanan ekonomik, teknolojik imkânları ve itibarı, belli seviyenin üzerindeki personele sağlaması güçtür.*

*Bahsi geçen şirketlerin küresel yayılım ve erişim açısından üst seviyede olması iddia edilen sonuçta etkilidir.*

*Bahsi geçen şirketler zaten öncülüğünü ABD'nin yapmış olduğu bilgisayar / internet devriminin bir ürünüdür. Dolayısıyla gelişmekte olan ülkelerin, ekonomik modelinin bir kısmını bu alandaki yetenekli insanları çekmek üzerine kurmuş ve yarım asırdır bu politikasından vazgeçmeyen bir ülke ile rekabeti, takip etmenin yanında öncülük edebileceği alanlar oluşturabilmesi ile mümkün olacaktır.*

# TARTIŞMA

Bu tez çalışmasında dijital dünyada hak ve sorumluluklara yönelik farkındalığın artırılması, dünya toplumunu olumsuz etkileyen temel sorunların çözümüne yönelik önerilerin sunulması hedeflenmiştir. Temel sorunlara yönelik çözüm önerilerini ortaya koymak amacıyla dijital dünyada vatandaşlık haklarıyla ilgili bilimsel çalışmalar yapmış bilim insanlarının ve uzmanların fikirleri değerlendirilerek sunulmuştur. Katılımcılar vatandaşların dijital dünyada aktif, dinamik, bilinçli, katılımcı bireyler olarak sorumluluklarının farkında olmaları ve bunlarla birlikte kapsamlı ve caydırıcı yasal düzenlenmelerin hazırlanması ve uygulanması hususunda önemli bilgiler paylaşmıştır. Gerçek dünyada olduğu gibi dijital dünyada da dezavantajlı konumda olan bireyler, toplumlar veya devletler dijital dünyada da mağdur veya sömürülen konumdadırlar. Katılımcıların görüşlerine göre dijital dünyadaki sorunların aradan kaldırılması için uluslararası iş birliği yapılarak hukuki çerçevenin hazırlanması, caydırıcı yaptırımların uygulanması ve bunun yanı sıra ulusal düzeyde güçlü güvenlik önlemlerinin alınması gerekmektedir.

Dijital sorunların boyutu devletlerin gelişmişlik düzeyine göre farklılık göstermektedir. Söz konusu farklılık düzeyi büyük ölçüde devletlerin sosyoekonomik ve sosyokültürel düzeyine bağlıdır. Başka bir ifadeyle ulusal düzeyde toplumların kültürel ve sosyoekonomik birikimleri farklı düzeylerde olduğu gibi sorunlardan etkilenme boyutları da farklıdır. Dijital olanaklar ulusal sınırları ortadan kaldırdığı için artık ulusal devlet düzeninin eski geleneklerle devam ettirilmesi dezavantajlı konumda olan kesime eziyet etmekten başka bir sonuç doğurmaz. Gelişmemiş ülkelerde hukuk sisteminin örümcek ağı gibi "güçlülerin delip geçtiği, zayıfların takılıp kaldığı" bir perde olduğu, egemen devletlerin de diğer devletlere karşı egemen tutum takınması ve onları sömürmesi bilinen bir gerçektir. Fakat yeni medya olanaklarının yaygınlaşmasıyla yaşanan hak ihlalleri devasa boyutlarda bilinir hale gelmiştir. Başka bir ifadeyle BİT sayesinde dünya genelinde kötülüklerin/hak ihlallerinin bilinirlilik oranı geçmişe nazaran çok artmıştır ve artmaya devam etmektedir. Bu gelişmelere paralel olarak dünya genelindeki huzursuzluk da kat kat artmış durumdadır. Fakat otoriter yönetimler, hükümetler, dev teknoloji şirketleri ısrarla dünya toplumunun büyük bir kısmının huzursuzluğunu ve sosyoekonomik

sorunların altında ezilmesini görmezden gelmektedir. Dünya genelinde ülkelerin dijital dünyadaki sorunlardan etkilenme boyutları farklı olsa da sorunlar tüm dünya düzenini etkilemektedir. Egemenlik mücadelesi uğruna milyonlarca insanın huzursuzluğunu görmezden gelen güç ve kontrol yapıları bencil ve saldırgan tavırlar sergilemektedirler.

Katılımcıların bir kısmı hem gerçek hem de dijital dünyada birçok sorunun temel nedeni olarak bilinen sosyoekonomik sorunların aradan kaldırılması gerektiğini, dijital eşitsizliklerin azaltılması amacıyla serbest piyasa koşullarının oluşturulmasının çözüm olabileceğini, bir kısmı da bilgi ve iletişim teknolojilerini tekelinde bulunduran hegemonik devletlerin ve şirketlerin elinde bulundurdukları gücü kolayca paylaşmak istemeyeceklerini vurgulamıştır. İkinci yaklaşımın günümüz dünyasında hüküm sürdüğü ve uluslararası ölçekte çok boyutlu çözümler üretilmediği bilinmektedir. Teknoloji liderlerinin elindeki imkânları gelişmemiş ülkelerle paylaşma olasılığı düşük olsa da anlamlı bir çözüm olabileceği kesindir. Çünkü dijital dünyada kazanılan servetlerde dünya toplumunun büyük bir kısmının katkısı veya karşılığı ödenmemiş emeği vardır. Dünya genelinde saldırı ve savunma amacıyla harcanan paraların küçük bir kısmının bile dünya toplumunun huzurlu yaşamasını temin etmek için yeterli olacağı tahmin edilmektedir.

Mevcut düzenin değiştirilmesi azami ölçüde dünya toplumunun bilinçlenmesine bağlıdır. Yapılan araştırmalara göre öğretmenlerin veya öğretmen adaylarının bile dijital vatandaşlık konusunda yeterli düzeyde bilinçli olmadığı ve farkındalıklarının artırılması gerektiği ortaya konulmuştur (Vajen, vd., 2023; Nezih, 2018; Martin vd., 2019; Karakuyu, 2023). Bu bilgilere dayanarak sıradan vatandaşların dijital vatandaşlıkla ilgili hangi düzeyde bilinçli olduklarını ve antidemokratik aktörlerin manipülasyon ve müdahalelerine ne kadar açık olduklarını tahmin etmek mümkündür. Dijital teknolojiler yaygınlaştıkça dijitalleşmenin vatandaşlık kavramı üzerindeki etkilerinin farkında olmak her geçen gün daha da zaruri hale gelmektedir. Dünya genelinde daha iyi eğitimin verilmesi ve farkındalığın artırılması, çok yönlü ve kapsamlı önleyici tedbirlerin alınması etkili çözüm olarak belirtilmektedir.

Dijital eşitsizliğe yönelik zararları minimize edebilmek için öncelikle toplumun farklı kesimleri arasındaki sosyoekonomik eşitsizliğin giderilmesi

gerekmektedir. Fakat günümüze kadar insanlık tarihi boyunca bu yönde anlamlı adımlar atılmamıştır. Gelişmekte olan ülkelerde yaşayan toplumlar şeffaflık ve güvenlik sorunu ile doğal olarak karşı karşıyadırlar. Dünya toplumunun neredeyse tamamı çok küçük sayıda güç ve kontrol yapılarının yaratığı eziyetlere katlanmak zorunda kalmıştır. Fakat tüm olumsuz koşullara ve baskılara rağmen dünya toplumu kollektif bilinçlenme ve örgütlenme yaklaşımıyla otoriter grupların girdabından kurtarılabilir.

Bu çalışmada katılımcıların sorunların çözümüne yönelik demokratik ve yasal çerçevedeki önerilerinin uygulanması pek kolay olmayacaktır. Gelişmemiş ülkelerde yargı sisteminin işlevsizliği, yargı iradesinin şantajlarla, parayla ve diğer yollarla ipotek altına alınması ulusal düzeyde kurutulabilecek bir bataklık değildir. Bu tür sofistike sorunların çözümü uluslararası düzeyde kurumların devreye girmesi, gerçek anlamda huzur ve demokrasi adına zorunlu bir ihtiyaçtır. Teknolojik imkânlarla otoriter hükümetlerin dünya toplumu için beka sorunu olduğu belirginleşmiştir. Özelikle otoriter, bencil ve saldırgan davranışlar sergileyen hükümetlerin nasıl kirli ilişkiler içinde olduğu ve nasıl sinsi planlar yaptıkları dijital ortamlarda sızdırılan belgelerle kanıtlanmıştır.

Dünya genelinde hükümetler iki kısma ayrılmaktadır; birincisi kendi çıkarlarını ve koltuğunu korumak için yönettikleri topluma eziyet eden ve sömüren hükümetler (gelişmemiş ülkeler), ikincisi ise yönettikleri toplumun refah düzeyini yükseltmek için başka ülkelerde veya bölgelerde yaşayan insanlara eziyet eden ve sömüren hükümetler (gelişmiş ülkeler). Gelişmemiş ülkelerde devletin imkânlarıyla ultra lüks hayat yaşayan politikacılar halka hizmet etmekten başka her türlü işle uğraşmaktadırlar. Bu düzene dur demek bilinçli, ahlaklı ve erdemli bireylerin girişimleriyle mümkün olacaktır.

# SONUÇ

Teknolojik gelişmelerle birlikte dijital dünyada vatandaşlık hakları konusunda farkındalık oluşturmak ve hak ihlallerine karşı çözüm önerilerinin ortaya konulması her geçen gün daha da elzem hale gelmektedir. Günümüzde dijital dünya ile ilgili durumsal farkındalık, büyük resmi görebilmek, fenomenleri takip etmek, tespit etmek, tanımlamak, zararlı davranışları analiz ederek etkilerini ve sonuçlarını tahmin edebilmek her bir birey için önemlidir. Dijital dünyada gözetim, ifade özgürlüğü, dijital uçurum ve toplumsal tabakalaşma, sansür, bilginin doğruluğu ve yalan haber, siyasi propaganda için dijital olanakların kullanılması, itaat ve direniş, troller ve algoritmalar aracılığıyla algı yönetimi, ötekileştirme ve yankı odaları, dijital ayak izlerinin olumsuz etkileri, dijital bağımlılık gibi sorunların toplumsal düzeni olumsuz etkilediği aşikardır. Özellikle gelişmekte olan ülkelerde otoriter yönetimlerin evrensel insan haklarına aykırı politikalar izlemesi insan haklarının ihlaline yol açmaktadır. Bununla birlikte dünya genelinde dijital uçurum da bireylerin yaşam kalitesini olumsuz etkilemektedir. Öte yandan sömürgeci devletlerin de dijital olanakları evrensel ölçekte bir sömürge aracı olarak kullandıkları da ciddi bir sorun olarak devam etmektedir. Global düzeyde dijital uçurum bağlamında tartışılan veri tekelciliğinin olumsuz etkileri pastadan pay alamayan hükümetleri ciddi anlamda rahatsız etmektedir. Aynı zamanda fiziksel dünya düzeninde olduğu gibi dijital dünya düzeninde de egemen güçler dijital olanaklardan istedikleri gibi faydalanmakta ve dijital teknolojileri toplumları şekillendirmek veya manipüle etmek için kullanmaktadırlar. Bu sorundan da en çok gelişmekte olan veya gelişmemiş ülkeler etkilenmektedir.

Dijital vatandaşlık yalnızca bir dizi hak, sorumluluk ya da uygun davranışlardan ibaret değildir; en samimi kültürel bağlamlarda bile kontrol mekanizmalarını insanlarla ve uygulamalarla birbirine bağlayan akıcı bir arayüz olarak ortaya çıkmaktadır (Vivienne vd., 2016: 1). Vatandaşların haklarının ve sorunlarının farkında olmamaları gündelik hayatın her alanını olumsuz etkilemektedir. Mobil cihazlarda depolanan bilgilerin kişiye özel olmadığını, teknoloji şirketlerinin algoritmalar aracılığıyla kişisel verileri toplayıp metaya dönüştürdüğü, kalitesine bağlı olarak dijital ortamda paylaşılan içerikler için

harcanan zamanın karşılığı ödenmemiş emek olduğu ve siber güvenlikle ilgili tehditlerin temel düzeyde bilinmesi kullanıcılar için faydalı olacaktır. Dijital ortamın adil ve güvenilir olmadığına dair çok sayıda içerikler veya kanıtlar dijital ortamın kendi bünyesinde mevcuttur. Bireysel olarak güvenliğin yüksek düzeyde temin edilmesi için üst düzey bilgi birikimine ve pratiğe sahip olmak gerekmektedir. Bu bağlamda tüm kullanıcıların gereken bilgi birikimine sahip olması pek mümkün değildir. Dijital ortamdaki tüm verilerin depolanabilir, erişilebilir kopyalanabilir ve farklı amaçlar için kullanılabilir olması dünya toplumunu her anlamda endişelendirmektedir. Yetkililer tarafından güvenlik önlemleri alınmış dijital bir ekosistem oluşturulamadığı için bireyler kendi imkânlarıyla güvende kalabilmek için olağanüstü çaba harcamak zorundadırlar. Büyük teknoloji şirketleri, uluslararası kurumlar ve hükümetler tarafından evrensel düzeyde yaşamı, çeşitliliği ve güzelliği desteklemek amacıyla güvenli bir dijital ekosistemin oluşturulması en önemli hedeflerden biri olmalıdır.

Bu çalışmada dijital dünyada vatandaşlık hakları ve sorumluluklarıyla ilgili farkındalığı artırmak amacıyla bazı bilgilere ve verilere yer verilmiştir. Bu bilgilerin yanı sıra tüm dünya toplumunu ilgilendiren beş temel sorunla ilgili bilim insanlarının ve uzmanların görüşleri alınarak farklı kategorilerde değerlendirilmiştir. Dijital dünyada en büyük sorunlardan biri olarak bilinen veri tekelciliğini ve olumsuz etkilerini azaltmak amacıyla uluslararası düzeyde iş birliği yapmak etkili bir çözüm olarak önerilmiştir. Dijital dünyadaki diğer sorunların çözümüne ilişkin önerilere de bakıldığında evrensel düzeyde bir standardizasyonun hazırlanması, ilgili yasal düzenlemelerin tüm dünya ülkeleri tarafından kabul edilmesi, caydırıcı yaptırımların keskin bir şekilde uygulanması en iyi seçenek olarak görülmektedir. Hükümetlerin hazırladıkları mevzuatların karmaşık ve bölük pörçük bir yapıya sahip olması, hak ihlalleriyle ilgili düzenlemelerin tek bir merkezden belirlenmemesi ve caydırıcı cezaların keskin bir şekilde uygulanmaması dijital dünyadaki sorunların artarak devam etmesini sağlamaktadır.

Ulusal düzeyde üretilen çözümlerin etkili olmadığı aşikardır. Ciddi gelir dengesizliğinin olduğu ve hükümetlerin istikrarlı siyasi politikalar yürütemediği, yargı sürecinin bağımsız olmadığı, yolsuzluğun had safhada olduğu, vatandaşların açlık sınırının altında yaşadığı dezavantajlı ülkelerde hükümetlerden dijital

dünyadaki sorunlara yönelik çözüm beklemek de anlamsızdır. Katılımcıların yasal düzenlemelerle ilgili önerilerine bakıldığında rekabet yasalarının uygulanması, tekelciliği önleyecek yasal düzenlemelerin yapılması ve politikaların izlenmesi, devlet bazında uygulanacak ağır yaptırımların ve kontrollerin kayda değer bir fark yaratabileceği, veri koruma yasalarının geliştirilmesi, verilerin uluslararası şirketlere pazarlanmasının önüne geçilmesi ve uluslararası hukuka yönelik düzenlemelerin yeniden yapılması gerektiği belirtilmiştir. Ama bu sorumlulukların ulusal hükümetler tarafından uluslararası bir kurumun baskısı olmadan gerçekleştirilmesi pek mümkün görünmemektedir. Ayrıca daha iyi veri erişiminin sağlanması, çevrimiçi hizmet sağlayanların veriler üzerindeki etkisinin azaltılması ve veri sağlayanlara daha fazla kontrol yetkisinin verilmesi gerektiği de önerilerden bazılarıdır. Gelişmiş ülkelerin gelişmekte olan ülkelerle iş birliği yaparak verilerin ve dijital araçların ücretsiz olarak paylaşılmasına veya dağıtılmasına izin veren açık veri politikaları ve açık kaynaklı yazılımlara erişme imkânı sunulursa onların da dijital ekonomiye katkı sağlayabilecekleri de çözüm olarak sunulmuştur. Fakat kapitalist dünya düzeninde ileri düzey teknoloji üreten ülkelerin bu pastayı gelişmekte olun ülkelerle paylaşmak istememesi bu seçeneğin gerçekleşmesini imkânsız kılmaktadır. Dijital çağda petrolden bile daha değerli olan veriye dayalı dijital ekonomiden elde edilen gelirleri hiçbir şirket kendi isteğiyle paylaşmayacaktır. Ama internet kullanıcılarının karşılığı ödenmemiş emeklerinden ve kullanıcı davranışları ile ilgili satılan verilerden elde edilen paraların adil bir şekilde paylaşılmasını sağlamak için tüm dünya ülkeleri ve ilgili sivil toplum kuruluşları iş birliği yapabilir. Önemli olan sorumluluk ve farkındalık ekseninde kolektif eylem başlatılabilir.

Devlet müdahalesinin ve kontrolünün iyimser amaçlarla artırılması açısından değerlendirildiğinde her ülkenin kendi vatandaşlarının uluslararası platformlar kadar, ulusal platformlara da dahil olmasına etki etmesi, yerel ekosistemin geliştirilmesi ve çözümlerin desteklenmesi, tüm teknolojik araç, cihaz, yazılım ve donanımda millileşmenin gerçekleştirilmesi, bütçeden eğitime ve ARGE çalışmalarına daha fazla olanağın sağlanması ve en önemlisi ise dijital dünyadaki sorunların çözümü için kültürel, ekonomik ve politik olarak çok boyutlu ve kapsamlı çalışmaların yapılması gerektiği belirtilmiştir. Ama gelişmemiş ülkelerde vatandaşların lehine böyle iyimser adımların atılması şimdiye kadar mümkün olmamıştır. Eğer otoriter rejimler

vatandaşların yararına bu kadar iyimser kararlar alsalar kurdukları rejimlerin sonunu getirmiş olurlar. Mantıkla bu önerilerin otoriter hükümetler tarafından gerçekleştirilmesinin mümkün olmayacağını düşünerek uluslararası bir kurumun devreye girmesi önerilmektedir. Perakende çözümlerin yerine dünya genelinde bir tane dijital ekosistemin kurulması ve yönetilmesi çok anlamlı olacaktır. Toplanan verinin niteliği, hangi amaçla ve hangi hizmet sebebiyle toplandığı çok net bir şekilde ifade edilse de kullanıcıların sayfalarca sözleşmeyi okumaya ne zamanı ne de kapasitesi yetmez. Veri etiği, verinin nasıl toplanması, saklanması, kullanılması ve paylaşılması gerektiği tüm dünya toplumu için standart hale getirilmelidir ve evrensel düzeyde standart bir çerçeve belirlenmelidir. Ulusal düzeyde kişisel verilerin toplanması, saklanması, korunması, kullanılması ve paylaşılmasına dair yasal düzenlemeler hazırlanmış olsa da uygulanmadığı yaygın olarak bilinmektedir.

Katılımcılar siber suçlara yönelik ülkeler arasında yapılan anlaşmaların büyük oranda güvenilir olmayacağını belirterek, dijital dünyada siber suçları ve savaşları önlemek amacıyla ağırlıklı olarak teknik tedbirlerin alınmasına ve hukuki düzenlemelerin geliştirilerek uygulanmasına dikkat çekmiştir. Günümüzde dijital evrende uluslararası düzeyde siber suçları önlemek amacıyla dezavantajlı ülkeleri de kapsayan teknik ve hukuku standardizasyonun hazırlanması için geç kalınmıştır. Siber uzayın mülkiyetinin olmamasından kaynaklı devletler arasında ciddi bir eşitsizlik bulunmaktadır. Yani gücü elinde bulunduran diğerleri üzerindeki tahakkümünü artırmakta ve insan haklarına karşı suç işlemektedir. Siber suçları ve savaşları önlemek amacıyla hukuki düzenlemelerin yanı sıra, katılımcıların büyük bir kısmının çeşitli önlemleri içeren çok yönlü bir yaklaşımın gerektiği konusunda hemfikir olduğu görüldü. Elde edilen bulgulara göre katılımcıların yaklaşık yarısı siber saldırılara karşı ülkeler arasında yapılan anlaşmaların güvenilir olmayacağını belirtmiştir. Fakat katılımcıların bir kısmına göre ise anlaşmaların seyrini devletlerarası siyasi ilişkiler belirler. Yani başka bir ifadeyle ülkeler arasındaki çıkar, güven veya iş birliği uluslararası anlaşmaların etkinliğini etkiler. Uluslararası iş birliğiyle siber suçluların tespit edilmesi ve suçluların cezalandırılmasına yönelik anlamlı çalışmalar yapılabilir.

Siber saldırıları ve savaşları önleyici tedbirlerin en başta işletim sistemlerini üretenler tarafından alınması gerektiği, CEH ve CISSP gibi yüksek güvenlik

sertifikalarına sahip uzmanların çalıştırılması veya onlardan destek alınması da önerilmiştir. Hukuki düzenlemeler kategorisindeki yanıtlara bakıldığında dijital güvenlik yasalarının geliştirilmesi, uluslararası normlar ve standartların geliştirilmesi, uluslararası kurumlar tarafından uluslararası standartların hazırlanması ve uygulanması gerektiği belirtilmiştir. Bu durumda uluslararası düzeyde bir yaptırım mekanizmasının geliştirilmesi anlamlı ve zaruri olacaktır. Önerilere dikkat edildiğinde büyük bir kısmı dijital dünyadaki sorunların uluslararası düzeyde çözülmesi gerektiğini vurgulamaktadır.

Eğitim ve farkındalık kategorisindeki öneriler kısmında daha iyi eğitim vermek ve farkındalık yaratmak, siber savunma yeteneklerinin geliştirilmesi, savunmanın her alanında nasıl bir yaklaşım sergileniyorsa aynı şekilde tedbirin alınması, kapsamlı önleyici tedbirlerin alınması gerektiği ifade edilmiştir. Bu öneriler anlamlı olmakla birlikte bireysel tedbirler olduğu için fazla kaynak, çaba ve emek gerektirmektedir. Dünya toplumunu kapsayan dijital standartlar hazırlanmadığı sürece bireyler bireysel olarak bu zahmetlere katlanmak zorunda kalacaklar. Uluslararası kuruluşlar ve hükümetler güvenlikle ilgili kara, deniz, hava boyutlarını önemsedikleri gibi büyük teknoloji şirketlerini de sürece dahil ederek siber güvenlik boyutunu da önemsemek ve önlemler almak zorundadırlar. Çünkü siber saldırıların gerçekleşme ihtimali her zaman vardır. Devletler kendilerinin dijital altyapılarını güçlendirmeli, çağa uygun güvenlik duvarları kurumalıdırlar. Siber saldırıları gerçekleşmeden önce engellemek için önlemler alınmalıdır. Örneğin saldırı zamanı güvenlik duvarı aşılmaya çalışıldığı esnasında uyarı veren ya da kendini kilitleyen sistemler kurulmalıdır.

Hem ulusal hem de uluslararası düzeyde saldıranlara karşı sıkı yaptırımlar uygulanmalıdır. Fakat bu saldırıları tespit etmek için yine uluslararası düzeyde çalışmalar yapmak gerekir. Örneğin BM tarafından dijital haklarla ilgili uluslararası sözleşme hazırlanıp tüm ülkelere imzalatılabilir, caydırıcı yaptırımlar düşünülebilir ve uygulanabilir. Anlaşmaları ihlal eden, özellikle Rus hükümeti gibi agresif yöntemlerle siber saldırılar düzenleyen devletlere karşı ciddi yaptırımlar, ambargolar uygulanmasının yanı sıra gerektiğinde askeri güç de kullanılabilir. Sunucular dünyanın her tarafında bulunduğuna göre, uluslararası iş birliği yapılmadan sorunları kontrol altına almak kolay olmayacaktır. Uluslararası iş birliği ve güvenlik

protokolleri gibi daha kapsamlı tedbirlere ihtiyaç vardır. Çözüm olarak dünya toplumunun haklarını güvence altına almak amacıyla uluslararası düzeyde bir yaptırım mekanizması geliştirilmelidir.

Katılımcılar toplumsal ilişkilerin çeşitli yöntemlerle şekillendirilmesi sorununun çözümüne ilişkin 26 farklı öneri sunmuştur. Bu bağlamda egemen sınıfın dijital dünyada toplumsal ilişkileri çeşitli yöntemlerle şekillendirmesi sorununa yönelik hem ulusal hem de uluslararası düzeyde çözüm olabilecek öneriler sunulmuştur. Dijital platformlarda örgütlenen dijital toplulukların bu tarz manipülasyonların önüne geçmede en etkin yol olabileceği, maddi durumu iyi olmayan vatandaşlar için de internet olanaklarından faydalanma imkânının sağlanması gerektiği, dijital eşitsizliğe yönelik zararları minimize edebilmek için öncelikle toplumun farklı kesimleri arasındaki sosyoekonomik eşitsizliğin giderilmesi gerektiği, toplumu düşünen kesimin bilgilendirme amaçlı videolar yayınlaması ve paylaşılması gerektiği, bu tür sorunları azaltmak için daha fazla açık kaynağa ihtiyaç olduğu, kâr amacı gütmeyen sivil toplum kuruluşlarının ön plana çıkması gerektiği, dijital kapsayıcılık yaklaşımının uygulanması gerektiği, çeşitliliğin ve katılımın teşvik edilmesi gerektiği, farkındalığın ve katılımın sağlanması gerektiği, medya çeşitliliğinin sağlanması gerektiği, dijital okuryazarlık ve eleştirel düşünmenin yaygınlaştırılması gerektiği katılımcılar tarafından önerilmiştir. Özetle kapsamlı önlemlerin alınması gerektiğine vurgu yapılmıştır.

Devletlerin üstlenmesi gereken sorumluluklar açısından bulgular değerlendirildiğinde şeffaflık ve hesap verebilirliğin sağlanması gerektiği, gizliliğin koruması gerektiği, devletlerin dijital dünyada etkin olması ve sahayı egemen sınıflara bırakmamaları gerektiğini dile getirmiştir. Fakat gelişmekte olan ülkelerde zaten devletin egemen güçler tarafından yönetildiği bilinen bir gerçektir. Diğerlerinden farklı olarak yalnız bir katılımcı kullanıcılar hakkında veri toplamak amacıyla genelde aktif katılımın teşvik edildiğini belirtmiştir. Bu yanıt kısmen doğrudur. Ama dünya genelinde, özellikle gelişmekte olan ülkelerde, kırsal alanlarda hale internet erişimi olmayan ve açlık sınırının altında yaşadıkları için son model teknolojik cihazları satın alamayan çok sayıda insanların olduğu da bilinen bir gerçektir. Manipülasyonlardan fazla etkilenmemek için, koşullara uygun yapılanmak, gereken tedbirleri ve önlemleri almak gerçek kişilerin, tüzel kişilerin ve devletlerin

öncelikli meselesi olmalıdır. Bu önerileri gelişmiş ülkelerde dikkate almak mümkündür. Fakat otoriter rejimlerde hükümetler de yönettikleri toplumu manipüle etmektedirler. Gelişmiş ülkelerden farklı olarak gelişmemiş ülkelerde bağımsız/özgür medya ve hukuk sistemi olmadığına göre yöneten sınıfın manipülatif girişimlerine karşı çıkmak mümkün değildir. Sistem büyük hırsızı değil küçük hırsızı yakalamak ve ezmek üzere kurgulandığı için egemen sınıfın sahip olduğu imkânlarla hem dijital dünyada hem de gerçek dünyada toplumu şekillendirmeye çalışması kaçınılmazdır. Genel olarak, dijital eşitsizliği azaltmak ve dijital dünyada toplumun manipülasyonunu önlemek, hükümetler, özel sektör kuruluşları, eğitimciler ve sivil toplum grupları dahil olmak üzere bir dizi paydaşı içeren kapsamlı bir yaklaşım gerekmektedir.

Katılımcılara göre dijital eşitsizlikten kaynaklanan zararları minimize edebilmek amacıyla öncelikle sosyoekonomik refahın yükseltilmesi, toplumun farklı kesimleri arasındaki gelir dengesizliğinin azaltılması, dijital medya okuryazarlığının artırılması ve farkındalıklarının üst seviyeye çıkartılması zaruridir. Bunun yanı sıra geniş bant erişimini artırmak, yeni teknolojileri elde etmek için vergiden muaf uygun fiyatlar, insanların dijital becerilerini geliştirmelerine yardımcı olacak eğitim ve öğretim programlarına erişebilme imkânı sağlanmalıdır. Kullanıcıların dijital dünyadaki yanlış bilgi ve manipülasyonu tespit edebilmesi için dijital okuryazarlık becerilerini ve eleştirel düşünme yeteneklerini geliştirmesi hayati önem taşımaktadır. Egemen sınıf toplumsal ilişkileri şekillendirmek amacıyla ağırlıklı olarak kitle iletişim araçlarını kullandığı için daha fazla medya çeşitliliği, insanların farklı görüşleri duymasına ve dijital dünyada daha geniş bir perspektife sahip olmalarına yardımcı olacaktır.

Dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılması ile ilgili sorunların çözümüne yönelik katılımcıların önerdiği çözümlerin temelini kapsamlı yasal düzenlemelerin hazırlanması, kontrol mekanizmalarının artırılması ve caydırıcı yaptırımların keskin bir şekilde uygulanması oluşturmaktadır. Bunun yanı sıra kullanıcıların bilinçlendirilmesi ve kişisel verilerin korunmasına yönelik önleyici tedbirlerin alınması gerektiği ifade edilmiştir. Bu kapsamda açık veri gizliliği ile ilgili yasaların oluşturulması, sıkı kanunların çıkarılması, kontrol mekanizmalarının artırılması ve yaptırımların taviz

vermeden uygulanması, şeffaflığın artırılması, uluslararası iş birliği ve anlaşmaların yapılması, kurumsal ve devlet düzeyinde de tedbirlerin alınması gerektiği önemle vurgulanmıştır. Kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına yönelik sorunların hem ulusal hem de uluslararası boyutunu göz önünde bulundurmak gerekir. Çünkü kişisel verilerle ilgili hakları hem ticari kurum ve kuruluşlar hem hükümetler hem büyük teknoloji şirketleri hem de dijital dünyadaki hegemonik devletler ihlal etmektedir. Bu sorun çok boyutlu olduğu için yine çözüm üretmek amacıyla uluslararası bir kuruluşun görevlendirilmesi anlamlı olacaktır. Katılımcılar veri etiğinin teşvik edilmesini, internet üzerinden alışverişlere yönelik düzenlemelerin yeniden gözden geçirilmesini ve şirketlere bazı kısıtlamaların getirilmesini, kişisel veri ihlallerinin kullanıcılara bildirilmesini, yasal, teknolojik ve etik önlemlerin bir kombinasyonuyla sorunların çözülmesi gerektiğini belirtmiştir. Uzmanlar bu koşullarda yüzde yüz veri güvenlinin mümkün olmayacağını, sadece bilinçli olanların verilerini rastgele erişilebilirlikten koruyabileceğini dile getirmiştir.

Dijital dünyada kişisel verilerin toplanması saklanması ve korunması hususunda uluslararası düzeyde henüz net bir konsensüs sağlanmamıştır. Dünya ülkelerinin büyük ekseriyeti henüz kendi sistemlerini üretemediklerine göre ABD ve Çin merkezli platformlara ve teknolojilere mahkûm durumdadırlar. Gelişmekte olan ülkeler tarafından üretilen teknolojiler de genelde düşük kalitede olduğu için pek tercih edilmemektedir. Kullanıcıların kişisel verileri ve davranış alışkanlıkları ticari amaçla satılabilecek veriler olduğu için kullanıcılar uygulamaları kullanmak için para ödeseler dahi yene de kişisel verileri toplayan büyük teknoloji şirketleri, kurum ve kuruluşlar tarafından kâr amacıyla kullanılmayacağına inanmak mümkün değildir.

Sosyal medya platformlarını geliştirip hizmete sunanlar işlerine geldiği gibi sözleşmeler düzenlemiş, eğer geliştirdiğim platformu kullanmak istiyorsan koşullarımı da kabul edeceksin diyorlar. Dolayısıyla o dayatılan sözleşmeleri kabul etmeden uygulamaları kullanmak mümkün olmadığına göre kullanıcılar onları okumadan bile kabul etmek mecburiyetinde kalıyorlar. Özetle kullanıcılar o küçük puntolarla yazılmış sayfalarca sözleşmeyi veya çerezleri istemeden kabul etmek zorundadırlar. En azından verilerin ikincil işlenmesine ilişkin veri sahiplerinden onay alınması için bir onay mekanizması geliştirilmelidir. Katılımcılara göre kişisel

verileri toplayan ve depolayan şirketler ve kuruluşlar, şifreleme, erişim kontrolleri ve izleme gibi güçlü veri koruma önlemleri uygulamalıdır. Kullanıcılar verilerine erişme, kim tarafından ve nerde saklandığını bilme, nasıl kullanılacağını bilme, istedikleri zaman silmek gibi daha fazla kontrole sahip olmalıdırlar. Avrupa'da Genel Veri Koruma Yönetmeliği anlamına gelen "General Data Protection Regulation (GDPR)" başta olmak üzere tüm dünyada bu konuda yürütülmekte olan çeşitli çalışmalar vardır. Ama sonuçlar yeterli düzeyde tatmin edici değildir. Kapsamlı bir yaklaşımla önleyici tedbirler alınmalıdır ve özellikle çok kullanıcılı kişisel veri barındıran siteler çok sıkı kontrol edilmelidir. Olay gerçekleştikten sonra cezaların verilmesi bile etkili bir yöntem değildir. Mevcut koşullarda kişisel verilere ilişkin sorunların etkili bir şekilde çözümü pek kolay olmayacaktır.

Katılımcıların gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketlerin, dijital platformların ve teknolojilerin serbest piyasada ABD merkezli büyük teknoloji şirketleriyle küresel ölçekte rekabet edebilmesini zorlaştıran faktörlere ilişkin görüşleri dört kategoride değerlendirilmiştir. Birinci kategoride görünüşte rekabet yasalarına aykırı olmayan nedenlere yer verilmiştir. Katılımcılara göre gelişmekte olan ülkelerin başarısız olmasının temel nedenleri kaynakların eksikliği, teknolojik alt yapının yetersizliği, fikri mülkiyet haklarıyla ilgili engeller, iç mevzuatlardan ve düzenlemelerden kaynaklanan sorunlar, finansal güç eksikliği, inovasyon eksikliği, marka bilinirliği, beyin göçü, coğrafi dağılım, kümülatif birikim, satın alma modeli ve devlet desteğinin olmamasıdır. Yarım asırdır ABD, yüksek hızlı internet ve güvenilir elektrik dahil olmak üzere teknoloji tabanlı şirketleri ve sosyal medya platformlarını desteklemek için iyi geliştirilmiş bir altyapıya sahiptir. Doğal olarak bu durumda piyasaya şimdiye kadar giriş yapamayan gelişmekte olan ülkelerin ABD ve Çin ile rekabet etmesi hiç kolay olmayacaktır. Fakat her zaman fırsatlar mevcuttur, Çin hükümetinin yaptığı gibi diğer hükümetler de ABD'nin tahakkümünü azaltmak için yerli teknolojiler ve platformular üretebilirler. Eğer dünya ülkeleri ABD'nin dijital egemenliğini zayıflatabilirse uluslararası düzeyde güvenli bir dijital ekosistemin oluşturulması süreci de hızlanmış olacaktır.

İkinci kategoride, katılımcılar aslında serbest piyasa koşullarının mevcut olmadığını, gelişmiş ülkelerin kendi şirketlerinin ve firmalarının çıkarlarını korumak

için uluslararası boyutta piyasaları etkilediğini dile getirmiştir. ABD merkezli şirketler, hem gelecek vaat eden teknoloji tabanlı şirketleri hem de alanda çalışan parlak beyinleri hızlı ve başarılı bir şekilde satın alıyorlar, satın alamadıkları şirketlerin maddi kaynaklarını ve veri kaynaklarını kısarak yok olması için gereken zemini hazırlıyorlar. ABD bu adımları sadece dijital dünyadaki egemenliğini korumak için değil, genel olarak her alanda egemenlik taslayabilmek için, kurdukları sömürü düzenini devam ettirebilmek için dijital olanakları bir araç olarak kullanmaktadır.

Üçüncü kategoride gelişmekte olan ülkelerde itibar, şeffaflık ve güvenlik sorununun olduğu vurgulanmıştır. Bu kategoride güvenlik sorunu iki alt kategoride değerlendirilmiştir. Birinci alt kategoride gelişmekte olan ülkelerdeki dijital teknoloji şirketlerin kişisel verilerin korunması açısından güvenilmez olduğu, ikinci alt kategoride ise gelişmekte olan ülkelerdeki siyasi istikrarsızlık ve hukuk sisteminin işleyişiyle ilgili sorunlara dikkat çekilmiştir. Katılımcılara göre; ABD merkezli teknoloji şirketleri, sundukları fırsatlarla bilim insanlarını, mühendisleri, yatırımcıları ve iş profesyonellerini dünyanın dört bir yanından cezbedebilmektedir. Fakat gelişmekte olan ülkeler, düşük ücretler, sınırlı kariyer gelişimi ve siyasi istikrarsızlık, kısıtlayıcı düzenlemeler gibi faktörler nedeniyle üst düzey yetenekleri çekmek ve elde tutabilmek konusunda çok zorlanmaktadır. Bu tür sorunlardan dolayı üst düzey yetenekli nüfus kendi yaşadıkları ülkeden daha iyi olanak ve koşulların sağlandığı ülkelere göçerek oralarda çalışabilmek için sıraya girmektedir.

Dördüncü kategoride bazı katılımcılar güçlü teknolojilerin ve sosyal medya platformların sadece finansal olarak güçlü olan ülkeler tarafından değil, finansal gücü zayıf olan ülkeler tarafından da üretilebildiğini ifade edilmiştir. Ayrıca gelişmekte olan ülkelerde elit kesimin inovasyondan çok kendilerini güvende tutmak için yatırımlar yaptığı çok açık bilinen sorunlardan bir tanesidir. Ancak kaynakların, altyapının, yeteneğin ve düzenleyici desteğin doğru bileşimi ile gelişmekte olan ülkelerdeki şirketlerin küresel pazarda rekabet etmesi ve başarılı olmaları mümkün olacaktır. Örneğin İsrail bu doğrultuda gereken yatırımlar yaparak ve uygun politikalar izleyerek dijital dünyanın avantajlarından faydalanmaktadır.

Dijital teknolojilerin yaygınlaşmasıyla dünyanın küçük bir köye dönüşmesini göz önünde bulundurarak uluslararası bir kuruluşun öncülüğünde, tüm paydaşların

katılımıyla global düzeyde güvenli bir dijital ekosistemin yaratılması gerekliliği bulunmaktadır. Dünyanın dört bir yanında uluslararası düzeyde iş birliğinin önemi her geçen gün artarak devam etmektedir. Bunula birlikte uluslararası normlara, ulusötesi anlaşmalara ve yerel uygulamalara daha çok atıf yapılmaktadır. Artık dünya genelinde etkin bir e-yönetişim modelinin uygulanması ve kamu hizmetlerinin modern bilgi ve iletişim altyapısı üzerinden yürütülmesinden ziyade dijital çağa uygun siyasal, hukuksal, sosyal, kültürel, güvenlik ve en önemlisi ekonomik yönleriyle koşulların uygun olduğu kapsamlı bir ekosisteme ihtiyaç vardır. Nitekim dünya bilişim devi Microsoft çevirim içi teknolojinin fırsatlarını ve tehditlerini iyi bildiği için dijitalleşme ve dijital vatandaşlığın tüm dünyada geçerli davranış normlarının hazırlanması gerektiğini yazılı rapor halinde hükümetlere sunmuştur (Çakmak, & Aslan, 2018: 79).

Etkili stratejiler, kökleri uluslararası iş birliğine dayanan kapsamlı ve sınırsız bir yaklaşım gerektirir (Veriter, 2021). İlk etapta evrensel düzeyde bir standardizasyon hazırlamak temel bir ihtiyaç olduğuna göre gerekli yasal düzenlemeler dünya ülkelerinin katılımıyla ortak mutabakat olarak çıkartılmalıdır. Ondan sonra en önemli husus çıkarılan yasaların uygulanması için uygun koşulların hazırlanması ve uygulanma sürecinin titizlikle takip edilmesidir. Sadece yasal çerçeve hazırlayıp uygulanmasını gelişmiş ülkeler hariç hükümetlerin inisiyatifine bırakmak hiçbir olumlu sonuç doğurmayacaktır. Gelişmiş ülkelerin diğer ülkelerden en önemli farkı ise belirli bir düzenin olması, özgür medyanın (ifade özgürlüğü) ve bilinçli toplumun hükümetleri keyfi hareket etmekten sakındırmasıdır. Çünkü devlet yönetiminde önemli olan kişiler değil, sistemdir. İnsan haklarını önemsemeyen yönetimler uluslararası kuruluşlar tarafından çeşitli teşviklerle veya zorlayıcı tedbirlerle hizaya getirilmelidir. Gelişmiş ülkeler yalnız kendilerini değil gelişmemiş ülkeleri de kapsayan tek tip ve sürdürülebilir çözümler üretmelidirler. Çünkü artık internet sayesinde tüm bariyerler ve sınırlar aşılmıştır. Uluslararası şirketlerin ekonomik, hukuki ve siyasi güçleri bazen ulusal devletlerin gücünü aşabilmektedir. Bu noktadan bakıldığında dünya genelinde çok boyutlu ve kapsayıcı önlemlerin alınması hayati önem taşımaktadır. Dijital dünyadaki sorunları çözmek için tek yol evrensel düzeyde tarafsız kuruluşlar tarafından kapsamlı yasal düzenlemelerin hazırlanması ve gerekirse zorla uygulanmasıdır.

Hükümetler, siber suçlara karşı kolluk kuvvetlerinin çabalarını güçlendirmekle siber suçluların soruşturulması ve kovuşturulmasında uluslararası iş birliğini geliştirmek için birlikte çalışabilirler. Çünkü dijital dünyada siber saldırıların ve savaşların önlenmesi meselesi, teknik, hukuki ve diplomatik tedbirler dahil olmak üzere çeşitli önlemleri içeren çok boyutlu bir yaklaşımı gerektirmektedir. Bunun yanı sıra bireyler, kuruluşlar ve ticari şirketler güvenlik duvarları, antivirüs yazılımı ve şifreleme gibi güçlü güvenlik önlemleri alarak kendilerini siber saldırılara karşı koruma yeteneklerini geliştirmelidirler. Bu bağlamda bireyleri ve kuruluşları siber saldırıların riskleri hakkında eğitmek, riskleri nasıl önleyecekleri veya nasıl müdahale edecekleri konusunda eğitmek etkili bir önlem olacaktır. Özetle dijital dünyadaki sorunları azaltmak için uluslararası düzeyde bir iş birliği modeliyle evrensel olarak adil ve güvenilir bir dijital ekosistem oluşturmak dünya toplumu için büyük önem arz etmektedir.

Dünya genelinde hükümetler ve ulusüstü oluşumlar (AB) dijital ortamdaki risklere karşı güvenlik önlemleri alarak kendilerini dijital dünyadaki zararlı eylemlerden korumaya çalışıyorlar. Ama bu tür girişimlerin sadece devletlere veya bölgelere yönelik değil global düzeyde düşünülmesi, tüm dünya toplumunun haklarının güvence altına alınması daha az zahmetli, daha az maliyetli ve etkili olacaktır. Şimdilik hükümetler ayrı ayrılıkta önlemler almak için büyük miktarda kaynak ve zaman harcasalar da etkili sonuç alamıyorlar. Dijital dünyadaki hak ihlalleri ve siber güvenlikle ilgili bireysel çabaların efektli olmadığını anladıktan sonra hükümetler dünya toplumunun güvenliğini sağlamak amacıyla daha geniş bir meşrulaştırıcı tahayyül içerisinde yer almaya mecbur kalacaklar. Örneğin ticari sırların korunması ile şeffaflık arasında doğru dengenin kurulamaması şirketler için, aşırı kaynak ve enerji israfına neden olduğu gibi, bireylerin de kendi imkânlarıyla haklarını korumaya çalışması, siber saldırılardan korunmaya çalışmaları kaynak, zaman ve enerji israfına neden olmaktadır. Bu örneklerden de anlaşıldığı gibi dünya genelinde güvenilir bir dijital ekosistemin oluşturulması, saldırgan tavırlar sergileyen bireylerin ve hükümetlerin keskin bir şekilde cezalandırılması barış ve huzuru korumak adına faydalı bir girişim olacaktır. Bu girişimlerin gerçekleştirile bilmesi için bölgesel güç olama saçmalığı sonlandırılmalı ve sömürü amaçlı bencil politikalar sergileyen devletler dünya toplumun eleştiri odağı olmalıdır. Örnek olarak

ABD'nin Ortadoğu'da "hak arama" saçmalığı gösterilebilir. Başka bir ülkenin tabii kaynaklarını sömürmeğe veya savaş ekonomisi yaratıp nemalanmaya hiçbir ülkenin hakkı olamaz. Bu tür girişimler en hafif tabirle etik sorun (ahlaksızlık) olarak nitelendirilmeli ve sonlandırılması için uluslararası düzeyde gereken adımlar atılmalıdır. Dünya genelinde barış ve huzuru tahsis edip korumak için dünya liderleri dürüst politikalar izlemelidir. ABD'nin Ukrayna'da insanlara karşı savaşı durdurmak için destek verdiği, ama Gazze'de binlerce (yaklaşık 45 bin) insanın ölümüne destek verdiği gibi çelişkili politikalara karşı dünya toplumu tarafından kitlesel tepkiler gösterilmelidir. İyi olan herkes için iyi, kötü olan herkes için kötüdür yaklaşımıyla dünya toplumu ikili politik standartlara karşı adete tek bir sesle konuşur gibi tepki göstermelidir.

Yapay zekâ ekosistemi, siber güvenlik ekosistemi gibi ayrı ayrı ekosistemler geliştirmekle birlikte evrensel bir güvenilir dijital ekosistem geliştirmek daha etkili bir çözüm olacaktır. Bilindiği gibi hiçbir araç kendiliğinden iye veya kötü olmadığı gibi teknolojiler de kendiliğinden iyi veya kötü değildir. Dijital teknolojileri iyi veya kötü yapan şey onların kullanım amacıdır. Aynı yaklaşım dijital olanaklar ve yenilikler için de geçerlidir. GAMAM (Google, Amazon, Meta, Apple, Microsoft) gibi büyük teknoloji şirketlerinin sahipleri isterse modern teknolojileri ve büyük veriyi istisnasız bir şekilde dünya toplumuna fayda sağlamak amacıyla kullanabilirler. Olumsuz senaryolara rağmen kullanım amacına bağlı olarak yapay zekâ ve blockchain teknolojileri adil bir dünya düzeni sağlamak için etkili bir araç olarak kullanılabilir. Çevrimiçi platformlara ilişkin düzenlemelerin etkili olabilmesi için, prosedürel şeffaflığa ve hesap verebilirliğe (içerik denetimi) odaklanmanın yanı sıra daha fazla rekabete ve çoğulculuğa izin verilmesi gerekir (Veriter, 2021). Aynı zamanda global bir dijital ekosistem üzerinden kullanıcı odaklı ve şeffaf hükümetlerle sınır ötesi hareketlilikler desteklenebilir, hükümetlerin devletin gücünü kötüye kullanması engellenebilir, sömürgeci politikalar izleyen devletlerin faaliyetlerine karşı çıkılabilir.

Silikon Vadisi ile ilgili politikalar, finansal yatırımlar, fikri mülkiyet hakları ile ilgili yasal düzenlemeler, beyin göçü politikaları ve başarılı projelerin büyük miktarda paralarla satın alınması gibi yöntemler diğer ülkelerdeki girişimlerin başarısız olmasını desteklemektedir. Bunula birlikte dijital dünyanın Silikon Vadisi'ndeki teknoloji

şirketlerinin tekelinde olduğu, serbest piyasa koşulların ve rekabet koşullarının ihlal edildiği bilinen bir durumdur. Mevcut düzende dijital olanakların sağladığı imkânlardan hem büyük teknoloji şirketleri hem de otoriter ve sömürgeci hükümetler insan haklarını ihlal ederek nemalanmaktadır. Anlaşılan dünya toplumu bilinçlenip hepsine karşı çıkmadığı sürece bu düzen kolay bir şekilde değişmeyecektir. Ayrıca Çin'in dijital dünyada ABD'ye karşı güçlü bir rakip olarak ortaya çıkması da olumlu bir gelişmedir. Çünkü tüm olumsuz koşullara rağmen kullanıcıların en azından dijital hizmetler, platformular ve ürünler arasında seçim yapma şansı olacaktır.

Hükümetler, uluslararası kuruluşlar, büyük teknoloji şirketleri ve uzman toplulukları uluslararası mutabakat çerçevesinde insan hakları, eğitim, şeffaflık ve kapsayıcı diyalog gibi değerlere odaklanarak dünya toplumunun tamamını kapsayan demokratik stratejiler izlemelidir. Dijital dünyada kilit rol oynayan kuantum hesaplama, yapay zekâ, blockchain ve kritik çip teknolojileriyle silahlanma yarışlarını, küresel liderlik ve ekonomik çıkar mücadelelerini hızlandırmak yerine dünya toplumunun yaşam kalitesini artırmak için kullanılması daha erdemli bir davranış olacaktır. Fakat bu erdemli davranışı büyük teknoloji şirketleri ve hükümetler kendi isteğiyle sergilemeyecekler. Dijital kalkınma stratejilerini ve küreselleşmenin gelecekteki hatlarını yeniden tanımlamak için yeni teknolojilerin akıllı bir şekilde benimsenmesi, gelişmiş ortaklıklar ve daha fazla entelektüel liderliğe ihtiyaç var (UNCTAD, 2019: 6). Dünya toplumu güvenli bir dijital ekosisteminin yaratılması ve onun korunmasına yönelik adımların atılması ve uluslararası bir kurumun bu konuda görev üstlenmesi hususunda hükümetlere, uluslararası kuruluşlara ve büyük teknoloji şirketlerine baskı yapmalıdır. Başka türlü dijital dünyada demokratik/insani değerler göz ardı edilerek saldırı ve savunma stratejilerinin geliştirilmesiyle ortaya çıkan çatışmaları ve huzursuzlukları sonlandırmak kolay olmayacaktır. Örneğin AB üye devletler için "Dijital Tek Pazar" tüzüğüyle büyük platformları ve arama motorlarını verilerin toplanması, saklanması, dezenformasyon, nefret söylemi gibi zararlı içeriklerle ilgili yeni kurallara uymak zorunda bırakmıştır. AB'nin 27 üye devlet için güvenli ekosistem oluşturma mantığıyla tüm dünya ülkeleri için de benzer sistemi oluşturmak mümkündür. Fakat bu projenin somut eylem planlarına nasıl dönüştürülebileceği konusu bu tez çalışmasının sınırlılıkları arasındadır.

Global bir dijital ekosisteme ait örnek bir platform olarak “Global Network Initiative (GNI)” gösterilebilir. GNI, şirketlerin, akademisyenlerin, yatırımcıların ve sivil toplumun tek bir sesle konuştuğu ve dünya çapında dijital dünyada insan haklarına saygı duyan yasa ve politikaları savunmak için hükümetleri ve uluslararası kurumları toplu olarak bir araya getiren benzersiz yetkili bir platformdur. GNI, 2017 yılından itibaren politika çalışmalarını dört öncelikli konu alanında yapmıştır: Ağ kesintileri, aracı sorumluluk ve içerik düzenlemesi, gizlilik ve gözetim ve yargı yetkisine ilişkin iddialar ve sınırlar (Global Network Initiative).

Bu çalışmada dijital hak ve sorumlulukların güvence altına alınması ve dünya toplumunu olumsuz etkileyen sorunların çözülmesi için uluslararası bir kurumun kontrolünde hükümetlerin, büyük teknoloji şirketlerinin iş birliği çerçevesinde evrensel ve güvenli bir dijital ekosistemin hazırlanması savunulmaktadır. Bu öneriler sosyal sistemlerin ve ekonomik sistemlerin işleyişi de göz önünde bulundurularak uluslararası tarafsız bir kurum tarafından gerçekleştirilse dünya düzeni daha şeffaf ve huzurlu hale gelebilir. Büyük teknoloji şirketlerinin hepsini kapsayan hesap verebilirlik mekanizması kurmak, verilen zararların tespit edilmesi (muhasebeleştirilmesi) ve tazmin edilmesi anlamlı bir girişim olacaktır. Gelecekteki araştırmaların ağırlıklı olarak dijital dünyada hak ve sorumlulukların kapsamlı bir şekilde güvence altına alınmasını hedefleyen evrensel ve güvenli bir dijital ekosistemin oluşturulması ve işleyişine yönelik yapılması önerilmektedir.

# KAYNAKÇA


Abudu, H., Wesseh Jr, P. K., & Lin, B. (2023) Does political propaganda matter in mitigating climate change? Insights from the United States of America. Journal of Management Science and Engineering, 8(3), 386-397.

Adak, M. M., & Mustafa, K. (2022) COVID-19 pandemi döneminde uygulanan uzaktan eğitim sürecinde bilişim teknolojileri öğretmenlerinin deneyimlerinin incelenmesi. Uşak Üniversitesi Eğitim Araştırmaları Dergisi, 8(1), 30-45.

Adams, T., Bezner, J., & Steinhardt, M. (1997). The conceptualization and measurement of perceived wellness: Integrating balance across and within dimensions. American Journal of health promotion, 11(3), 208-218.

Against Disinformation, A. P. (2018) Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 5.12.2018 version. URL: https://ec. europa. eu/newsroom/dae/document. cfm.

Ahmed, I., Jeon, G., & Piccialli, F. (2022) From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where. IEEE Transactions on Industrial Informatics, 18(8), 5031-5042.

Akçay, D. (2020) Ebeveynlerin çocukların dijital video oyunları bağımlılığı karşısında tutum ve davranışları. Middle Black Sea Journal of Communication Studies, 5(2), 65-71.

Akkuş, B., & İzci, N. A. (2018) Sistem yaklaşımı, kavramları ve yönetim. Recep Tayyip Erdoğan Üniversitesi Sosyal Bilimler Dergisi, 4(7), 223-237.

Akman, A. Z. (2023) Toplum 5.0 yapılanmasında dijital dönüşüm ile örgüt kültürü etkileşiminin yeri: Bir alan araştırması (Doctoral dissertation, Necmettin Erbakan University (Turkey).

Aksakallı, G. (2023) Sosyal Medyada Nefret Söylemi: Toplumsal Sorunun Büyüyen Tehlikesi. 2 Ağustos, 2023. Güvenliweb. Erişim tarihi; 06.04.2023. https://www.guvenliweb.org.tr/blog-

detay/sosyal-medyada-nefret-soylemi-toplumsal-sorunun-buyuyen-tehlikesi

Aktan, E. (2018) Büyük veri: Uygulama alanları, analitiği ve güvenlik boyutu. Bilgi Yönetimi, 1(1), 1-22.

Aktaş, Z. (2023) David Hume'da Siyasal Otoriteye İtaat Yükümlülüğünün Gerekçesi ve Sınırları. Felsefe Dünyası, (77), 140-164.

Alatawi, F., Cheng, L., Tahir, A., Karami, M., Jiang, B., Black, T., & Liu, H. (2021) A survey on echo chambers on social media: Description, detection and mitigation. arXiv preprint arXiv:2112.05084.

Alblwi, A., Al-Thani, D., McAlaney, J. ve Ali, R. (2020, Aralık) Sosyal ağ sitelerinde ertelemeyi yönetmek: D-Crastinate yöntemi. Sağlık Hizmetlerinde (Cilt 8, Sayı 4, s. 577). Multidisipliner Dijital Yayıncılık Enstitüsü.

Alhazbi, S. (2020) Behavior-based machine learning approaches to identify state-sponsored trolls on twitter. Ieee access, 8, 195132-195141.

Allen, D. W., & Berg, C. (2020) Blockchain governance: what we can learn from the economics of corporate governance. Allen, DWE and Berg, C (Forthcoming) Blockchain Governance: What can we Learn from the Economics of Corporate Governance.

Al-Rawy, M., & Elci, A. (2021) Advanced Security Using Blockchain and Distributed Ledger Technology. In Blockchain Technology for Data Privacy Management (pp. 109-131). CRC Press.

Altuwairiqi, M., Arden-Close, E., Bolat, E., Renshaw-Vuillier, L., & Ali, R. (2019, October) When people are problematically attached to social media: How would the design matter? In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 4211-4218). IEEE.

Amanzholova, A., Doğru, İ. A., & Coşkun, A. (2019) Twitterda Veri Madenciliği Yöntemlerin Kullanarak Bot Tespiti. Journal on Mathematic, Engineering and Natural Sciences (EJONS), 3(11), 98-107.

American Library American library association presidential committee on

Association. (1989) information literacy. http://www.ala.org/ala/acrl/acrlpubs/whitepapers/presidential. htm.

Andrew, J., & Bernard, F. (Eds.). (2021) Human Rights Responsibilities in the Digital Age: States, Companies and Individuals. Bloomsbury Publishing.

Andrzejewski, C., Horigoshi, A., Maher, A. I., & Solis, J. A. (2023) Innovators and emulators: China and Russia's compounding influence on digital censorship. Orbis, 67(4), 626-654.

Ankaralı, E., & Yılmaz, B. (2022) Türkiye'de Düşünce Özgürlüğü Konusundaki Basılı Kaynakların Nicelik ve İçerik Analizi: 1928-2020. Bilgi Yönetimi, 5(2), 280-301.

Ansbacher, H. L., & Ansbacher, R. R. (1956) The individual psychology of Alfred Adler.

Ardahanlıoğlu, B. (2022) Nitel araştırmalarda online derinlemesine görüşme tekniği ile veri toplama: bir lisansüstü tez örneği. Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (51), 1-12.

Aristotle (1999) Politics. Batoche books: Kitchener. Çev. Benjamin Jowett. Ss 37-38.

Arora, A., Barrett, M., Lee, E., Oborn, E., & Prince, K. (2023) Risk and the future of AI: Algorithmic bias, data colonialism, and marginalization. Information and Organization, 33(3), 100478.

Asch, S. E. (2016) Effects of group pressure upon the modification and distortion of judgments. In Organizational influence processes (pp. 295-303). Routledge.

Aslan, A. (2022) Dijital Hayattaki Etik İhlallerin Tespiti ve Analizi: Cambridge Analytica Veri Skandalı. Yeni Bir Dergi: Medya Okuryazarlığı Araştırmaları Dergisi, 57.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023) A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Atalay, G. (2022) Yerel Katılım Hakkının Dijitalleşen Yönü: Dijital Katılımcı Bütçe Pratiklerine Bağlantısal Bütünsellik Açısından Bakış.

Austin, E. W., Pinkleton, B. E., Chen, Y. C., & Austin, B. W. (2015) Processing of sexual media messages improves due to media literacy effects on perceived message desirability. Mass Communication and Society, 18(4), 399-421.

Avrupa Birliği'nin resmî gazetesi (2022) Avrupa Parlamentosu ve Konseyin (AB) 2022/2481 sayılı kararı. 19.12.2022. Avrupa Birliği'nin resmî web sitesi: http://data.europa.eu/eli/dec/2022/2481/oj

Avrupa Konseyi (2021, 06 26) Anahtar alan adları. Avrupa Konseyi: https://www.coe.int/en/web/digital-citizenship-education/active-participation

Aydemir, M. (2019) Yenilenen sosyal bilgiler dersi öğretim programının dijital vatandaşlık ve alt boyutları açısından incelenmesi. Uluslararası Güncel Eğitim Araştırmaları Dergisi, 4(2), 15-38.

Aydın, A. (2023) Türkiye'de akıllı şehir uygulamalarına bakış: Esenler akıllı belediye uygulamaları ve nar inovasyon bölgesi örneği.

Baezner, M., & Robin, P. (2017) Stuxnet (No. 4). ETH Zurich.

Bahar, H. İ. (2009) Sosyoloji (Vol. 31). Usak Books.

Bakan, S., & Tuncel, G. (2012) Küreselleşmenin ulus devlet üzerindeki etkisi. Birey ve Toplum Sosyal Bilimler Dergisi, 2(1), 51-66.

Balcı Candan, İ., & Güzelipek, Y. A. (2023) Siber çatışmaların Çin-ABD ilişkileri üzerine etkisi (Master's thesis, Karamanoğlu Mehmetbey Üniversitesi).

Bamman, D., O'Connor, B., & Smith, N. (2012) Censorship and deletion practices in Chinese social media. First Monday.

Barkuş, F., & Mustafa, K. (2019) Dijital mahremiyet kavramı ve ilgili çalışmalar üzerine bir derleme. Bilim Eğitim Sanat ve Teknoloji Dergisi, 3(1), 35-

44.

Barrantes, R. (2007) 2. Analysis of ICT demand: what is and how to measure digital poverty?

Bates, C. C., & Rose, M. C. (2022) Leveraging Talent to Dominate in Cyber War—An Army Perspective. The Great Power Competition Volume 3: Cyberspace: The Fifth Domain, 319-346.

Batke, J., & Ohlberg, M. (2020) Message Control: How a New For-Profit Industry Helps China's Leaders 'Manage Public Opinion.'. China File.

Batson, C. D. (2009) These things called empathy: eight related but distinct phenomena.

Bauman, Z. (2011) Postmodern Etik, (Çev: Alev Türker), Ayrıntı Yayınları, İstanbul. 2.basım.

Bauman, Z. (2017) Akışkan Modernite, Çev: Sinan Okan Çavuş, İstanbul: Can Yayınları.

Bauman, Z., & Lyon, D. (2013) Akışkan Gözetim (Çev. Elçin Yılmaz), İstanbul: Ayrıntı Yayınları.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. ve Walker, RB (2014) Snowden'dan Sonra: Gözetimin etkisini yeniden düşünmek. Uluslararası siyaset sosyolojisi, 8 (2), 121-144.

Bausch, K. C. (2001) The emerging consensus in social systems theory (p. c2001). New York: Kluwer Academic/Plenum Publishers.

Bayraktar, H., Gülşen, B., Sengör, E. S., & Badem, H. (2022) Akıllı şehirlerde veri. CBS Sempozyumu (UZAL-CBS 2022), 17-19 Kasım 2022, Ankara.

Beck, M. (2020) The aggravated struggle for regional power in the Middle East: American allies Saudi Arabia and Israel versus Iran. Global Policy, 11(1), 84-92.

Bedford, S. (2017) "The Election Game:" Authoritarian Consolidation Processes in Belarus. Demokratizatsiya: The Journal of Post-Soviet Democratization, 25(4), 381-405.

Beesley, A. (22 May 2023) Meta Fined Record €1.2bn by Irish Regulator for Violating European Privacy Rules, IRISH TIMES. Access Date: 20.04.2024. https://www.irishtimes.com/technology/big-tech/2023/05/22/facebook-owner-meta-fined-record-12bn-by-irish-regulator-for-violating-european-privacy-rules/

Bellamy, R. (2008) Citizenship: A very short introduction. OUP Oxford.

Bellavitis, C., Fisch, C., & Momtaz, P. P. (2023) The rise of decentralized autonomous organizations (DAOs): a first empirical glimpse. Venture Capital, 25(2), 187-203.

Benedek, W. (2023) Digital Human Rights and Artificial Intelligence. Union UL Sch. Rev., 14, 227.

Bentham, J. (2020) The panopticon writings. Verso Books.

Bergengruen, V. (2024) “How Tech Giants Turned Ukraine Into an AI War Lab,” Time, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

Bertsou, E., & Caramani, D. (2022) People haven’t had enough of experts: Technocratic attitudes among citizens in nine European democracies. American Journal of Political Science, 66(1), 5-23

Bıçakcı, S. (2014) NATO’nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. Uluslararası İlişkiler Dergisi, 10(40), 100-130.

Biden, J. R. (2023) Executive order on the safe, secure, and trustworthy development and use of artificial intelligence.

Bilge, R. (2016) Sosyal medyada nefret söyleminin inşası ve nefret suçlarına ilişkin yasal düzenlemeler. Yeni medya, (1), 1-14.

Bilgi ve İletişim Güvenliği Rehberi (2020) Bilgi ve İletişim Güvenliği Rehberi. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. Available at:

https://cbddo.gov.tr/bigrehber/ Accessed: 24, 04, 2023.

Bilgin, K. R. (2023) Geleceğin Savaşlarında Yapay Zekâ. Güvenlik Stratejileri Dergisi, 145-166.

Bincan, S. (2022) Nüfus ve Vatandaşlık Hizmetlerinde Yaşanan Dijital Dönüşüm Sürecinin Bürokrasi Üzerindeki Etkisi. Igdir University Journal of Faculty of Economics and Administrative Sciences, (8), 105-122.

Bingöl, T. Y., & Eker, H. (2022) Ergenlerde dijital oyun bağımlılığının boş zaman can sıkıntısı tarafından yordanması.

Biolcati, R., Mancini, G., & Trombini, E. (2018) Proneness to boredom and risk behaviors during adolescents' free time. Psychological reports, 121(2), 303-323.

Borges, P. M., & Gambarato, R. R. (2019) The role of beliefs and behavior on facebook: a semiotic approach to algorithms, fake news, and transmedia journalism.

Borges-Rey, E. (2019) Data journalism in Latin America: Community, development and contestation. In Data Journalism in the Global South (pp. 257-283). Palgrave Macmillan, Cham.

Bourdieu, P. (1996) Distinction: A social critique of the judgement of taste. Translated by Richard Nice. Eighth printing. Harvard university press.

Bouregh, A. S., Maniruzzaman, K. M., Abubakar, I. R., Alshihri, F. S., Alrawaf, T. I., Ahmed, S. M., & Boureggah, M. S. (2023) Investigating the prospect of e-participation in urban planning in Saudi Arabia. Cities, 134, 104186.

Bouvier, G. (2022) 'Yankı odalarından' 'kaos odalarına' MeToo Twitter

beslemesindeki söylemsel tutarlılık ve çelişki. Eleştirel Söylem Çalışmaları, 19 (2), 179-195.

Boztepe Taşkıran, H. (2019) Kamu Yönetiminde Vatandaş Katılımı ve Şeffaflığın Sağlanmasında Dijital İletişim Uygulamalarının Rolü. Amme İdaresi Dergisi, 52(1).

Boztepe, M. (2018) Yeni kamu yönetimi ve geleneksel kamu personel rejimi üzerine etkileri. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 20(3), 191-210.

Bradbury, D. (2011) Routing around censorship. Network Security, 2011(5), 5-8.

Bradshaw, S., & Howard, P. (2017) Troops, trolls and troublemakers: A global inventory of organized social media manipulation. Computational Propaganda Research Project.

Bradshaw, S., & Howard, P. N. (2019) The global disinformation order: 2019 global inventory of organised social media manipulation.

Bradshaw, S., DiResta, R., & Miller, C. (2023) Playing both sides: Russian state-backed media coverage of the# BlackLivesMatter movement. The International Journal of Press/Politics, 28(4), 791-817.

Bruce, C. (2000) Information literacy programs and research: An international review. The Australian Library Journal, 49(3), 209-218.

Bruce, C. (2003) Information literacy as a catalyst for educational change: A background paper. In International information literacy conferences and meetings (pp. 1-17). NCLIS.gov.

Buchi, M., & Hargittai, E. (2022) A need for considering digital inequality when studying social media use and well-being. Social Media+ Society, 8(1), 20563051211069125.

Buckman R. H. (2004) Building a knowledge-driven organization. McGraw-Hill.

Buğday, B, E. (2015) Bilinçli Tüketici Ölçeği geliştirme çalışması (Doktora tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Business Standard. (Jan 29 2021) Worried about power of social media companies: UN chief Guterres (accessed 09 June 2022) https://www.business-standard.com/article/technology/worried-about-power-of-social-media-companies-un-chief-guterres-121012900737_1.html

Bychawska-Siniarska, D. (2018) Avrupa İnsan Hakları Sözleşmesi Kapsamında İfade Özgürlüğünün Korunması. Çev: Av. Tuğçe Duygu Köksal. Uygulamacılar İçin El Kitabı.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022) Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.

Canclini, N. G. Néstor García Canclini (2018) Disposal and reinvention: Citizenship in an era of electronic capitalism. Open Cultural Studies, 2(1), 273-284.

Candeub, A. (2021) Bölüm 230'un Yazılı Olarak Okunması. J. İfade Özgürlüğü L., 1, 139.

Canöz, K., Berkay, İ., & Kaya, K. K. (2023) Halkla İlişkiler, Yapay Zekâ ve Hegemonya: Eleştirel Bir Değerlendirme. Karatay Sosyal Araştırmalar Dergisi, (11), 335-352.

Carrasco-Farré, C. (2022) The fingerprints of misinformation: how deceptive content differs from reliable sources in terms of cognitive effort and appeal to emotions. Humanities and Social Sciences Communications, 9(1), 1-18.

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021) Internet, social media and online hate speech. Systematic review. Aggression and violent behavior, 58, 101608.

Celeste, E. (2021) The Constitutionalisation of the digital ecosystem: Lessons from international law. Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper, (2021-16).

Celot, P. (2012) EAVI studies on media literacy in Europe. Media Studies, 3(6).

Cemiloglu, D., Almourad, M. B., McAlaney, J., & Ali, R. (2022) Combatting digital addiction: Current approaches and future directions. Technology in Society, 68, 101832.

Ceylan, T. (2011) Toplumsal Sistem Analizinde Toplumsal Statü ve Rol. Journal of Graduate School of Social Sciences, 15(1).

Chawla, A. (2021) Pegasus Spyware – 'A Privacy Killer'. Available at SSRN 3890657.

Chaykowski, K. (2018, January 11) Facebook focuses news feed on friends and family, curbing the reach of brands and media. Forbes. Retrieved from https://www.forbes.com/sites/kathleenchaykowski/2018/01/11/facebook-focuses-news-feed-onfriends-and-family-curbing-the-reach-of-brands-and-media/#6fd525555b69

Chen, C., & Ganapati, S. (2023) Do transparency mechanisms reduce government corruption? A meta-analysis. International Review of Administrative Sciences, 89(1), 257-272.

Chen, H. C., Wang, J. Y., Lin, Y. L., & Yang, S. Y. (2020) Association of internet addiction with family functionality, depression, self-efficacy and self-esteem among early adolescents. International journal of environmental research and public health, 17(23), 8820.

Chen, L. L., Mirpuri, S., Rao, N., & Law, N. (2021) Conceptualization and measurement of digital citizenship across disciplines. Educational Research Review, 33, 100379.

Chen, S. (2022) "Chinese Researchers Say They've Developed an AI Text

Censor That is 91% Accurate," The Star, Apr. 15, 2022, https://www.thestar.com.my/tech/tech-news/2021/04/15/chinese-researchers-say-theyve-developed-an-ai-text-censor-that-is-91-accurate

Cherepanov, A., & Lipovsky, R. (2016) Blackenergy–what we really know about the notorious cyber attacks. Virus Bulletin October, 541.

China 2021 human rights report. Erişim tarihi: 06.06.2024. https://www.state.gov/wp-content/uploads/2022/03/3136152_CHINA-2021-HUMAN-RIGHTS-REPORT.pdf

Chiru, M., & Enyedi, Z. (2022) Who wants technocrats? A comparative study of citizen attitudes in nine young and consolidated democracies. The British Journal of Politics and International Relations, 24(1), 95-112.

Christensen, Z. (2023, February 28) Economic poverty trends: global, regional and national. Development initiatives. https://tls.tc/MtaOo

Ciolan, I. M. (2014) Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. Revista de Administratie Publica si Politici Sociale, 12(1), 40.

Civelek, M. A., (2005) Ulus Devlet. Bitti" Diyenlere Hatırlatmalar", Gelenek Dergisi, (85).

Claussen, V. (2018) Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation. Media Laws, 3(3), 110-136.

Clercq, D. D., Azeem, M. U. ve Haq, I. U. (2021) But they promised! How psychological contracts influence the impact of felt violations on jobrelated anxiety and performance. Personnel Review, 50(2), 648-666. https://doi.org/10.1108/PR-07-2019-0388

Cocito, C., & De Hert, P. (2023) The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights). Computer Law & Security Review, 50, 105846.

Cohen, J. E. (2017) Examined lives: Informational privacy and the subject as

object. In Law and Society Approaches to Cyberspace (pp. 473-538). Routledge.

Collins, A. M., Warburton W. A., Bussey, K., Sweller, N. (2023) Factor Structure and Psychometric Properties of the Digital Communication Empathy Scale (DCES), International Journal of Human-Computer Studies, 103183.

Collins, R. (1988) Theoretical Sociology. Harcourt Brace Jovanovich Publishers.

Conner, T. S., DeYoung, C. G., & Silvia, P. J. (2018) Everyday creative activity as a path to flourishing. The Journal of Positive Psychology, 13(2), 181-189.

Cooke, S. (2021) Cosmopolitan disobedience. Journal of International Political Theory, 17(3), 222-239.

Corrêa, N. K., Galvão, C., Santos, J. W., Del Pino, C., Pinto, E. P., Barbosa, C., ... & de Oliveira, N. (2023) Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. Patterns, 4(10).

Couldry, N., & Mejias, U. A. (2019) Data colonialism: Rethinking big data's relation to the contemporary subject. Television & New Media, 20(4), 336-349.

Couldry, N., & Mejias, U. A. (2020) The costs of connection: How data are colonizing human life and appropriating it for capitalism.

Couldry, N., & Mejias, U. A. (2023) The decolonial turn in data and technology research: what is at stake and where is it heading? Information, Communication & Society, 26(4), 786-802.

Council of Europe (2023) Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, December 18, 2023, https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043

Creswell, J. W., & Poth, C. N. (2016) Qualitative inquiry and research design: Choosing among five approaches. 4. Edition. Sage publications.

CRS Report (October 16, 2023) War Crimes in Ukraine. Congressional Research Service. R47762 https://crsreports.congress.gov

Csernatoni, R. (2024) Charting the Geopolitics and European Governance of Artificial Intelligence.

Custers, B. (2022) New digital rights: Imagining additional fundamental rights for the digital era. Computer Law & Security Review, 44, 105636.

Cüceloğlu, D. (2018) Öğretmenim bir bakar mısın? Öğretmen'in gücü üzerine. Final Kültür Sanat Yayınları.

Çağlar, N., & Ayber, M. (2022) Uluslararası Başarılarda Siyasi Aktörlerin Tebrik Mesajlarına Yapılan Şiddet İçerikli Paylaşımlar Üzerine Bir İnceleme: Tokyo 2020 Örneği. İletişim ve Toplum Araştırmaları Dergisi, 2(2), 171-191.

Çakmak, Z., & Aslan, S. (2018) An investigation of digital citizens' behaviours of social science teachers for some variables. Adıyaman University Journal of Educational Sciences, 8(1), 72-99.

Çaldağ, M. T., & Gökalp, E. (2023) Understanding barriers affecting the adoption and usage of open access data in the context of organizations. Data and Information Management, 100049.

Çalıkoğlu, M. C. (2024) Kolektif Siber Güvenliğin Önemi ve Türk Devletler Teşkilatı: Kolektif Siber Güvenliğin Önemi ve Türk Devletler Teşkilatı. Kuantum Teknolojileri ve Enformatik Araştırmaları Dergisi, 2(1), 1-13.

Çapar, F., & Vural, Ö. F. (2013) Obstacle to e-government: Digital division E-devletleşme önündeki engel: Dijital eşitsizlik. Journal of Human Sciences, 10(1), 1674-1692.

Çatlı, M., & Keskin, S. İnsan haklarının değişime açık konusu: dijital dünyada

(2021) vatandaşlık kavramı üzerine bir inceleme. Ombudsman Akademik, 7(14), 199-229.

Çelebican, Ö. (1993: 299-300) Roma egemenliği: yurttaşlık ve kölelik. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 43(1). https://www.degruyter.com/document/doi/10.1515/culture-2018-0025/html

Çelik, S., & Çeliktaş, B. (2018) Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar. CyberPolitik Journal, 3(5), 105-132.

Çiftçi, N. (2023) Yönetişim ve Dijitalleşme (Doctoral dissertation, Marmara Universitesi, Turkey).

Çildan, C., Ertemiz, M., Tumuçin, H. K., Küçük, E., & Albayrak, D. (2012) Sosyal medyanın politik katılım ve hareketlerdeki rolü. Akademik Bilişim, 3(1), 1-9.

Çilingirtürk, A. M., & Demirci, V. G. (2020) Sosyal Ağ Analizi. Bursa: EKİN.

Dağ, Ü. (2020) George Orwell'ın 1984 ve Selim Erdoğan'ın İkibinseksendört Bir Dijital Kara Ütopya eserlerinde Distopyanın Panoraması. Humanıtas-Uluslararası Sosyal Bilimler Dergisi, 8(16), 107-124.

Daigle, B., & Khan, M. (2022) The Changing Tides of Data Protection Regulation and Enforcement in Europe. Office of Industries, US International Trade Commission.

Dalton, J. C., & Crosby, P. C. (2013) Digital identity: How social media are influencing student learning and development in college. Journal of College and Character, 14(1), 1-4.

Dame Adjin-Tettey, T. (2022) Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. Cogent arts & humanities, 9(1), 2037229.

Danziger, R. (2020) The pragmatics of flattery: The strategic use of solidarity-

oriented actions. Journal of Pragmatics, 170, 413-425.

Danziger, R. (2021) The democratic king: The role of ritualized flattery in political discourse. Discourse & Society, 32(6), 645-665.

Davidson, E., Wessel, L., Winter, J. S., & Winter, S. (2023) Future directions for scholarship on data governance, digital innovation, and grand challenges. Information and Organization, 33(1), 100454.

Davis, M. H. (1996) Empathy: A social psychological approach. Madison, WI: Brown & Benchmark.

Davison, R. M., Ou, C. X., & Martinsons, M. G. (2018) Interpersonal knowledge exchange in China: The impact of guanxi and social media. Information & Management, 55(2), 224-234.

De Mesquita, B. B., & Smith, A. (2010) Leader survival, revolutions, and the nature of government finance. American journal of political science, 54(4), 936-950.

De Renzio, P., & Wehner, J. (2017) The impacts of fiscal openness. The World Bank Research Observer, 32(2), 185-210.

De Vos, M., Ishmaev, G., & Pouwelse, J. (2024) DeScan: Censorship-resistant indexing and search for Web3. Future Generation Computer Systems, 152, 257-272.

Debs, A. (2010) Economic theories of dictatorship. The Economics of Peace and Security Journal, 5(1).

Dede, A. (2024) Dijital İletişim, Dijital Vatandaşlık, Dijital Yönetişim ve CİMER. Abant Sosyal Bilimler Dergisi, 24(1), 355-365. doi: 10.11616/asbi.1396928

Değer, K. G. (2022) Sosyal medyada aşı distopyası ve yankı odaları. İletişim ve Medya Alanında Uluslararası Araştırmalar X, 31.

De-Lima-Santos, M. F., & Mesquita, L. (2021) The Strategic Value of Data Journalism. In Journalism, Data and Technology in Latin America (pp. 97-136). Palgrave Macmillan, Cham.

Demirel, S., Kahraman, E., & Gündüz, U. (2024) A text mining analysis of the change in status of the Hagia Sophia on Twitter: the political discourse and its reflections on the public opinion. Atlantic Journal of Communication, 32(1), 63-90.

Derdiyok, T., Doğru, Ç., & Serkan, Ü. N. A. L. (2020) Dijital çağda entelektüel sermayenin dönüşümü ve şirketlerin rekabet güçlerine etkileri. Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 9(18), 7-26.

Dezuanni, M., Foth, M., Mallan, K., & Hughes, H. (Eds.). (2017) Digital participation through social living labs: Valuing local knowledge, enhancing engagement. Chandos Publishing.

Diniz, E. H., Santos, T. R. R., & Cunha, M. A. (2022) Measuring the Grand Challenge of the Digital Transformation of Society: Practices for Operationalizing Robust Action Strategies. IEEE Transactions on Engineering Management, 70(3), 1076-1088.

Dolgun, U. (2004) Gözetim toplumunun yükselişi: enformasyon toplumundan gözetim toplumuna. Yönetim Bilimleri Dergisi, 2(1), 55-74.

Dolgun, U. (2015) Şeffaf hapishane yahut gözetim toplumu: küreselleşen dünyada gözetim, toplumsal denetim ve iktidar ilişkileri. Ötüken.

Donnelly, D. (2022) China social credit system explained what is it and how does it work? Horizons. Oğuz, M. C., (2023). Authoritarianism extending to diaspora: transnational repression policies of authoritarian regimes and the İranian example.

Dossier Center. (2023, March 18) Кибервойска Пригожина (Prigozhin's cyber troops: How the IT infrastructure of Wagner, Troll Factory and Concorde works). Dossier Center. https://dossiercenter.appspot.com/prig-it/

Doyle, C. S. (1994) Information literacy in an information society: A concept for the information age. Diane Publishing.

Doyle, W. (2023) Sufism, Attention and Digital Colonization. Tasavvuf Araştırmaları Enstitüsü Dergisi, 2(1), 11-25.

Dönmez, E. & Torun, N. K. (2022) Siber Cehennem: Sağlık Sektörü Üzerine Bir Değerlendirme. Ö. K. Tüfekci & L. Akbaş (Ed.), Sosyal Bilimler Araştırmaları: Çıkarımlar, Bileşenler, Çözümlemeler (s. 1-14). Klaipeda: SRA Academic Publishing.

Duan, Z., Li, J., Lukito, J., Yang, K. C., Chen, F., Shah, D. V., & Yang, S. (2022) Algorithmic agents in the hybrid media system: Social bots, selective amplification, and partisan news about COVID-19. Human Communication Research, 48(3), 516-542.

Duman, M. Ç. (2022, June) Toplum 5.0: insan odaklı dijital dönüşüm. In Journal of Social Policy Conferences (No. 82, pp. 309-336). Istanbul University.

Duo, W., Zhou, M., & Abusorrah, A. (2022) A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), 784-800.

Echendu, A. J. (2021) Combatting Chemical Weapon Disinformation. Academia Letters, 2.

EDRİ. (2020) The EU's attempt to regulate Big Tech: What it brings and what is missing? By EDRİ December 18, 2020. https://edri.org/our-work/eu-attempt-to-regulate-big-tech/ erişim tarihi; 25.03.2034.

Engels, F., & Marx, K. (2013) Alman ideolojisi, çev. Tonguç Ok- Olcay Geridönmez. Evrensel Basım Yayın.

Epifanova, A., & Dietrich, P. (2022) Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World.

Erdem, F. H. (2012) Anayasal vatandaşlık ve yeni anayasa. Liberal Düşünce Dergisi, (51), 49-56. https://dergipark.org.tr/en/download/article-file/790764

Eren, A. (2005) Korku kültürü, değerler kültürü ve şiddet. Sosyal Politika Çalışmaları Dergisi, 8(8).

Eren, A. (2022) Michel Foucault'nun Çalışmalarında Panoptikon,

Kapatılma ve Okul Kurumu. Eğitim Bilim Toplum Dergisi, 20(79), 64-82.

Erkmen, B. (2013) İşkoliklik ile esenlik arasındaki ilişki (Doctoral dissertation, Marmara Universitesi), Türkiye.

Ermiş, U. (2018) Bir güvenlik sorunu olarak siber uzay. Türk Asya Stratejik Araştırmalar Merkezi.

Eroğul, C. (1974) Marksist Devlet Kuramı Hakkında Bir Not.

Ertong, G. (2011) Niklas Luhmann'ın Sosyal Sistemler Kuramı ve Güven Tartışmaları Bağlamında Sağlık Sistemi (Health System in the Context of Niklas Luhmann's Social Systems Theory and Trust Discussions). Available at SSRN 3285137.

Eser Akkuş, D. (2017) Türkiye'deki azınlıkların dijital vatandaşlık pratikleri. Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

European Commission (2021) EU-US Trade and Technology Council, 15 June 2021 in Brussels. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

European Commission (2023) European Digital Rights and Principles. Last update: 5 December 2023.

European Commission. (2021) 2030 digital compass: the European way for the digital decade. COM (2021) 118 final.

Ezemenaka, E. (2013) The usage and impact of internet enabled phones on academic concentration among students of tertiary institutions: A study of University of Ibadan, Nigeria. International Journal of Education and Development using ICT, 9(3).

Fayyaz, Z., Ebrahimian, M., Nawara, D., Ibrahim, A., & Kashef, R. (2020) Recommendation systems: Algorithms, challenges, metrics, and business opportunities. applied sciences, 10(21), 7748.

Fedasiuk, R. (12 Oca 2021) Buying Silence: The Price of Internet Censorship in China. Publication: China Brief Volume: 21 Issue: 1.

https://jamestown.org/wp-content/uploads/2021/01/Read-the-1-13-2021-Issue-in-PDF.pdf

Fekete, L. (2023) Civilisational racism, ethnonationalism and the clash of imperialisms in Ukraine. Race & Class, 64(4), 3-26.

Feng, G. C., & Guo, S. Z. (2013) Tracing the route of China's Internet censorship: An empirical study. Telematics and Informatics, 30(4), 335-345.

Fernandes, G., Yunes, M. A. M., & Finkler, L. (2020) The social networks of adolescent victims of domestic violence and bullying. Paidéia (Ribeirão Preto), 30, e3007.

Ferrara, E., Chang, H., Chen, E., Muric, G., & Patel, J. (2020) Characterizing social media manipulation in the 2020 US presidential election. First Monday.

Fichman, P., & Akter, S. (2023) Trolling asymmetry toward Republicans and Democrats and the shift from foreign to domestic trolling. Telematics and Informatics, 82, 101998.

Fiğan, M., Özdemir, Y. D., Ağaoğlu, E., Özdemir, M. B., Önen, N., & Derneği, A. B. (2020) Dijital Kültür, Dijital Eşitsizlikler ve Yaşlanma.

Fino, A. (2020) Defining hate speech: a seemingly elusive task. Journal of international criminal justice, 18(1), 31-57.

Fleming, M. (2005) Ergen Özerkliği: Erken ve Geç Ergenlik Döneminde Arzu, Başarı ve İtaatsizlik Eden Ebeveynler. Avustralya Eğitim ve Gelişim Psikolojisi Dergisi, 5, 1-16.

Fokin, A. (2016) Internet trolling as a tool of hybrid warfare: the case of latvia.

Foucoult, M. (1975) Discipline and punish. A. Sheridan, Tr., Paris, FR, Gallimard.

Fraillon, J., Ainley, J., Schulz, W., Friedman, T., Preparing for life in a digital world: IEA international computer and information literacy study 2018 international

& Duckworth, D. (2020) report (p. 297). Springer Nature.

Freedom House (2020) Freedom on the Net 2020: The Pandemic's Digital Shadow, Washington, DC

Friesem, Y. (2016) Empathy for the digital age: Using video production to enhance social, emotional, and cognitive skills. In Emotions, technology, and behaviors (pp. 21-45). Academic Press.

Fuchs, C. (2009) The role of income inequality in a multivariate cross-national analysis of the digital divide. Social science computer review, 27(1), 41-58.

Fuchs, C. (2016) Sosyal Medya: Eleştirel Bir Giriş. Çev: Diyar Saraçoğlu ve İlker Kalaycı. Ankara: Nota Bene Yayınları

Gambrell, J. (9 February 2024) Meta removes Instagram and Facebook accounts for Iran's Supreme Leader Ayatollah Ali Khamenei. The Associated Press (AP). Erişim tarihi. 17.03.2024. https://apnews.com/article/iran-meta-supreme-leader-ayatollah-ali-khamenei-cb6a0551528903b6b1531afe39ee79cb

Gan, N., Hu, C. and Watson, I. (2020) 'Beijing tightens grip over coronavirus research, amid US-China row on virus origin', CNN, 16 April 2020, https://edition.cnn.com/2020/04/12/asia/china-coronavirus-researchrestrictions-intl-hnk/index.html.

Garrett, D. E. (1987) The effectiveness of marketing policy boycotts: Environmental opposition to marketing. Journal of marketing, 51(2), 46-57.

Gcaza, N., & Von Solms, R. (2017) Cybersecurity culture: An ill-defined problem. In Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10 (pp. 98-109). Springer International Publishing.

Gebhardt, E., Thomson, S., Ainley, J., & Hillman, K. (2019) Introduction to gender differences in computer and information literacy. Gender differences in computer and information literacy, 1-12.

Girish, G. J., Williams, C. B., & Yates, D. J. (2014) Predictors of on-line services and e-participation: A cross-national comparison. Government Information Quarterly, 31(4), 526-533.

Glaser, A. (2018) Gençlerin özgürleşmesi (Doktora tezi, Chapel Hill'deki Kuzey Carolina Üniversitesi).

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., ... & Zanin, C. (2023) Contested spatialities of digital sovereignty. Geopolitics, 28(2), 919-958.

Global Network Initiative (GNI) Empower Policy. https://globalnetworkinitiative.org/what-we-do/empower-policy/

Goffman, E., & Cezar, B. (2009) Günlük yaşamda benliğin sunumu. İstanbul: Metis.

Göçoğlu, V. (2020) Kamu hizmetlerinin sunumunda dijital dönüşüm: Nesnelerin interneti üzerine bir inceleme. MANAS Sosyal Araştırmalar Dergisi, 9(1), 615-628.

Gökçınar, B. (2022) Sosyal bilgiler ders kitaplarının temel vatandaşlık değerleri ve becerileri açısından değerlendirilmesi (Doctoral dissertation, Necmettin Erbakan University (Turkey).

Gönç Şavran, T., Suğur, S., Koçak Turhanoğlu, F. A., Gökalp, E., & Karkıner, N. (2019) Modern Sosyoloji Tarihi. Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayını. Yayın, (2595).

Gracia Calandín, J. (2018) El desafío ético de la Educación. Madrid: Dykinson.

Guarte, J. M., & Barrios, E. B. (2006) Estimation under purposive sampling. Communications in Statistics-Simulation and Computation, 35(2), 277-284.

Gümüş, S. (2023) Sosyal Medyanın Kamusal Alan Temsiliyeti Üzerine Bir Tartışma. 4. Boyut Medya ve Kültürel Çalışmalar Dergisi, (22), 21-48.

Gündüz, U. (2018) Osmanlı'dan günümüze basın ve modernleşme. İmge Kitabevi.

Gündüz, U. (2020) Küresel Pandemi Sürecinde Dijitalleşme, Sosyal Medya ve

Gelecek Öngörüleri. İletişim Araştırmaları ve Film Çözümlemeleri II Dijital Çağda Medya (ss.9-19), Konya: Eğitim Kitabevi.

Güngör, S. (2023) Denetimli Çevrimiçi Sınav Uygulamaları İçin Web Tabanlı Bir Kontrol Sistemi: "ERÜ İİBF Online İşlemler Sistemi" ÖRNEĞİ. Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, (64), 53-61.

Gürgen, H. (1990) Propaganda. Kurgu, 8(2), 135-157.

Gwagwa, A., Kazim, E., & Hilliard, A. (2022) The role of the African value of Ubuntu in global AI inclusion discourse: A normative ethics perspective. Patterns, 3(4).

Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2022) Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. British Journal of Management, 33(3), 1238-1253

Hammersley, R. (2015) Revolutionary moments: reading revolutionary texts (p. 224). Bloomsbury Academic.

Harari, Y. N. (2016) Homo deus: Yarının kısa bir tarihi. Kolektif Kitap. İstanbul.

Harrijvan, M., & Weerdesteijn, M. (2020) To appease or to repress: how dictators use economic dynamics to increase their regime longevity. Crime, Law and Social Change, 74, 315-338.

Hasanzadeh, S., & Shakeebaee, G. (2023) Use of cultulings in business communication: A case of flattery. Journal of Business, Communication & Technology, 2(1), 50-63.

Hatlevik, O. E., Ottestad, G., & Throndsen, I. (2015) Predictors of digital competence in 7th grade: a multilevel analysis. Journal of Computer Assisted Learning, 31(3), 220-231.

Hawk, S. T., Fischer, A. H., & Van Kleef, G. A. (2011) Taking your place or matching your face: Two paths to empathic embarrassment. Emotion, 11(3), 502.

Hayat, A. A., Kojuri, J., & Mitra Amini, M. D. (2020) Academic procrastination of medical students: The role of Internet addiction. Journal of advances in medical education & professionalism, 8(2), 83

Heeks, R. (2022) Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South. Information Technology for Development, 28(4), 688-704.

Henry, N., Vasil, S., & Witt, A. (2022) Digital citizenship in a global society: a feminist approach. Feminist Media Studies, 22(8), 1972-1989.

Hermida, A. (2017) Herkese Söyle. İstanbul: EpsilonYayınevi

Hinds, J., Williams, E. J., & Joinson, A. N. (2020) "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 143, 102498.

Hoffman, M. L. (2001) Empathy and moral development: Implications for caring and justice. Cambridge University Press.

Howard, P., Lin, F., & Tuzov, V. (2023) Computational propaganda: Concepts, methods, and challenges. Communication and the Public, 8(2), 47-53.

Hsiao, SC ve Kao, DY (2018, Şubat) WannaCry fidye yazılımının statik analizi. 2018'de 20. uluslararası ileri iletişim teknolojisi konferansı (ICACT) (s. 153-158). IEEE

Huang, H. (2018) The pathology of hard propaganda. The Journal of Politics, 80(3), 1034-1038.

Hüsnüoğlu, N., & Öztürk, L. (2017) Dijital bölünme: Nedenleri ve türleri. Giresun Üniversitesi İktisadi ve İdari Bilimler Dergisi, 3(5), 6-21.

Hyliaka, S. (2021) Human rights in the digital age: Challenges, threats and prospects. Науковий юридичний журнал, 28(1), 16.

Iganski, P. (2008) 'Hate crime'and the city. Policy Press.

INSIGHT, C. (2021) Colonial pipeline: the darkside strikes. Congressional research service.

Isopahkala-Bouret, U., Siivonen, P., & Haltia, N. (2023) 'Some people may feel socially excluded and distressed': finnish business students' participation in extracurricular activities and the accumulation of cultural capital. Journal

of Education and Work, 36(1), 52-64.

Işikli, Ş. (2015) Digital citizenship: An actual contribution to theory of participatory democracy. AJIT-e: Academic Journal of Information Technology, 6(18), 21-37.

İnceoğlu, Y. (2020) Covid-19 pandemisi ve medya. TTB Covid-19 pandemisi, 6, 632-643.

İyigüngör, T. (2022) Ekonomik ve Toplumsal Dijitalleşme: Endüstri 4.0'dan Toplum 5.0'a. Smac Journal, 47-59.

Jack, C. (2017) Lexicon of lies: Terms for problematic information.

Jannusch, T., David-Spickermann, F., Shannon, D., Ressel, J., Völler, M., Murphy, F., ... & Mullins, M. (2021) Surveillance and privacy–Beyond the panopticon. An exploration of 720-degree observation in level 3 and 4 vehicle automation. Technology in Society, 66, 101667.

Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015) Significance and challenges of big data research. Big data research, 2(2), 59-64.

Jonas, H. (1995) El principio de responsabilidad. Ensayo de una ética para la civilización tecnológica. Barcelona: Herder.

Jones, T., Payton, M., & Feather, B. (2019) Source: Leaked documents show the US government tracking journalists and immigration advocates through a secret Database. NBC 7 Investigates.

Kalaycı, N. (2023) Dijitalleşememe ve Dijital Eşitsizlik. Scientific Journal of Space Management and Space Economy, 2(1), 43-52.

Kamil, C. (2020) Tirana Direnmek: Salisburyli John ve Thomas Aquinas Karşılaştırılması. Akademik İzdüşüm Dergisi, 5(2), 281-294.

Kanten, P., Pazarcık, Y., Durmaz, M. G., & Arda, B. (2022) İşyerinde Sosyal Cesaretin Prososyal Ses Çıkarma Davranışı Üzerindeki Etkisinde Proaktif Kişiliğin Aracılık Rolünün Belirlenmesi. İşletme Araştırmaları Dergisi, 14(4), 2867-2877.

Kara, T., & Atasoy, E. (2019) Sosyal Bilgiler Öğretim Programı ve Ders Kitaplarının (2018) Dijital Vatandaşlık Kavramı ve Alt Boyutları

Bağlamında İncelenmesi. Balikesir University Journal of Social Sciences Institute, 22(41).

Karaboğa, E. N. C. (2022) Bilinçli tüketici kavramına ilişkin algıların değerlendirilmesi: Bir metafor analizi çalışması. Business & Management Studies: An International Journal, 10(1), 412-428.

Karaduman, S. (2019) Yeni medya okuryazarlığı: Yeni beceriler/olanaklar/riskler. Erciyes İletişim Dergisi, 6(1), 683-700.

Karakuyu, A. (2023) Dijital vatandaşlık öğretim programının tasarlanması, uygulanması ve değerlendirilmesi. Doktora tezi. Afyon Kocatepe Üniversitesi.

Karaoğlu, G. (2022) Dijital Okuryazarlık. Karaoğlu, G. (Edit.) Efe Akademik Yayıncılık.

Karasoy, H. A & Gezici, H. S. (2023) Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekânın Siber Güvenlikteki Önemi. Uluslararası Yönetim Akademisi Dergisi, 6(1), 173-188.

Kaster, S. D., & Ensign, P. C. (2023) Privatized espionage: NSO Group Technologies and its Pegasus spyware. Thunderbird International Business Review, 65(3), 355-364.

Katibah, L. (2023) The Politics of Pegasus Spyware: Examining the Impact of Surveillance on Journalism.

Katyal, N. K. (2001) Criminal law in cyberspace. University of Pennsylvania Law Review, 149(4), 1003-1114.

Kaur, S. (2021) The untangled view of digital citizenship: A bibliometric analysis. Journal of General Management Research, 8(2).

Kaypak, Ş., Bimay, M., & Yılmaz, V. (2017) Dijital çağda kamu yönetimi ve etik. DOI: 10.26449/sssj.128

Ke, T. T., & Sudhir, K. (2023) Privacy rights and data security: GDPR and personal data markets. Management Science, 69(8), 4389-4412.

Keller, T. R., & Klinger, U. (2019) Social bots in election campaigns: Theoretical, empirical, and methodological implications. Political Communication, 36(1), 171-189.

Kermani, H., Bayat Makou, A., Tafreshi, A., Mohamad Ghodsi, A., & Ataee, H. (2023) Bots Versus Humans: Discursive Activism During the Pandemic in the Iranian Twittersphere. Social Media+ Society, 9(4), 20563051231216927.

Khan A. K. (25 Mayıs 2023) The Power of Empathy: Building Connections in the Digital World. Moderndiplomacy. https://moderndiplomacy.eu/2023/05/25/the-power-of-empathy-building-connections-in-the-digital-world/

Khan, S., & Abbas, M. (2023) Interactive effects of consumers' ethical beliefs and authenticity on ethical consumption and pro-environmental behaviors. Journal of Retailing and Consumer Services, 71, 103226.

Kılıç, S. (2011) Bir hizmet işletmesinde müşteri memnuniyet sürecinin dinamik bir analizi: Karar destek sistemi uygulaması (Master's thesis, Sosyal Bilimler Enstitüsü).

Kıran, Ö. (2021) Dijital Ortamlarda Benlik Sunumu ve Kimlik İnşası. İnsan ve Toplum Bilimleri Araştırmaları Dergisi, 10(3), 2038-2065.

Kiçir, İ., & Cengiz, A. (2022) Yeni toplumsal hareketler bağlamında siyasal tüketicilik. SDÜ İfade, 4(1), 95-116.

Kim, S., & Lee, J. (2012) E-participation, transparency, and trust in local government. Public administration review, 72(6), 819-828.

King, G., Pan, J., & Roberts, M. E. (2017) How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. American political science review, 111(3), 484-501.

King, Gary, Jennifer Pan, and Margaret E. Roberts. (2017) "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." American Political Science Review 111 (3): 484–501.

Kişman, Z. A., & Güleç, Ö. (2021) Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. Akademik Açı, 1(1), 127-154.

Koçoğlu, Y. (2014) Barışın aracı olarak tarih ders kitapları: Türk-Yunan tarih ders kitapları örneklemi (Master's thesis, Eğitim Bilimleri

Enstitüsü).

Korkmaz, İ. (2013) Facebook ve mahremiyet: Görmek ve gözetle (n) mek. Yalova Sosyal Bilimler Dergisi, 3(5).

Korkut, L. (2014) Siyasi kimlik olarak vatandaşlık: Türkiye'de ve dünya devletlerinde anayasal vatandaşlık tanımları. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 1(2), 5-42.

Kovanic, M., & Spac, S. (2022) Conceptions of privacy in the digital era: Perceptions of slovak citizens. Surveillance & Society, 20(2), 186-201.

Kuhn, T. (1962) The Structure of Scientific Revolutions. Chicago: University of Chicago Press

Kurnaz, A. (2022) Dijital Siyasetin Yükselişi ve Yapay Zekâ (The Rise of Digital Politics and Artificial Intelligence). Kamu Yönetimi ve Uluslararası İlişkiler Bağlamında Yapay Zekâ Tartışmaları, Ekin Yayınevi.

Kuş, O. (2021) Algoritmaların gölgesinde toplum ve iletişim.

Kutlu, A. (2019). Suskunluk sarmali 2.0: türkiye'de facebook kullanimi üzerine bir araştirma. TESAM Akademi Dergisi, 6(1), 43-75.

Küçükbezirci, Y. (2023) Dijital Çağın Vebası Siber Suçlar. Çizgi Kitabevi Yayınları (e-kitap).

Kütükoğlu, E. (2019) Sosyal medyada çocuk mahremiyeti: Annelerin mahremiyet algısı üzerine bir araştırma.

Kwet, M. (2019) Digital colonialism: US empire and the new imperialism in the Global South. Race & Class, 60(4), 3-26.

Laatikainen, G., Li, M., & Abrahamsson, P. (2023) A system-based view of blockchain governance. Information and Software Technology, 157, 107149.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021) Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

Laudon, K. C., & Laudon, J. P. (2012) Management Information Systems, Managing Digital Companies, Book 1.

Leaning, M. (2019) An approach to digital literacy through the integration of media and information literacy. Media and Communication, 7(2), 4-13.

Ledford, J. A. (2022) The 1% Rule of the Internet: How to be a Content Creator. Medium. Feb 22, 2022. https://medium.com/illumination/the-1-rule-of-the-internet-how-to-be-a-content-creator-d51698247bbe

Lemke, T., & Habegger, M. W. (2022) Foreign interference and social media networks: A relational approach to studying contemporary Russian disinformation. Journal of Global Security Studies, 7(2), ogac004.

Lennon, M., Kirsch, I., Von Davier, M., Wagner, M., & Yamamoto, K. (2003) Feasibility Study for the PISA ICT Literacy Assessment: Report to Network A. Educational Testing Service.

Lenz, T. (2017) The Rising Authority of International Organisations.

Leveringhaus, A. (2016) Ethics and autonomous weapons. Springer.

Li, G. (2023) Internet censorship in China: A functioning digital panopticon. In Communications in Contemporary China (pp. 11-26). Routledge.

Li, Y., & Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Li, YY, Sun, Y., Meng, SQ, Bao, YP, Cheng, JL, Chang, XW, ... & Shi, J. (2021) COVID-19 sırasında genel nüfusta internet bağımlılığı artıyor: Çin'den kanıtlar. Amerikan bağımlılık dergisi 30 (4), 389-397.

Lin, Y. (2024) More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance. Columbia Journal of Transnational Law, 62(1).

| | |
|---|---|
| Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019) | "The Russıans Are Hackıng My Braın!" investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign. Computers in Human Behavior, 99, 292-300. |
| Linvill, D. L., Warren, P. L., & Moore, A. E. (2022) | Talking to trolls—how users respond to a coordinated information operation and why they're so supportive. Journal of Computer-Mediated Communication, 27(1), zmab022. |
| Lipset, S. M. (1959) | Some social requisites of democracy: Economic development and political legitimacy1. American political science review, 53(1), 69-105. |
| List, A., Brante, E. W., & Klee, H. L. (2020) | A framework of pre-service teachers' conceptions about digital literacy: Comparing the United States and Sweden. Computers & Education, 148, 103788. |
| Liu, M., & Lu, Y. (2024) | Blame-avoiding strategies for a digital scandal: A critical discourse analysis of Mark Zuckerberg's Congressional hearings. Pragmatics and Society, 15(3), 471-494. |
| Livingstone, S., Van Couvering, E., Thumin, N., Coiro, J., Knobel, M., Lankshear, C., & Leu, D. (2008) | Converging traditions of research on media and information literacies. Handbook of research on new literacies, 103-132. |
| Luhmann, N. (1995) | Social systems. stanford university Press. |
| Lumineau, F., Wang, W., & Schilke, O. (2021) | Blockchain governance—A new way of organizing collaborations? Organization Science, 32(2), 500-521. |
| Lyon, D. (2007) | Surveillance Studies: An Overview. Cambridge: Polity Press |
| MacQueen, N. (2014) | Colonialism. Routledge. |
| Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019) | The future digital work force: robotic process automation (RPA). JISTEM-Journal of Information Systems and Technology Management, 16. |

Mahmut, M. (2023) Sosyal Kimlik Teorisi ve Göçmen Kimliğinin Ötekileştirilmesi Süreci: Stereotipleştirmeye Yönelik Psikopolitik Bir Analiz. Akademik İncelemeler Dergisi, 18(2), 470-489.

Mardan, M. (2020) Rus üslerine ev sahipliği yapan ülkelerdeki krizlere Rusya'nın askeri müdahaleleri. Güvenlik Çalışmaları Dergisi, 22(1), 108-128.

Martin, F., Gezer, T., & Wang, C. (2019) Educators' perceptions of student digital citizenship practices. Computers in the Schools, 36(4), 238-254.

Martino, G. D. S., Cresci, S., Barrón-Cedeño, A., Yu, S., Di Pietro, R., & Nakov, P. (2020) A survey on computational propaganda detection. arXiv preprint arXiv:2007.08024.

Maslej, N., Fattorini, L., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., ... & Perrault, R. (2023) Artificial intelligence index report 2023. arXiv preprint arXiv:2310.03715.

Matias, G. (2016) Citizenship as a Human right. Editor (s)(if applicable) and the Author (s).

Matsakis, L. (2020) 'How WeChat Censored the Coronavirus Pandemic', Wired, 27 August 2020, www.wired.com/story/wechat-chinese-internet-censorship-coronavirus.

Maxwell, J. A. (2012) Qualitative research design: An interactive approach. Sage publications.

Mbinjama-Gamatham, A., & Olivier, B. (2020). 'Dark technology', aggressiveness and the question of cyber-ethics. Acta Academica, 52(1), 99-120.

McCosker, A., Vivienne, S., & Johns, A. (Eds.). (2016) Negotiating digital citizenship: Control, contest and culture. Rowman & Littlefield

McFaul, M. (2019) Securing American Elections.

McLeod, J. D. (2013) Social stratification and inequality. Handbook of the sociology of mental health, 229-253.

McLeod, S. (2007) Maslow's hierarchy of needs. Simply psychology, 1(1-18).

Medeni, T. D., Soylu, D., Andekina, R., & Medeni, İ. T. (2020) Abay-lnspired Refractive Amphoras Against Echo Chambers. Türk Kütüphaneciliği, 34(3), 536-547.

Menaldo, V. ve Wittstock, N. (2021) ABD'den Çin'e teknoloji transferi Amerikan firmalarına, çalışanlarına ve tüketicilerine zarar verir mi? Tarihsel ve analitik bir araştırma. Ekonomik ve Siyasi Çalışmalar, 9 (4), 417-446.

Merriam, S. B., & Grenier, R. S. (Eds.). (2019) Qualitative research in practice: Examples for discussion and analysis. John Wiley & Sons.

Micheletti, M., & Boström, M. (2014) Political consumerism: consumer choice, information and labeling.

Mihr, A. (2022) The System of Glocal Governance. In: Glocal Governance. SpringerBriefs in Political Science. Springer, Cham. https://doi.org/10.1007/978-3-031-02108-4_5

Milgram, S. (1963) Behavioral study of obedience. The Journal of abnormal and social psychology, 67(4), 371-378.

Miller, J. A., Caldwell, L. L., Weybright, E. H., Smith, E. A., Vergnani, T., & Wegner, L. (2014) Was Bob Seger right? Relation between boredom in leisure and [risky] sex. Leisure Sciences, 36(1), 52-67.

Miller, M. L., & Vaccari, C. (2020) Digital threats to democracy: Comparative lessons and possible remedies. The International Journal of Press/Politics, 25(3), 333-356.

Moores, E., Summers, R. J., Horton, M., Woodfield, L., Evaluation of access and participation plans: Understanding what works. In Frontiers in Education (Vol. 8, p. 6).

Austen, L., & Crockford, J. (2023, January) Frontiers.

Moreland-Capuia, A. (2021) The Role of Fear in Politics, Politicians, Government, and Society. In The Trauma of Racism: Exploring the Systems and People Fear Built (pp. 35-61). Cham: Springer International Publishing.

Morozov, E. (2018, Eylül 28) Büyük Veri herkesin yararına olmalıdır. İşte nedeni bu. designatlarge: https://www.designatlarge.it/evgeny-morozov-big-data-ai-interview/?lang=en

Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007) Digital citizenship: The Internet, society, and participation. MIt Press.

Mueller, M. L., & Farhat, K. (2022) Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. Policy & Internet, 14(2), 348-367.

Mullahi, A., & Dhimitri, J. (2015) Education issues in a totalitarian state (case of Albania). Procedia-Social and Behavioral Sciences, 174, 4103-4107.

Mumford, M. D., Scott, G. M., Gaddis, B., & Strange, J. M. (2002) Leading creative people: Orchestrating expertise and relationships. The leadership quarterly, 13(6), 705-750.

Munich Security Conference (MSC), (2023) "Tech Accord to Combat Deceptive Use of AI in 2024 Elections," Munich Security Conference, https://securityconference.org/en/aielectionsaccord/

Muñoz-Rodríguez, J. M., Hernández-Serrano, M. J., & Tabernero, C. (2020) Digital identity levels in older learners: A new focus for sustainable lifelong education and inclusion. Sustainability, 12(24), 10657. doi.org/10.3390/su122410657

Murat, İ. (2017) Toplumsal tabakalaşma ve eşitsizlik. Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 19(1), 294-319.

Murphy, B. (2023) Disinformation and National Power. In Foreign

Disinformation in America and the US Government's Ethical Obligations to Respond (pp. 81-102). Cham: Springer Nature Switzerland.

Murray, A., Kuban, S., Josefy, M. ve Anderson, J. (2021) Akıllı çağda sözleşme: Blockchain ve merkezi olmayan özerk organizasyonların sözleşme ve kurumsal yönetim açısından etkileri. Yönetim Akademisi Perspektifleri, 35 (4), 622-641.

Muthuppalaniappan, M., & Stevenson, K. (2021) Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1), mzaa117.

Narin, B. (2018) Kişiselleştirilmiş çevrimiçi haber akışının yankı odası etkisi, filtre balonu ve siberbalkanizasyon kavramları çerçevesinde incelenmesi. Selçuk İletişim, 11(2), 232-251.

Nasr Esfahani, A. (2011) Flattery in Organization. Organizational culture management, 8(22), 95-114.

Neciyev, S., & Pazarbaşı, B. (2024) Siber Güvenlik, Siber Savaş Alanında Seçili Anahtar Kelimeler ile İlgili Araştırmaların Bibliyometrik Analizi. Gazi University Journal of Science Part C: Design and Technology, 1-1.

Nerse, S. (2020) Dijital eğitimde eşitsizlikler: Kırsal-kentsel ayrımlar ve sosyoekonomik farklılaşmalar. İnsan ve Toplum, 10(4), 413-444.

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021) Developing a global data breach database and the challenges encountered. Journal of Data and Information Quality (JDIQ), 13(1), 1-33.

New Zealand Human Rights Commission, (2018) Privacy, Data and Technology: Human Rights Challenges in the Digital Age. Auckland, Nueva Zelanda: New Zealand Human Rights Commission.

Nezih, Ö. (2018) Bilişim Teknolojileri Öğretmen Adayları Mesleki Eğitimleri İçin Neler Düşünüyor? Türkiye Sosyal Araştırmalar Dergisi, 22(1), 299-322.

Nguyen, M. H., Jin, R., Examining contributors to Vietnamese high school

Hoang, G., Nguyen, M. H. T., Nguyen, P. L., Le, T. T., ... & Vuong, Q. H. (2023) students' digital creativity under the serendipity-mindsponge-3D knowledge management framework. Thinking Skills and Creativity, 101350.

Noelle-Neumann, E. (1974) The spiral of silence a theory of public opinion. Journal of communication, 24(2), 43-51.

Nohutçu, A., & Yörükoğlu, E. (2023) Hukuk ve Kamu Yönetimi Politikalarında Yeni Medyanın Güçlü Etkisi: Sosyal Medya Yönetişimi. Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 9(2-1), 455-467.

Novella-García, C., & Cloquell-Lozano, A. (2021) The ethical dimension of digital competence in teacher training. Education and Information Technologies, 26(3), 3529-3541.

Nugent, D., & Vincent, J. (Eds.). (2008) A Companion to the Anthropology of Politics. John Wiley & Sons.

Núñez-Gómez, C., & Garcia-Font, V. (2022) HyperNet: A conditional k-anonymous and censorship resistant decentralized hypermedia architecture. Expert Systems with Applications, 208, 118079.

O'Connor, C., & Weatherall, J. O. (2019) The misinformation age: How false beliefs spread. Yale University Press.

Odabaşı, F. (2021) Kime/Neye, Niçin ve Nasıl İtaat Ediyorlar? Gençlerin İtaat Algısı ve Din Üzerine Sosyolojik Bir Araştırma. Amasya Üniversitesi Sosyal Bilimler Dergisi, (9), 33-81.

OECD (2022) Focus on rights in the digital age. Organisation for Economic Co-operation and Development: https://www.oecd.org/digital/rights/

OECD Publishing. (2019) How's life in the digital age?: Opportunities and risks of the digital transformation for people's well-being. Organisation for Economic Co-operation and Development OECD.

Oğuz, M. C. (2023) Authoritarianism extending to diaspora: transnational repression policies of authoritarian regimes and the İranian example.

Oğuzhan, M. (2023) Dijitalleşme ve Dijital Dönüşüm Üzerine Güncel

Araştırmalar. Dumrul, C., Kılıçarslan, Z., & Dumrul, Y. (Editörler). Kamu Yönetiminde Dijital Dönüşüm: E-Devletten Dijital Dönüşüm Ofisine. Sayfa 112-135. Ekin Yayınevi.

Oh, S. (2021) Is There Evidence of Antitrust Harm in the House Judiciary Committee's Hot Docs? Santa Clara High Tech. LJ, 37, 193.

Okmeydan, S. B. (2017) Postmodern kültürde gözetim toplumunun dönüşümü: 'Panoptikon'dan 'sinoptikon've 'omniptikon'a. AJIT-e: Academic Journal of Information Technology, 8(30), 45-69.

Oppenheimer, F. (2005) Devlet. Çev: Alâeddin Şenel-Yavuz Sabuncu. Ankara, Phoenix Yayınevi, https://www.franz-oppenheimer.de/tr/Devlet_TR.htm

Orwell, G. (1949) 1984.https://www.middletownhs.org/ourpages/auto/2016/3/22/36706638/1984%20text.pdf

Oxford Analytica. (2024) TikTok tasarısı ABD-Çin arasındaki uçurumu genişletecek. Emerald Uzman Brifingleri, (oxan-db).

Öçal, B. (2023) Sosyal bilimlerde toplumsal sorunlara bakış: teorik çalışmalar.

Önok, M. (2013) Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19(2), 1229-1270.

Örs, F., & Tetik, S. (2010) Küreselleşen Dünyada Yeni Yönetim Paradigmaları: Değişim ve İletişim. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 19(3), 439-455.

Öteleş, F., & Merey, Z. (2022) Sosyal Bilgiler Öğretmenlerinin Dijital Etik Kavramına İlişkin Görüşleri. İnönü Üniversitesi Eğitim Fakültesi Dergisi, 23(3), 1302-1323. DOI: 10.17679/inuefd.1135696

Özbay, R. D., & Genç, S. Y. (2023) Dijital Ekonomi: Sistematik Bir Literatür Araştırması. JOEEP: Journal of Emerging Economies and Policy, 8(2), 1-5.

Özdemir, İ., & Sinan, A., (2022) Post-Corona:" Hiçbir Şey Eskisi Gibi Olmayacak" mı? Eğitim Bilim Toplum, 20(79), 83-117.

Özdemir, U. (2022) Facebook-Cambrıdge Analytıca Skandalının Katılımcı Kültür, Dijital Emek Sömürüsü ve Mahremiyetin İhlali Çerçevesinde İncelenmesi. Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi, (10), 22-34.

Özer, M. A., & Kartal, M. (2023) Eylem ve Katılım İlişkisi Açısından Siyasal İletişim, Dijital Propaganda ve Sosyal Medya. Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 13(4), 1593-1619.

Özkan, Ö., & Kaya, Ş. Ş. (2015) Bilimsel makalede "sınırlılıklar" neden ve nasıl yazılır. TAF Preventive Medicine Bulletin, 14(6), 496-505.

Özlü, S., & Kösecik, M. (2016) "Anayasal vatandaşlık" ve Türkiye'de "yeni anayasa" yapım sürecinde siyasi partilerin vatandaşlık söylemleri. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 21(2), 513-537. Arş. Gör. Serpil Ozulu1, Prof. Dr. Muhammet Kösecik2

Özsoy, B. (2022) NATO'nun Genişlemesi ve Kazakistan Olayları Bağlamında Kolektif Güvenlik Antlaşması Örgütü'nün Geleceği. Журнал российских исследований, (8), 101-125.

Öztürk, M. S. (2018) Siber Saldirilar, Siber Güvenlik Denetimleri ve Bütüncül bir Denetim Modeli Önerisi. Journal of Accounting and Taxation Studies, 208-232.

Pacheco, D., Flammini, A., & Menczer, F. (2020, April) Unveiling coordinated groups behind white helmets disinformation. In Companion proceedings of the web conference 2020 (pp. 611-616).

Pangrazio, L., & Sefton-Green, J. (2021) Digital rights, digital citizenship and digital literacy: What's the difference? NAER: Journal of New Approaches in Educational Research, 10(1), 15-27.

Patton, M. Q. (2002) Qualitative research and evaluation methods. Thousand Oaks. Cal.: Sage Publications, 4.

Paul, K., & Ayiter, K., (1977) Roma özel hukukunun ana hatları. Ankara Üniversitesi Hukuk Fakültesi yayınları no. 414. Sevinç Matbaası,

Ankara

Pavel, B., Ke, I., Spirtas, M., Ryseff, J., Sabbag, L., Smith, G., ... & Lumpkin, D. (2023) AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?

Pérez-Escolar, M., & Noguera-Vivo, J. M. (2022) Hate speech and polarization in participatory society (p. 278). Taylor & Francis.

Peršak, N. (2022, June) Criminalising hate crime and hate speech at EU level: Extending the list of Eurocrimes under Article 83 (1) TFEU. In Criminal Law Forum (Vol. 33, No. 2, pp. 85-119). Dordrecht: Springer Netherlands.

Pholmat, P. (2023) Dijital Vatandaşlık Kavramını Yeniden Düşünmek: Sosyolojik Bir Perspektif. Yerel Yönetim ve Kalkınma Dergisi Pibulsongkram Rajabhat Üniversitesi, 3 (2), 95-105.

Pinto, M., Cordon, J. A., & Gómez Díaz, R. (2010) Thirty years of information literacy (1977—2007) A terminological, conceptual and statistical analysis. Journal of librarianship and information science, 42(1), 3-19.

Pinto, M., Fernández-Pascual, R., Caballero-Mariscal, D., & Sales, D. (2020) Information literacy trends in higher education (2006–2019): visualizing the emerging field of mobile information literacy. Scientometrics, 124(2), 1479-1510.

Pinto, M., Fernández-Pascual, R., Caballero-Mariscal, D., Sales, D., Guerrero, D., & Uribe, A. (2019) Scientific production on mobile information literacy in higher education: a bibliometric analysis (2006–2017). Scientometrics, 120(1), 57-85.

Platon (Eflatun), (1999) Devlet, (Çev. Sabahattin Eyüpoğlu & M. Ali Cimcoz), Türkiye İş Bankası Kültür Yayınları, İstanbul. 369 a-d

Polat, E. G. (2010) Anayasal Vatandaşlık, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Polat, G. E., & Akçakaya, M. (2022) Kamu Yönetiminde Verimlilik: Kavramsal Bir İnceleme. Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi,

8(2), 250-268.

Politikyol (22 Mayıs, 2021) Yeni dünyanın sorunu: Dijital eşitsizlik. Erişim tarihi 11.05.2024. https://www.politikyol.com/yeni-dunyanin-sorunu-dijital-esitsizlik/

Polkinghorne, D. E. (2005) Language and meaning: Data collection in qualitative research. Journal of counseling psychology, 52(2), 137.

Polona, C. (2022) European declaration on digital rights and principles.

Preece, J. (2000) Online communities: Designing usability and supporting socialbilty. John Wiley & Sons, Inc.

Pronzato, R. (2023) Reproducing hegemony, returning to critical pedagogy. The relationships of youth with digital platforms.

Punch, K. F. (2014) Sosyal Araştırmalara Giriş, Nicel ve Nitel Yaklaşımlar, 3. Baskı, (Çev: D. Bayrak, H. B. Arslan, Z. Akyüz), Siyasal Kitabevi, Ankara.

Punch, K. F., & Etöz, Z. (2005) Sosyal araştırmalara giriş: Nicel ve nitel yaklaşımlar. Siyasal Kitabevi.

Pyc, L. S., Meltzer, D. P. ve Liu, C. (2017) Ineffective leadership and employees' negative outcomes: The mediating effect of anxiety and depression. International Journal of Stress Management, 24(2), 196–215. https://doi.org/10.1037/str0000030

Qin, B., Strömberg, D., & Wu, Y. (2017) Why does China allow freer social media? Protests versus surveillance and propaganda. Journal of Economic Perspectives, 31(1), 117-40.

Ragnedda, M. (2018) Conceptualizing digital capital. Telematics and informatics, 35(8), 2366-2375.

Rahimnia, F., Mazidi, A. K. ve Mohammadzadeh, Z. (2013) Emotional mediators of psychological capital on well-being: The role of stress, anxiety, and depression. Management Science Letters,3, 913-926. https://doi.org/10.5267/j.msl.2013.01.029

Rahma, S. D., Putra, B. A., & Djarwadi, L. F. (2023, Analysis of the Indonesian Government's Efforts in Overcoming Public Data Leak Cases. In Proceedings of

December) Sunan Ampel International Conference of Political and Social Sciences (Vol. 1, pp. 254-266).

Rantanen, M. M., Koskinen, J., & Hyrynsalmi, S. (2019, May) E-government ecosystem: A new view to explain complex phenomenon. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1408-1413). IEEE.

Rao, S. (2019) The Nation-State and Journalism. In Oxford Research Encyclopedia of Communication. https://doi.org/10.1093/acrefore/9780190228613.013.878

Rasool, Z. (2020) Toplumsal Tabakalaşmanın Bir Aracı Olarak Kültürel Sermaye. The Journal of Social Sciences, (45), 482-491.

Ratchford, B. T. (2019) The Impact of Digital Innovations on Marketing and Consumers. Marketing in a Digital World, 35–61. doi:10.1108/s1548-643520190000016005

Rayburn, N. R., Mendoza, M., & Davidson, G. C. (2003) Bystanders' perceptions of perpetrators and victims of hate crime: An investigation using the person perception paradigm. Journal of Interpersonal Violence, 18(9), 1055-1074.

Regulation, P. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (eu), 679, 2016.

Reisach, U. (2021) The responsibility of social media in times of societal and political manipulation. European journal of operational research, 291(3), 906-917.

Reuters, (2020) Report says China internet firms censored coronavirus terms, criticism early in outbreak, 3 Marth 2020. Erişim 24. 11,2022. https://www.reuters.com/article/us-health-coronavirus-china-censorship-idUSKBN20Q1VS

Rheingold, H. (2000) Sanal topluluk, gözden geçirilmiş baskı: Elektronik sınırda ev sahipliği. MİT basını.

Ribble, M. (2015) Digital citizenship in schools: Nine elements all students should know. International Society for technology in Education.

Ricaurte, P. (2019) Data epistemologies, the coloniality of power, and

resistance. Television & New Media, 20(4), 350-365.

Richardson, J., & Milovidov, E. (2022) Digital citizenship education handbook: Being online, well-being online, and rights online. Council of Europe. https://rm.coe.int/prems-003222-gbr-2511-handbook-for-schools-16x24-2022-web-bat-1-/1680a67cab

Rindfleisch, A., & Malter, A. J. (2019) "Transitioning to a Digital World". Marketing in a digital world. Rindfleisch, A., & Malter, A. J. (Eds.). Emerald Group Publishing.

Roberts, M. (2018) Censored: distraction and diversion inside China's Great Firewall. Princeton University Press.

Robin, C. (2004) Fear: The history of a political idea. Oxford University Press.

Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022) Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. Technological Forecasting and Social Change, 178, 121562.

Rojon, S., Pilet, J. B., Vittori, D., Panel, S., & Paulis, E. (2023) Which political outsiders do Europeans prefer as ministers?. European Political Science Review, 1-21. 2023;15(3):444-464. doi:10.1017/S1755773923000048

Rone, J. (2022) Sahte profiller, troller ve dijital paranoya: Öfkeliler hareketini kırmak için dijital medya uygulamaları. Toplumsal Hareket Çalışmaları, 21 (1-2), 25-41.

Royal, C. C. (2023) Cybersecurity Safeguards: What Cybersecurity Safeguards Could Have Prevented the Intelligence/Data Breach by a Member of the Air National Guard.

Runco, M. A., & Jaeger, G. J. (2012) The standard definition of creativity. Creativity research journal, 24(1), 92-96.

Sağlam, T. Ç., & Yaşar, M. (2017) Teoride, pratikte ve araştirmalarda öteki ve ötekileştirme. Electronic Turkish Studies, 12(3).

Saka, E. (2022, Haziran 6) Dijitalleşen propaganda ve botların rolü. nl (newslabturkey): https://www.newslabturkey.org/2022/06/06/dijitallesen-propaganda-ve-botlarin-rolu/

Sawyer, R. K. (2010) Learning for creativity.

Saylam, A. (2022) E-Devlet Kavramının Dijital Devlet ve Elektronik/Dijital Yönetişim Kavramları Ekseninde Değerlendirilmesi. Third Sector Social Economic Review, 57(3), 2130-2149.

Schneider, R. D. (2012) Hadoop for Dummies. (Special Edition). Mississauga, Canada: John Wiley &Sons.

Schweppe, J. (2021) Nefret suçu nedir? Cogent Sosyal Bilimler, 7 (1), 1902643.

Sebastián, L. P., Fernández Vázquez, P. A., & Ramiro Fernandez, L. J. (2021) Technocratic Attitudes in COVID-19 Times: Change and Preference Over Types of Experts.

Seeliger, M. ve Baum, M. (2024) Twitter Trump'ı engellediğinde: Dijitalleşmiş halkların paradoksu, kararsızlığı ve diyalektiği. Felsefe ve Sosyal Eleştiri, 50 (1), 239-254.

Segal, E. A., Gerdes, K. E., Lietz, C. A., Wagaman, M. A., & Geiger, J. M. (2017) Assessing empathy. Columbia University Press.

Selçuk, O. C. (2019) İnternet bağımlılığı için risk faktörleri: Öz düzenleme yetersizliği ve boş zaman can sıkıntısı (Master's thesis, Sağlık Bilimleri Enstitüsü).

Sertaç, K. (2021) Sosyal medya kullanıcılarının dijital kimlik inşası sürecinde kültürel faaliyet ve sanat ile ilgili paylaşımlarının rolü. Turkish Online Journal of Design Art and Communication, 11(4), 1403-1419.

Setthasuravich, P., & Kato, H. (2020) The mediating role of the digital divide in outcomes of short-term transportation policy in Thailand. Transport Policy, 97, 161-171.

Sevda, Ü., & Sezgin, A. A. (2021) Büyük veri (big data)'nin yapay zeka uygulamalarında toplumsal sınıflandırmaya yönelik kaygılar. AJIT-e: Academic Journal of Information Technology, 12(44), 47-70.

Sever, S. (2007) Okuma kültürü edinme sürecinde Türkçe öğretiminin sorumluluğu. Okuma Kültürü ve Okullarda Uygulama Sorunları Toplantısı, 6, 108-126.

Shahab, S., Bagheri, B., & Potts, R. (2021) Barriers to employing e-participation in the Iranian planning system. Cities, 116, 103281.

Shany, Y. (2023) Digital Rights and the Outer Limits of International Human Rights Law. German Law Journal, 24(3), 461-472.

Shi, W., Liu, D., Yang, J., Zhang, J., Wen, S., & Su, J. (2020) Social bots' sentiment engagement in health emergencies: A topic-based analysis of the COVID-19 pandemic discussions on Twitter. International Journal of Environmental Research and Public Health, 17(22), 8701.

Skyttner, L. (2005) General Systems Theory: Problems, Perspectives. Practice, 2.

Snowden, E. (2019) Permanent Record: A Memoir of a Reluctant Whistleblower. Pan Macmillan.

Sobolev, A. (2019) Hükümet yanlısı "troller" Rusya'daki çevrimiçi sohbetleri nasıl etkiliyor?

Solmaz, S. B. (2023) Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi ve Savunma Stratejileri. Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi, 3(1), 1-9.

Solomon, P. H. (2007) Courts and judges in authoritarian regimes. World Politics, 60(1), 122-145.

Som Vural, S. (2016) Üniversite öğrencilerinin bakış açısıyla dijital vatandaşlık göstergelerinin incelenmesi. Doktora Tezi. Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.

Stepien, K. A., & Baernstein, A. (2006) Educating for empathy: a review. Journal of general internal medicine, 21, 524-530.

Stewart, M. (2021) Defending weapons inspections from the effects of disinformation.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2019) Children's data and privacy online: growing up in a digital age: research findings.

Stolle, D., & Micheletti, M. (2013) Political consumerism: Global responsibility in action. Cambridge University Press.

Strang, K. D., & Vajjhala, N. R. (2023) Why Cyberattacks Disrupt Society and How to Mitigate Risk. In Cybersecurity for Decision Makers (pp. 1-28). CRC Press.

Stukal, D., Sanovich, S., Tucker, J. A., & Bonneau, R. (2019) For whom the bot tolls: A neural networks approach to measuring political orientation of Twitter bots in Russia. Sage Open, 9(2), 2158244019827715.

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021) Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. Technology in Society, 65, 101565. https://doi.org/10.1016/j.techsoc.2021.101565

Şengül, N. A. (2023) Dijital Kültür ve Siberfeminizme Dijital Bölünme Üzerinden Bir Eleştiri. Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi, (12), 25-42.

Şenkardeş, İ. Ç. G. (2023) Merkeziyetsiz Kamusal Alan: Metaverse Bağlamında Kamusal Alanı Yeniden Düşünmek. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, (76), 149-159.

Şenol, Y., Şenol, FB ve Can Yaşar, M. (2024) Covid-19 salgınında okul öncesi çocukların dijital oyun bağımlılığı: sosyal duygusal gelişim ve ebeveyn rehberliği. Güncel Psikoloji, 43 (1), 839-847.

Taha, K. (2023) Panoptikondan Data Diktatörlüğüne: Özgürlüğün Sonu mu? Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Dergisi, 1(2), 137-162.

Tan, C. S., Tan, S. A., Mohd Hashim, I. H., Lee, M. N., Ong, A. W. H., & Problem-solving ability and stress mediate the relationship between creativity and happiness. Creativity Research Journal, 31(1), 15-25.

Yaacob, S. N. B. (2019)

Tapias, B. H., Guzmán, D. H., Muñoz, P. C., & Duarte, N. R. (2024) Digital Citizenship and Sustainable Governance: A Design Thinking Approach. Procedia Computer Science, 231, 78-85.

Tavares, A. F., Martins, J., & Lameiras, M. (2020) Electronic participation in a comparative perspective: Institutional determinants of performance. In Digital Government and Achieving E-Public Participation: Emerging Research and Opportunities (pp. 87-123). IGI Global.

Tayanç, M. (2021) Çağın gerisinde yaşayanlar: Göç, kent ve dijital eşitsizlik. Vankulu Sosyal Araştırmalar Dergisi, (8), 133-154.

Taylor, A. M. (2019) Examining the contribution of social work education to the digital professionalism of students for practice in the connected age (Doctoral Dissertation). University of Central Lancashire.

Taylor, C. (1992) The ethics of authenticity. Harvard University Press.

Tecim, V. (2004) Sistem Yaklaşımı ve Soft Sistem Düşüncesi. Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, 19(2), 75-100.

Tekeli, E. S. (2021) Özgürlük ve Sansür Tartışmaları Çerçevesinde İnternet Düzenlemeleri ve Gözetim. Yeni Medya, 2021(10), 164-176.

Tekin, H. H. (2006) Nitel araştırma yönteminin bir veri toplama tekniği olarak derinlemesine görüşme. İstanbul University Journal of Sociology, 3(13), 101-116.

Terry, C., & Cain, J. (2016) The emerging issue of digital empathy. American journal of pharmaceutical education, 80(4).

The European Association for Viewers Interests (EAVI) Let's talk about media literacy. https://eavi.eu/lets-talk-about-media-literacy/

| | |
|---|---|
| The World Economic Forum (10 January 2024) | Global Risks Report 2024, 19th Edition.https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf |
| Tidy, B. J. (2021, 06 16) | Why cyber gangs won't worry about US-Russia talks. BBC news: https://www.bbc.com/news/world-europe-57504755 |
| Tokmak, M. (2016) | Sözlü tarih ve derinlemesine görüşme. Ardahan Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2(3), 83-98. |
| Toots, M. (2019) | Why E-participation systems fail: The case of Estonia's Osale. ee. Government Information Quarterly, 36(3), 546-559. |
| Torlak, Ö. (2020) | Dijital Karteller ve Eşitsizlikler: Gelir Eşitsizliğinin Artmasında Şirketlerin Rolü. İnsan ve Toplum, 10(4), 383-412. |
| Turan, E. A. (2022) | Dijital Teknolojilerin Mahremiyet Üzerindeki Etkileri. Şarkiyat, 14(2), 834-849. |
| Tutar, F. K., Tutar, E., & Özlem, O. (2022) | Pandemi Döneminde Eğitim Sektöründeki Dijital Uçurum: Dezavantajlı Gruplar Üzerine Etkisi Türkiye Örneği. Social Sciences Studies Journal (SSSJournal), 8(98), 1681-1690. |
| Türay, A. (2016) | Nefret söylemi bağlamında halkı kin ve düşmanlığa tahrik suçu. Seçkin Yayıncılık |
| Türk, G. D., Bayrakcı, S., & Akçay, E. (2022: 316) | Metaverse ve benlik sunumu. Turkish Online Journal of Design Art and Communication, 12(2), 316-333. |
| Uçkan, Ö. (2011) | Gençlik, Bilgi Toplumu, Yönetişim, Sansür ve Türkiye. Katılımın" e-hali", 105. |
| Uddin, R., & Kumar, S. (2023) | Sdn-based federated learning approach for satellite-iot framework to enhance data security and privacy in space communication. IEEE Journal of Radio Frequency Identification. |
| Uladi, A. İ., & Arı, E. S. (2023) | Uladi, A. İ., & Arı, E. S. (2023). Büyük Veri, Büyük Veri Analizi ve Uygulama Alanları. Yönetim Bilişim Sistemleri Dergisi, 9(1), 1-14. |
| Uluocak, N. (1986) | Türk vatandaşlık hukuku (karşılaştırmalı-uygulamalı). Filiz |

Kitabevi.

UNCTAD. (2019) Digital Economy Report. Value Creation and Capture: Implications for Developing Countries. 4 Sep 2019. https://unctad.org/publication/digital-economy-report-2019

UNCTAD. (2021) Digital Economy Report 2021: Cross-border Data Flows and Development-For Whom the Data Flow. UN.

Ünlü, D. G. (2021) COVID-19 pandemisi dönemindeki ev içi boş zaman aktivitelerinin dijital yansıması. Türkiye İletişim Araştırmaları Dergisi, (38), 1-18.

Ünsal, R. (2020) Neoliberal Hegemonya ve Dijital Kültürün İşgali: Byung-Chul Han Perspektifinden Bir Değerlendirme. Sosyoloji Divanı, (15).

Vajen, B., Kenner, S., & Reichert, F. (2023) Digital citizenship education–Teachers' perspectives and practices in Germany and Hong Kong. Teaching and Teacher Education, 122, 103972.

Varış, M., & Avşar, B. (2022) Sosyal medyada nefret söylemi. TRT Akademi, 7(14), 348-359.

Veriter, S. (2021) European Democracy and Counter-Disinformation: Toward a new paradigm?

Viera, C. (2023) How to Write Limitations of the Study (with examples). August 25, 2023. Erişim tarihi; 01.04.2023, https://www.aje.com/arc/how-to-write-limitations-of-the-study/

Vivienne, S., McCosker, A., Johns, A., McCosker, A., Vivienne, S., & Johns, A. (2016) Digital citizenship as fluid interface (pp. 1-17). London, UK: Rowman & Littlefield International, Ltd.

Voo, J., Hemani, I., & Cassidy, D. (2022) National Cyber Power Index 2022.

Vosoughi, S., Roy, D., & Aral, S. (2018) The spread of true and false news online. science, 359(6380), 1146-1151.

Vrolijk, A., & Szajnfarber, Z. (2015) When Policy Structures Technology: Balancing upfront decomposition and in-process coordination in Europe′ s decentralized space technology ecosystem. Acta Astronautica, 106, 33-46.

Wagner, H. F., & Zeume, S. (2023) Data leaks and tax havens. Research Handbook on the Economics of Tax Havens.

Wang, W. C. (2019) Exploring the relationship among free-time management, leisure boredom, and internet addiction in undergraduates in Taiwan. Psychological reports, 122(5), 1651-1665.

Watanabe, H., Bouazizi, M., & Ohtsuki, T. (2018) Hate speech on twitter: A pragmatic approach to collect hateful and offensive expressions and perform hate speech detection. IEEE access, 6, 13825-13835.

Weber, A. (2009) Nefret söylemi el kitabı. Strazburg: Avrupa Konseyi.

Weisberg, R. (2020) Creativity: What It Is. In Rethinking Creativity: Inside-the-Box Thinking as the Basis for Innovation (pp. 41-72). Cambridge: Cambridge University Press. doi:10.1017/9781108785259.002.

Wen, J., Huang, Y., Liu, G., & Miao, M. (2023) The nature of nomophobia and its associations with contents of smartphone use and fear of missing out: a network perspective. Telematics and Informatics, 82, 102011.

West, S. M. (2019) Data capitalism: Redefining the logics of surveillance and privacy. Business & society, 58(1), 20-41.

Williamson, S. (2021) Elections, legitimacy, and compliance in authoritarian regimes: evidence from the Arab world. Democratization, 28(8), 1483-1504.

Wilson, T., & Starbird, K. (2020) Cross-platform disinformation campaigns: lessons learned and next steps. Harvard Kennedy School Misinformation Review, 1(1).

Windley, P. J. (2005) Digital Identity: Unmasking identity management architecture (IMA). " O'Reilly Media, Inc.".

Wirtz, B. W., Daiser, P., & Binkowska, B. (2018) E-participation: A strategic framework. International Journal of Public Administration, 41(1), 1-12.

Wondra, J. D., & Ellsworth, P. C. (2015) An appraisal theory of empathy and other vicarious emotional experiences. Psychological review, 122(3), 411.

Woolley, S. C., & Howard, P. N. (Eds.), (2018) Computational propaganda: Political parties, politicians, and political manipulation on social media. Oxford University Press.

Wylde, A. (2021, June) Zero trust: Never trust, always verify. In 2021 international conference on cyber situational awareness, data analytics and assessment (cybersa) (pp. 1-4). IEEE.

X (12 June 2020) Disclosing networks of state-linked information operations we've removed. Date of access: 19.04.2024. https://blog.x.com/en_us/topics/company/2020/information-operations-june-2020

Xu, B., & Albert, E. (2014) Media censorship in China. Council on Foreign Relations, 25, 243.

Yakacak, G. A., & Gümrükçüoğlu, Y. B. (2024) Yapay Zekanın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 72(4), 1701-1757.

Yanık, A. (2017) Bir Süperpanoptikon Olarak Yeni Medya: Yeni Medya Işığında Gözetimin Eleştirisi. Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 5(2), 784-800.

Yanli, X., & Danni, L. (2021, April) Prospect of Vocational Education under the Background of Digital Age: Analysis of European Union's "Digital Education Action Plan (2021-2027)". In 2021 International Conference on Internet, Education and Information Technology (IEIT) (pp. 164-167). IEEE.

Yazıcı, T. (2022) Kitle Kaynak ve Yapay Zekâ. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 24(4), 1301-1313.

Ye, W., & Zhao, L. (2023) "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. Discourse, Context & Media, 51, 100666.

Yıldırım, A. ve Şimşek, H. (2021) Sosyal bilimlerde nitel araştırma yöntemleri. Ankara: Seçkin Yayıncılık.

Yıldırım, F., Abukan, B., Öztürk, H., & Eker, H. (2020) Sosyal hizmette teknoloji kullanımı ve sosyal hizmet uzmanlarının dijital yapabilirlikleri: Covid-19 salgını odağında bir değerlendirme. Electronic Turkish Studies, 15(8).

Yıldız, A., Akar Vural, R. (2020) Covid-19 pandemisi ve derinleşen eğitim eşitsizlikleri. Türk Tabipleri Birliği Covid-19 pandemisi altıncı ay değerlendirme raporu, 556-565.

Yıldız, S. K. (2021) Teknoloji Şirketlerinin Mahremiyet Algısını Dönüştürmesi: Sosyal Medya Tekelleşmesine Yönelik Etik Kaygılar. Communication and Technology Congress – CTC 2021 (April 12th-14th, 2021 – Turkey, Istanbul)

Yılmaz, B., & Özcan, E. (2022) Dördüncü Kuşak İnsan Hakları Bağlamında Sosyal Bilimlerde Büyük Veri Sorunsalı. Turkish Studies-Social Sciences, 17(3).

Yılmaz, O., Kaplan, B. T., & Kaplan, M. (2022) Blockchain teknolojileri ve sektörel etkileri.

Yılmaz, Y. (2013) Meşru otoritenin birey üzerinde yarattığı korku: korkunun iktidarına medyanın etkisi.

Yurdakul, D. (2021, Mayıs 22) Yeni dünyanın sorunu: Dijital eşitsizlik. Politikyol: https://www.politikyol.com/yeni-dunyanin-sorunu-dijital-esitsizlik/ erişim tarihi:13.04.2023

Yükselbaba, Ü. (2017) Milgram deneyi: Otorite ve itaate dair. Journal of Istanbul University Law Faculty, 75(1), 227-270.

Zaki, J. (2017) Moving beyond stereotypes of empathy. Trends in Cognitive Sciences, 21(2), 59-60.

Zhang, C. (2020) Covid-19 in China: From 'Chernobyl moment'to impetus

for nationalism. Made in China Journal, 5(2), 162-165.

Zhang, Y., Chen, F., & Lukito, J. (2023) Network amplification of politicized information and misinformation about COVID-19 by conservative media and partisan influencers on Twitter. Political Communication, 40(1), 24-47.

Zhang, Y., Lukito, J., Su, M. H., Suk, J., Xia, Y., Kim, S. J., ... & Wells, C. (2021) Assembling the networks and audiences of disinformation: How successful Russian IRA Twitter accounts built their followings, 2015–2017. Journal of Communication, 71(2), 305-331.

Zhao, H. (2020) Politicizing crisis communication via social media: A contextual understanding of organizational crises in China. Lund University.

Zhou, H., & Jiang, F. K. (2023) 'The study has clear limitations': Presentation of limitations in conclusion sections of PhD dissertations and research articles in applied linguistics. English for Specific Purposes, 71, 34-47.

Zhu, J., Ni, P., Tong, G., Wang, G., & Huang, J. (2021) Influence maximization problem with echo chamber effect in social network. IEEE Transactions on Computational Social Systems, 8(5), 1163-1171.

Zinderen, A. (2021) Dijital Sosyoloji Çalışmaları. Nobel Bilimsel Eserler.

Zorell, C. V. (2018) Varieties of political consumerism: From boycotting to buycotting. Springer.

Zuboff, S. (2019, January) Surveillance capitalism and the challenge of collective action. In New labor forum (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: SAGE Publications.

Zuboff, S. (2023) The age of surveillance capitalism. In Social theory re-wired (pp. 203-213). Routledge.

Zurkowski, P. G. (1974) The Information Service Environment Relationships and Priorities. Related Paper No. 5.

# EKLER

## EK – 1 YARI YAPILANDIRILMIŞ GÖRÜŞME FORMU

| KATILIMCI HAKKINDA GENEL BİLGİLER | |
|---|---|
| Cinsiyet | |
| Eğitim Durumu | |
| Mesleği | |
| Yaş Bilgileri | |
| İş Deneyimi(yıl) | |

| SORULAR | |
|---|---|
| **1** | Dijital dünyada endişe duyulan sorunlardan biri veri tekelciliği ve olumsuz etkileridir, bu konuda dezavantajlı ülkeleri de kapsayacak çözüm önerileri neler olabilir? |
| **2** | Dijital dünyada siber saldırıları ve savaşları önlemek amacıyla ne tür tedbirler alınmalıdır, siber suçlara yönelik ülkeler arasında yapılan anlaşmalar ne kadar güvenilir olabilir? |
| **3** | Egemen sınıf dijital dünyada toplumsal ilişkileri manipüle etmek amacıyla dijital eşitsizlikleri görmezden gelir ve aktif katılımı çeşitli yöntemlerle engellemeye çalışır. Bu sorunları en azından azaltabilmek amacıyla ne tür önlemler alınabilir? |
| **4** | Dijital dünyada kişisel verilerin toplanması, saklanması, korunması ve farklı amaçlarla kullanılmasına ilişkin sorunların çözülmesine yönelik hangi adımlar atılmalıdır? |
| **5** | Gelişmekte olan ülkeler tarafından altyapısı hazırlanan teknoloji tabanlı şirketler, dijital platformlar ve teknolojiler neden rekabet esasları üzerine kurulan serbest piyasada ABD merkezli büyük teknoloji şirketleriyle (Alphabet, Apple, Amazon, Meta, Microsoft, ...) küresel ölçekte rekabet edemezler? |

# ÖZGEÇMİŞ

Sehavet Neciyev (Səxavət Nəciyev) 2004 yılında Visten köy Lisesi'nden mezun oldu. 2006 yılında askerlik görevini tamamladı, 2013 yılında Kocaeli Üniversitesi İletişim Fakültesi Gazetecilik Bölümü'nden mezun oldu. 2015 yılında Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim Dalı'nda 'Türkiye'de ve Azerbaycan'daki Haber Partallarının Tarafsızlık Kavramı Bağlamında İncelenmesi' adlı teziyle yüksek lisans eğitimini tamamladı. Eğitimi devam ederken reklam ajansında ve haber partallarında çalıştı. İletişim alanında akademik çalışmalar yaptı. Yeni medya, fotoğraf düzenleme, tasarım, çizim, video kurgu, ses tasarımı, siber güvenlik, yapay zekâ ve Arama Motoru Optimizasyonu (SEO) ilgi duyduğu çalışma alanlarıdır.