SOSYAL MEDYADA KİŞİSEL VERİLERİN KORUNMASI SORUNU

Damla Sabiha VAROL
211128103

YÜKSEK LİSANS TEZİ
Disiplinlerarası İnsan Hakları Anabilim Dalı
İnsan Hakları Tezli Yüksek Lisans Programı
Danışman: Prof. Dr. Betül ÇOTUKSÖKEN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2023

SOSYAL MEDYADA KİŞİSEL VERİLERİN KORUNMASI SORUNU

Damla Sabiha VAROL
211128103
ORCID: 0009-0004-3309-3714

YÜKSEK LİSANS TEZİ
Disiplinlerarası İnsan Hakları Anabilim Dalı
İnsan Hakları Tezli Yüksek Lisans Programı
Danışman: Prof. Dr. Betül ÇOTUKSÖKEN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2023



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Tez çalışmamın oluşturulmasındaki emekleri için önerilerinden ve felsefi yaklaşımından yararlandığım değerli danışman hocam Prof. Dr. Betül Çotuksöken'e, insan hakları sorunlarını değerlendirirken başvuracağım felsefi-etik temeli kazandırmakta büyük emeği olan değerli hocam Prof. Dr. İoanna Kuçuradi'ye ve tez çalışmamı geliştirmeme katkı sunan Doç. Dr. Özge Yücel Dericiler'e teşekkür ederim.

Damla Sabiha VAROL

Eylül, 2023

ÖZET

SOSYAL MEDYADA KİŞİSEL VERİLERİN KORUNMASI SORUNU

Damla Sabiha Varol
Yüksek Lisans Tezi
Disiplinlerarası İnsan Hakları Anabilim Dalı
İnsan Hakları Tezli Yüksek Lisans Programı
Danışman: Prof. Dr. Betül Çotuksöken
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2023

Sosyal medya, hemen her kişinin hayatında yeri olan, toplumsallığın bir biçimi olarak toplumla etkileşen ve onu birçok yönden etkileme ve değiştirme gücüne sahip kendine özgü biçimi, dili ve farklı işlevleri olan bir araç haline gelmiştir. Sosyal medya platformları, kullanıcıların kişisel verilerini toplamaktadır. Bu verileri kaydedip işlemekte ve üçüncü taraflarla paylaşarak çıkar sağlamaktadırlar. Bireyler de kendileri için bir gereksinim haline gelen sosyal medya kullanımı sırasında özel yaşamlarıyla ilgili pek çok veriyi gönüllü olarak paylaşmaktadır. Çağımızda, artık hiçbir şeyin gizlenemeyeceğine ve mahremiyetin giderek olanaksızlaştığına dair görüşler öne çıkmaktadır.

Tez çalışmamızın amacı, sosyal medyada gönüllü olarak veya yeterince bilgi sahibi olmadan aktarılan ve kaydedilen kişisel verilerin, bireyler için yaratacağı riskleri ve söz konusu verilerin kullanılması durumunda toplumu etkileyecek sorunları belirlemek; ayrıca sadece yasal düzenlemelerin tek başına bu bağlamdaki tüm sorunları çözümlemede ve çözüme kavuşturmada yeterli olamayacağını savunarak sorunu ele almada felsefi-etik yaklaşımın önemini ortaya koymaktır.

Araştırma üç bölümden oluşmaktadır. İlk bölümde, kişisel veri kavramı açıklandıktan sonra kişisel verilerin korunması hakkının tarihsel gelişimine değinilmiştir. Kişisel verilerin korunması hakkının diğer temel hak ve özgürlüklerle ilişkisi belirtilerek bir insan hakkı olarak kişisel verilerin korunması konusu ele alınmıştır. Ayrıca kişisel verilerin korunmasıyla ilgili hukuki düzenlemeler hakkında bilgi verilip hukuki çerçeve belirlenmiştir.

İkinci bölümde, sosyal medya kavramı ve bu olgunun ortaya çıkışıyla gelişiminin tarihi üzerinde durulmuştur. Bazı medya platformlarına ait gizlilik politikaları hakkında bilgi verilmiştir. Kişisel verilerin işlenmesinin gereğini ve bu verilerin korunmasındaki riskleri yaratan nedenlerden büyük veri teknolojisi ve veri madenciliği üzerinde durulmuştur.

Üçüncü bölüm, ana problemin açımlandığı kısımdır. Sosyal medyada kişisel verilerin korunması ihtiyacı, temel hak ve özgürlükler bağlamında incelenmiş ve veri gizliliğinin sağlanmasında alınması gereken önlemler hakkında bilgi verilmiştir. Son olarak hukuki düzenlemelerin dışında bu konuda ortaya çıkan ve çıkabilecek hak ihlallerinin önlenmesinde çok büyük bir işleve sahip olan, toplumun konuyla ilgili bilinçlenme edimi gerçekleştirilirken temele alınması gereken insan hakları bilgisiyle etik konusu ele alınmıştır.

Anahtar Sözcükler: Sosyal Medya, Mahremiyet, Kişisel Veri, Büyük Veri, İnsan Hakları.

ABSTRACT

THE ISSUE OF PERSONAL DATA PROTECTION IN SOCIAL MEDIA

Damla Sabiha Varol
Master Thesis
Interdisciplinary Department of Human Rights
Human Rights Master's Program with Thesis
Advisor: Prof. Dr. Betül Çotuksöken
Maltepe University Graduate School, 2023

Social media has become a tool with its own distinct shape, vocabulary, and functions that has a place in practically everyone's life, interacts with society as a type of sociality, and has the ability to affect and modify it in a variety of ways. Social media networks collect personal information about users. They collect, handle, and distribute/share this data with third parties for their own interests. Individuals freely share a considerable quantity of information about their personal lives on social media, which has become an essential aspect in their everyday lives. There are some who believe that nothing can be hidden anymore and that privacy is getting increasingly difficult.

The aim of our thesis is to identify the risks that personal data shared and recorded in social media, voluntarily or without sufficient information, may pose to individuals and the problems that will affect society in case of the use of such data; and also to show the importance of the philosophical-ethical approach in addressing the problem, arguing that legal regulations alone are not sufficient to solve and resolve all the problems in this context.

The research consists of three sections. In the first part, after explaining the concept of personal data, the historical development of the right to protection of personal data is mentioned. The relationship between the right to protection of personal data and other fundamental rights and freedoms is stated and the protection of personal data as a human right is discussed. In addition, information about the legal regulations on the protection of personal data is given and the legal framework is determined.

In the second section, the concept of social media and the history of the emergence and development of this phenomenon are emphasized. Information about the privacy policies of some media platforms is given. The necessity of processing personal data and the reasons that create risks in the protection of this data, big data technology and data mining are emphasized.

The third chapter is the part where the main problem is explained. The need for the protection of personal data in social media is analyzed in the context of fundamental rights and freedoms and information is given about the measures to be taken to ensure data privacy. Finally, apart from legal regulations, the issue of ethics is discussed with the knowledge of human rights, which has a great function in preventing the violations of rights that have arisen and may arise in this regard, and which should be taken as a basis while raising awareness of the society on the subject.

Keywords: Social Media, Privacy, Personal Data, Big Data, Human Rights.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii

ETİK İLKE VE KURALLARA UYUM BEYANI iii

TEŞEKKÜR iv

ÖZET v

ABSTRACT vii

İÇİNDEKİLER ix

KISALTMALAR xii

1. GİRİŞ 1

1.1 Tezin Problemi 1

1.2 Tezin Amacı 5

1.3 Tezin Önemi 6

2. KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI 7

2.1. Kişisel Veri Kavramı 7

2.1.1 Hassas veriler (Özel nitelikli kişisel veriler) 12

2.1.2 Hassas Olmayan Veriler 13

2.1.3 Kişisel verilerin toplanması ve işlenmesi 14

2.1.4 Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi 15

2.2 Kişisel Verilerin Korunması Hakkının Tarihsel ve Hukuki Boyutu 17

2.2.1 Özel hayatın gizliliğinin korunmasıyla ilgili uluslararası düzenlemeler 19

2.2.2 Kişisel verilerin korunmasıyla ilgili uluslararası düzenlemeler 20

2.2.2.1 OECD rehber ilkeleri 21

2.2.2.2 Avrupa Konseyi düzenlemeleri 21

2.2.2.3 Avrupa Birliği düzenlemeleri 22

2.2.3 Kişisel verilerin korunmasıyla ilgili ulusal düzenlemeler 24

2.2.3.1 Türkiye Cumhuriyeti Anayasası 24

2.2.3.2 5237 Sayılı Türk Ceza Kanunu 25

2.2.3.3 6698 Sayılı Kişisel Verilerin Korunması Kanunu 26

2.3 Bir İnsan Hakkı Olarak Kişisel Verilerin Korunması ve İlişkili Olduğu Temel Haklar 31

2.3.1 Bir insan hakkı olarak kişisel verilerin korunmasının felsefi boyutu ve mahremiyet hakkı ile ilişkisi 31

2.3.2 Kişisel verilerin korunmasının diğer hak ve özgürlüklerle ilişkisi 41

2.3.3 Bir kişilik hakkı olarak kişisel verilerin korunması 44

3. SOSYAL MEDYA 47

3.1 Sosyal Medya Kavramı ve Sosyal Medyanın Gelişimi 47

3.1.1 Sosyal medya kavramı 47

3.1.2 Sosyal medyanın gelişimi 49

3.1.2.1 İnternetin Doğuşu ve Web 0.1 49

3.1.2.2 Sosyal ağ platformlarının doğuşu ve Web 0.2 50

3.1.2.3 Anlamsal (Semantik) Web'in doğuşu, Web 0.3 ve Web. 04 52

3.1.3 Sosyal medyanın özellikleri ve türleri 53

3.2 Çeşitli Sosyal Medya Siteleri ve Gizlilik Politikaları 56

3.2.1 Facebook, Instagram ve Meta gizlilik politikası 59

3.2.2 X (Twitter) ve gizlilik politikası 66

3.3 Büyük Veri Devrimi ve Sosyal Medya Madenciliği 75

4. SOSYAL MEDYADA KİŞİSEL VERİLERİN KORUNMASI 83

4.1 Temel Hak ve Özgürlükler Bağlamında Sosyal Medyada Kişisel Verilerin Korunması Gereksinimi 83

4.2 Sosyal Medyada Kişisel Veri Gizliliği Sorunları ve Gizliliğin Sağlanmasında Alınması Gereken Önlemler 103

4.3 Sosyal Medyada Kişisel Veri Gizliliğini ve Güvenliğini Sağlamada İnsan Hakları ve Etik Bilginin Önemi 125

SONUÇ ve ÖNERİLER 134

KAYNAKLAR 144

ÖZGEÇMİŞ 171

KISALTMALAR

AİHM:	Avrupa İnsan Hakları Mahkemesi
AİHS:	Avrupa İnsan Hakları Sözleşmesi
GDPR:	General Data Protection Regulation (Genel Veri Koruma Tüzüğü
KVKK:	6698 Sayılı Kişisel Verilerin Korunması Kanunu
OECD:	Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
OECD Rehber İlkeleri:	OECD Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri
TCK:	5237 Sayılı Türk Ceza Kanunu
108 Sayılı Sözleşme:	108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
95/46/EC Sayılı Veri Koruma Direktifi:	95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi

1. GİRİŞ

1.1 Tezin Problemi

Bilişim sistemlerindeki gelişmelerin hayatımız üzerinde yarattığı değişiklikler birtakım sorunları da beraberinde getirmektedir. Tarihe baktığımızda bilimsel gelişmelerin sonucunda ortaya çıkan pek çok teknolojik ürünün, günlük yaşamda sunduğu kolaylıkların ve yararların yanı sıra bazı olumsuzlukların da olduğunu fark etmekteyiz. İnternet devrimiyle birlikte sosyal medyanın hayatımıza girmesi nedeniyle günümüzde birçok kişilik hakkı ihlali ortaya çıkmaktadır. Özellikle özel hayatın gizliliği konusunda yaşanan sıkıntılar, kullanıcıların sayısı ve sosyal medyanın hayatımızda kapladığı yer arttıkça, sosyal medyada kişisel verilerin korunması, önemi gittikçe artan bir sorun alanı haline gelmiştir. Bu araştırmanın ana problemi, sosyal medyanın kullanımı sırasında işlenen kişisel verilerin, insan hakları açısından ortaya çıkardığı bireysel ve toplumsal sorunlardır.

Kişisel verinin mevzuatta yapılan tanımı genel olarak kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi şeklindedir. Bu tanım, ülkemizin 6698 sayılı Kişisel Verilerin Korunması Kanununda (KVKK) da belirtilen tanımdır (KVKK, 3. Madde), Kişisel veriler ayrıca hassas veri ve hassas olmayan veri olarak ikiye ayrılmaktadır. Hassas veriler olarak tanımlanan veriler korunması gereken en önemli kişisel verilerdir. Hassas olmayan veriler ise paylaşılması durumunda hassas veriler gibi bireylere zarar vermeyecek olan ve başkaları tarafından bilinmesinde sakınca olmayan verilerdir.

Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem ise kişisel verilerin işlenmesi olarak tanımlanmaktadır (KVKK, 3. Madde)

Kişisel verilerin belirtilen şekilde toplandıktan sonra silinmesine, yok edilmesine ya da anonim hale getirilmesine kadar olan işlemler sırasında gerçekleştirilen her türlü faaliyet de kişisel verilerin işlenmesi olarak kabul edilmektedir.

Sosyal medya ise, dergi, gazete, radyo, televizyon ve diğer kitle iletişim araçları gibi yeni bir medya ortamıdır. Bu ortam diğer medya araçları gibi çeşitli bilgilerin ve düşüncelerin paylaşıldığı ve kitlelere taşındığı bir ortamdır. Geleneksel medya kategorisinde yer alan dergi, gazete, radyo ve televizyon gibi tek yönlü ve durağan yayın teknolojilerinden farklı olarak herkesin kendi içeriğini oluşturduğu ve dağıtımını yine kendisinin yaptığı yeni web teknolojileri sosyal medya olarak değerlendirilmektedir (Zarrella, 2010 akt. Tarhan, 2019b, s. 106). Sosyal medyanın çeşitli kaynaklarda farklı birçok tanımı bulunmaktadır. Ancak yaygın olarak tanımlanması Web 0.1'den Web 0.2'ye geçiş aşamasında ortaya çıkmıştır. Çünkü Web 0.2'ye geçişle birlikte kullanıcılar etkileşimli şekilde çift taraflı iletişim kurma olanağına sahip olmuşlardır. Sosyal medya, insanların kendi içeriklerini oluşturabildikleri, etkileşimli olarak birebir veya toplumsal iletişim kurabildikleri ve çeşitli içerikleri kolayca paylaşabildikleri Web 0.2 ortamlarıdır. Günümüzdeki yapay zekâ çalışmaları ile anlamsal ağ (semantic web) olarak adlandırılan Web 0.3 kavramı ortaya çıkmıştır. İnternetin yeni çağı olarak görülen Web 0.3 ve büyük veri (big data), pek çok alanda kullanılmaya başlanan sosyal medya madenciliği uygulamalarının ortaya çıkmasıyla özellikle kişisel veri gizliliği konusunda önemli riskleri beraberinde getirmiştir.

Büyük veri, çok çeşitli, hacmi büyük ve çok hızlı üretilen veri bütünleridir. Dünya genelinde üretilen dijital verilerdeki olağanüstü artış, çok çeşitli ve çok büyük veri bütünlerinin saklanması, işlenmesi ve bunlardan anlamlı sonuçlar çıkarılmasını sağlayan büyük veri uygulamalarının doğmasına neden olmuştur. Büyük veri, hem geleneksel veri araçlarının depolayıp saklayamayacağı kadar büyük bir veri yığınını hem de veri yığını çok büyük olduğu için bu verileri yapay zekâ yoluyla anlamlandırmayı ve bilgiye dönüştürmeyi içeren uygulamaları ifade eden bir kavram haline gelmiştir (Løkke, 2020, s. 60). Büyük veriyle birlikte ele alınması gereken diğer bir kavram ise veri madenciliğidir. Veri madenciliği, büyük ölçekli veriler arasından, enformasyon oluşturacak değerli veriyi madenleme işidir (Esgin, 2015, s. 53-55). Veri madenciliği ayrıca, büyük veri yığınları arasından öngörülerde bulunulmasını sağlayabilecek

bağlantıların bilgisayar programı kullanılarak aranmasıdır. Veri madenciliğinin veri işleme metotları sadece belli bir veri tabanı üzerinde bulunan veriler için geçerlidir. Ancak günümüzde asıl veriler çevrimiçi ortamda bulunmaktadır. Şirketler dahi verilerinin tamamını internete taşımışlardır. Bu nedenle web madenciliği *(web mining)* kavramı ortaya çıkmıştır. Web madenciliği, web sayfalarında bulunan içeriklerin ve kullanıcıların bu içeriklerle etkileşiminin veri madenciliği ilkeleri doğrultusunda yorumlanıp anlamlı sonuçlar haline getirilmesini amaçlamaktadır (Esgin, 2015, s. 53-55). Web madenciliğinin bir parçası olarak sosyal medya sitelerinin ortaya çıkmasıyla da sosyal medya madenciliği kavramı doğmuştur. Sosyal medya madenciliği ise kullanıcıların ürettiği sosyal medya içeriklerinin ve bu içeriklerle ilgili etkileşimlerin incelenmesi ve değerlendirilmesiyle anlamlı sonuçlar çıkarmayı sağlayan ve bunu yaparken veri madenciliği ilkelerini kullanan bir araştırma dalıdır. Kullanıcıların sosyal medya verileri toplanmakta, düzenlenmekte ve çözümlenerek anlamlı sonuçlar çıkarılmaya çalışılmaktadır (Ünver, 2015, s. 79).

"Çağımızın ham maddesi" olarak değerlendirilen büyük verinin en önemli kaynaklarından olan sosyal medya verileri çok değerlidir. Büyük verinin değeri, Google, Amazon, X (Twitter) ve Facebook gibi dev bilişim kuruluşları tarafından en başından beri bilinmekte, hatta adı geçen şirketlerin kuruluş yaklaşımının, ilkelerinin temelinde bulunmaktadır. Genellikle ücretsiz hizmet veren bu firmalar gizlilik sözleşmelerinin kullanıcılar tarafından onaylanması sayesinde yapay zekâ destekli büyük veri uygulamalarından yararlanarak kullanıcıların internetteki hareketlerini izlemekte ve bunları çözümleyerek anlamlandırmaktadır. Böylece kullanıcıların hoşlanacağı türde reklam, haber vb. içerikleri de belirleyebilmektedirler. Hatta kullanıcıların hassas verileri olarak kabul edilen siyasi görüş, inanç gibi tercihleri de belirlenebilmektedir (Ege, 2013). Kişisel veri kaynaklı öngörü ürünlerinin ticaretiyle pek çok şirket, gelecekteki davranışlarımızı tahmin ederek bu ticari faaliyetler üzerinden olağanüstü servetler elde etmektedirler (Zuboff, 2021, s. 20-21).

Büyük veri analizlerinin çok değerli olmasının en önemli nedenlerinden biri, veriyi yeniden kullanabilme olanağıdır. Depolama kapasitesi genişledikçe ve işleme olanakları arttıkça verilerin yeniden kullanılma olanağı da artmaktadır. Verilerin yeniden kullanımı, kişilerin internette bıraktıkları dijital izlerin belirli amaçlar için kullanıldıktan sonra

muhtemelen onay almaksızın başka amaçlar için de kullanılabileceği anlamına gelmektedir ve mahremiyet açısından bu durum potansiyel bir sorun olarak karşımıza çıkmaktadır (Løkke, 2020, s. 63).

Büyük veri teknolojileri sadece reklamcılık ve pazarlama alanında yararlanılan bir olanak değildir. Çünkü kullanıcılar söz konusu sosyal ağlarda bir fikir, bilgi veya haber paylaşırken, video ararken, e-posta yazarken, kitap sipariş ederken veya bir arama motorunda belirli kavramları ararken ister istemez siyasal görüşleri gibi bazı kişisel görüşlerini yansıtmaktadırlar (Ege, 2013). Sosyal medya madenciliği yoluyla uygulanan büyük veri teknolojilerinin toplumu ilgilendiren en önemli olanaklarından biri sosyal ağlar yoluyla toplanan verilerin analiz edilerek çeşitli müdahale yolları için kullanılabilecek olmasıdır. Bu noktada, sosyal medyanın çağın toplumsal-siyasal yönlendirme ve gözetim aracı haline gelmesi konusuna değinmek gerekmektedir.

Teknolojik olanakların gelişmesiyle birlikte gözetim olgusu da dönüşmekte ve özellikle sosyal medya kullanımı yoluyla gözetim, kişilerin gönüllü bir şekilde özel yaşamlarını paylaşmalarıyla olağanlaşmakta ve yayılmaktadır. Sosyal medya ve internet üzerinden toplanan kişisel verilerin büyük bir çoğunluğunu, aslında kişilerin akıllı telefonlar kullanarak gönüllü bir şekilde sağlamaları, sosyal medyada kişisel verilerin korunması sorununun en önemli zorluklarından biri olarak ortaya çıkmaktadır. Özel yaşamı paylaşmayı olağan hale getirmeye neden olan şeffaflık ideolojisi toplumun gözetime gönüllü olarak teslim olmasına yol açmaktadır. İnternet ve sosyal medya kullanımıyla artık iletişim ve ticaret, özgürlük ve denetim aynı şey haline gelmiştir (Han, 2020, s. 71-72). Bir kişinin verileri bizzat o kişinin yaşamını etkileme ve ona zarar verme amacıyla kullanılmasa da veya tek başına o kişinin bilgileri önemli olmasa da büyük ölçekte bakıldığında milyonlarca ya da milyarlarca kişinin verilerinin yapay zekâ teknolojileriyle çözümlenmesi, bu enformasyona sahip kişilere tüm bu insanlar üzerinde kullanabilecekleri, üstelik bugüne kadar sahip olunmayan çok büyük bir güç, yönlendirme ve denetim olanağı vermektedir. Böylece kişisel verilerin gizliliği sorunu, verileri açıklanan tek tek bireyler için, söz konusu verilerin açığa çıkmasının ortaya çıkaracağı zararların ötesinde, toplumsal ve küresel etkiler yaratacak riskler taşıması bakımından da önemle ele alınması gereken bir konu olarak karşımızda durmaktadır. Sosyal medyada kişisel verilerin korunması sorunu sadece özel hayatın gizliliğini değil,

pek çok temel hak ve özgürlüğü kapsayan ve tezimizde ortaya koymaya çalıştığımız gibi insan hakları düşüncesinde çözülmelere neden olabilecek uzantıları da olan bir sorundur.

1.2 Tezin Amacı

Araştırmanın amacı, sosyal medyada gönüllü olarak ya da yeterince bilgi sahibi olmadan aktarılan ve kayıt altına alınan kişisel verilerin, bireyler için yaratacağı riskleri ve söz konusu verilerin kullanılması durumunda toplumu etkileyecek sorunları belirlemek; ayrıca sadece yasal düzenlemelerin tek başına bu bağlamdaki tüm sorunları çözümlemede ve çözüme kavuşturmada yeterli olamayacağını savunmaktır. Kişisel verilerin korunması gereğini ortaya çıkaran, diğer temel hak ve özgürlükler bakımından kişilerin karşı karşıya kalabilecekleri sorunlar belirlendiğinde kişisel verilerin korunmasının veya veri gizliliğinin günümüzde özel hayatın gizliliğinin korunması hakkıyla ilişkisinin ötesinde başlı başına bir insan hakkı olarak tanınması gerektiği ortaya çıkmaktadır.

Çağın dijital toplumunda, bir kamusal alan olarak şekillenebilecek sosyal medya bireylerin özel yaşamlarının ve kişisel verilerinin ortaya serilmesiyle, özel alanın kamusallaşması sorununu da ortaya çıkarmaktadır. Sosyal medyada kişisel gizliliğin korunması konusunda güvenlik-gizlilik ikilemi olarak adlandırılabilecek duruma da değinmek önem taşımaktadır. Çünkü özellikle kurumlar ve yasalar yoluyla alınacak önlemlerde güvenlik ve gizlilik dengesini sağlamak son derece kritik bir noktadır. Konunun etik ve insan hakları açısından değerlendirilmesinde de bu dengenin doğru şekilde ele alınması çok önemlidir. İnsanların diğer tüm hak ve özgürlüklerini kullanabilmeleri için başat rolde kabul edilen yaşam hakkını korumak güvenliği sağlamayı gerektirmektedir. Fakat güvenliği sağlamak için alınacak bazı önlemler, özel hayatın ve kişisel verilerin gizliliğini tehlikeye atabilmektedir. Bu bağlamda kişisel verilerin korunmasında özel yarar ve kamu yararıyla güvenlik ve mahremiyet arasındaki dengeleri kurmanın ve bu dengelerin insan haklarının felsefi temellerine göre kurulmasının gerekliliğini ortaya koymak da büyük önem taşımaktadır.

Bilişim teknolojilerindeki gelişmeler ve sosyal medya kullanımının yaşamımızın önemli bir parçası haline gelmesi, insanın anlam ve değer dünyasını da dönüştürmektedir. Örneğin, sosyal medya kullanımı artık insanları öyle etkisi altına almıştır ki, özel hayatımızın gizliliğine ilişkin algımız değişmiş, mahremiyete verdiğimiz önem gittikçe

azalarak bunun neden önemli olması gerektiğiyle ilgili farkındalıklarımız neredeyse körleşmiştir. Bu nedenle, bu gelişmelerin, insan onuru dediğimiz şeyi belirlememizi sağlayan değer anlayışımız üzerinde de oluşturduğu veya oluşturabileceği etkilerin üzerinde durmak ve bunlar üzerine düşünmek gerekmektedir.

1.3 Tezin Önemi

Araştırmamız, kişisel verilerin korunmasındaki en önemli sorunun, bireylerin hizmet almak için verdikleri veya gönüllü olarak sosyal medyada paylaştıkları kişisel verilerinin, hangi koşullarda korunduğu ve bunların hangi amaçlarla kullanıldığı konularında bilgi eksikliklerinin bulunması ve bunların öneminin yeterince fark edilememesi olduğunu ortaya koymaya çalışmaktadır. Kişisel verilerin korunması konusunda alınması gereken en önemli önlem, farkındalık kazandırmadır. Çünkü yapılan hiçbir hukuksal düzenleme ve alınacak hiçbir teknik önlem bilişim teknolojilerinin olanakları düşünüldüğünde veri gizliliğinin korunmasını mutlak olarak sağlayamamaktadır. Dolayısıyla her birey, kişi, yurttaş ya da ağdaş sosyal medyayı, yaptığı paylaşımlar yoluyla sağladığı verilerinin hangi amaçlarla kullanılabilme ihtimalinin olduğunun farkında olarak ve düşünerek kullanmalıdır. Tez çalışmamızda üzerinde duracağımız gibi, sadece bireysel ve küçük ölçekte bir bakış açısıyla değil, toplumsal ve büyük ölçekte bakış açısıyla konunun değerlendirilmesi gerekmektedir. Doğru değerlendirmelerin yapılabilmesi için ise bireylerin ve karar vericilerin bu konularla ilgili bilgi sahibi olması son derece önemlidir. Elbette sadece bilgi sahibi olmak değil, aynı zamanda bilginin kazandırdığı farkındalıkla eylemleri de bu yönde gerçekleştirmek gerekmektedir.

Sadece ülkemizde değil dünyanın tüm ülkelerinde kişisel verilerin gizliliği sorununun gündemde tutulması ve dijital etik ilkeler konusunda çalışmaların güçlendirilmesi, insanların diğer hak ve özgürlüklerinin korunması bakımından büyük önem taşımaktadır. Araştırmamız bu bağlamda, sosyal medyanın sağladığı, büyük kısmı kişisellik özelliği taşıyan verilerin kullanım amaçlarının değerlendirilmesinin ve veri gizliliğinin insan hakları için önemli bir gündem maddesi oluşturması gerektiğini ortaya koyması bakımından literatüre katkı sağlayacaktır.

2. KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

2.1. Kişisel Veri Kavramı

Kişisel veri *(personal data)* kavramını anlamak için öncelikle "kişisel" ve "veri" kavramlarının anlamlarını ele almak gerekmektedir.

"Kişisel" sözcüğü, kişiyle ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zatî anlamına gelir. Kişi ise, kadın veya erkeğe verilen genel ad, şahıs, zat, nefer olarak tanımlanmaktadır (Çevrimiçi Türk Dil Kurumu Sözlükleri, 2023)

Birçok dilde kişi kavramı, Latince "persona'' sözcüğünden türetilmiştir. Fransızcada "personne", Almancada "person" ve İngilizcede "person", İtalyancada ise "persona" kişi anlamına gelmektedir. Latincede "persona", Yunan ve Roma tiyatrolarında tiyatro oyuncularının kullandıkları her rol için değişmez biçimde belirlenmiş maskeleri ifade etmektedir. Rol yapmayı ifade eden bu kelime zamanla hayatta oynanan rolü ifade etmek üzere kişi anlamında kullanılmaya başlanmıştır (Ergün, 2017).

"Persona", Roma hukukunda da kullanılan bir terimdir/kavramdır. Bu kavram, Roma hukukunda bireyin hukuki rolünü, diğer bir deyişle, bireyin hayatta temsil ettiği hukuki durumu ifade edecek şekilde kullanılmıştır (Karaman, 2015). 743 sayılı Türk Kanunu Medenisinde ise kişi kelimesi yerine Arapça kökenli "şahıs" kelimesi kullanılmıştır. Şahıs; belirgin, tanınır hale gelme, yükselme, görünür olma, gitme, seyahat etme, bir halden başka hale gelme anlamlarını taşımaktadır (Ergün, 2017).

Doğal hukukta kişi olma açısından insanlar arasında bir ayırım yapılmamıştır ve her insan bir kişi olarak kabul edilmektedir. Pozitif hukukta da kişi, hak ehliyetine sahip varlıktır. Buna göre her insan, hak ve yükümlülüklerin öznesi olarak "kişi"dir (Ergün, 2017). Kişiler, gerçek kişiler ve tüzel kişiler olarak ikiye ayrılmaktadırlar. Gerçek kişiler hak ehliyetine sahip bireyleri ifade ederken, tüzel kişiler ise gerçek kişiler olmayıp hukuk tarafından oluşturulmuş kişilerdir. Tüzel kişiler, insanların bir amaca hizmet etmek için

bir araya gelerek oluşturdukları kişi ve mal topluluklarını ifade etmek için kullanılmaktadır.

"Veri" sözcüğü ise bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done ve bilişimde de olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak tanımlanmaktadır (Çevrimiçi Türk Dil Kurumu Sözlükleri, 2023). Veri *(data)* kelimesi Latincede verilen veya kabul edilen demektir ve Latince vermek anlamına gelen "dare"den türemiş "datum" sözcüğünün çoğuludur (Online Etymology Dictionary, 2023). Günümüzde kişisel veri kavramının ve bu verilerin korunmasının çok önemli hale gelmesi bilişim alanındaki gelişmeler ve verilerin dijital olarak kayıt altına alınmasıyla gerçekleşmiştir. Tezimizin ana konusunu sosyal medyadaki kişisel veriler oluşturmaktadır. Dolayısıyla veri kavramının bilişim alanındaki karşılığını ayrıca ele almak, bilgi, enformasyon ve veri arasındaki ayrıma değinmek gerekmektedir.

Türkçede bilgi sözcüğü, bazen İngilizceki "data" bazen "information" bazen de "knowledge" anlamlarında kullanılabilmektedir. Örneğin, kişisel verilerden söz edildiğinde kimi zaman veri, kimi zaman, bilgi veya enformasyon sözcükleri kullanılabilmektedir. En sık karşılaşılan karışıklık ise enformasyon *(information)* ve bilgi *(knowledge)* kavramlarının kullanımlarında ortaya çıkmaktadır. Felsefe tarihinde de bilgi kavramı çok farklı şekillerde tanımlanmıştır. Bilgi, "öznenin amaçlı yönelimi sonucunda, özneyle nesne arasında kurulan ilişkinin ürünü olan şey" olarak tanımlanmaktadır (Cevizci, 2005). "Bir şeyin ayırdına ya da bilincine varma, bir şeyle aktüel deneyim yoluyla kurulan yakınlık ya da tanışıklık, olgu, doğru ya da ödev olarak görülen bir şeye ilişkin açık algı, doğruluğu gerekli ve yeterli sayılan delillerle temellendirilmiş önermelerle ifade edilen bilinç içeriği" gibi tanımları da bulunmaktadır (Cevizci, 2005). İoanna Kuçuradi, bilginin (*knowledge),* her zaman "bir şeyin bilgisi" olduğunu ve bilme etkinliğinin veya bunun sonucunda ortaya çıkan şeyin insana özgü olduğunu vurgulamaktadır (Kuçuradi, 1995). Bilginin veya bilmenin insana ait bir etkinlik olması bilişim alanında da bilgi *(knowledge)* sözcüğünün kabul edildiği anlam açısından önemli bir noktadır. Türkçe literatürdeki bilişim alanında ve veri biliminde[1] *(data science)* veri

[1] Gökalp, vd. "Büyük Veri Çağında İşletmelerde Veri Bilimi" makalesinde veri bilimini, işletmede ortaya çıkan gerçek iş problemlerini verilerle anlamlandıran ve bu problemlere çözüm sunacak veri uygulamaları

anlamlandırma şeklinde de kullanılan, veri yığınlarının analiz edilmesiyle "anlamlı örüntüler *(meaningful patterns)* veya "anlaşılabilir örüntüler *(understandable patterns)* keşfetme" (Kuonen, 2004) işleminin hiyerarşik bir şekilde gerçekleştirilmesinde kullanılan DIKW *(data, information, knowledge, wisdom)* piramidini açıklamak konumuz açısından önemlidir. Tezimizde üzerinde önemle duracağımız büyük veri *(big data)* ve veri madenciliğinin *(data mining)* kavranabilmesi için bu ayrımları belirlemek gerekmektedir.

Bilgisayar sistemleri ile üretilen veri tek başına anlamsız olduğu için değersizdir. Bu veriler belli bir amaç için işlendiği zaman bir anlam kazanmaya başlamaktadır. Veri biliminde, büyük miktardaki veri yığınları kullanılarak yapılan veri madenciliğiyle amaçlanan, çeşitli analiz yöntemleriyle verilerdeki örüntüleri keşfederek bir anlam çıkarmak ve böylece ileriye yönelik durumsal öngörüler elde edebilmektir (Savaş, Topaloğlu ve Yılmaz, 2012). Sosyal medyadaki kişisel verilerin gizliliği sorunu da günümüzde kullanılan bu bilişim teknolojileriyle giderek büyümektedir. Bu nedenle tezimizde bilgi kavramının felsefi tartışmalarını açmadan kavramların bilişim alanındaki karşılıkları belirtilecektir. Fakat veri işleme yapılırken yapay zekâdan[2] yararlanılması da enformasyon ve bilgi arasındaki ayrımın felsefeciler tarafından günümüz bağlamında ayrıca ele alınmasını gerektirmektedir. Bilginin veya bilmenin insana özgü olduğunu ifade eden felsefi duruş ve tartışmalar, insan karşısında insan zekâsını taklit eden makinaların durumu konusunun değerlendirilmesinde oldukça önemlidir. Hukuk alanında "kişisel veri" olarak ifade edilen şeyler, daha sonra ayrıntılı olarak ele alacağımız gibi, büyük veri teknolojileri kullanıldığında kişisel enformasyon ve kişisel bilgi basamakları olarak da ifade edilebilen daha anlamlı biçimlere dönüştürülebilmektedir.

DIKW piramidinin en alt basamağı olan veri, enformasyonun temelini oluşturan, herhangi bir işlem yapılmayan, gözlem veya ölçüm yöntemleriyle elde edilen ham şekildeki her türlü değer olarak tanımlanmaktadır (Doğan ve Arslantekin 2016). Veriler, nesneleri, olayları veya onlarla ilgili nitelikleri temsil eden sembolleri içermektedir

geliştiren, içinde bilgisayar bilimleri, istatistik, matematik ve bilişim bilimleri dâhil olmak üzere birçok bilim dalını içeren disiplinlerarası bir çalışma alanı olarak tanımlamıştır.

[2] Öztemel, "Yapay Zekâ ve İnsanlığın Geleceği" makalesinde yapay zekâyı, zeki makineler, özellikle de zeki bilgisayar programları oluşturan bir bilim ve mühendislik dalı haline de gelen, insan zekâsının karakteristik özelliklerini bilgisayara kazandırmayı, algoritmalar geliştirmeyi ve problemlere insan gibi zeki davranışlar sergileyerek çözümler üretebilmeyi amaçlayan sistem olarak tanımlamıştır.

(Yılmaz, 2009). Bilgi sistemleriyle verinin üretimi, alınması ve işlenmesi sonrasında enformasyon ortaya çıkarılmaktadır. Veriler, enformasyona ve bilgiye dönüşmeleri için ilişkilendirilmeli, gruplandırılmalı, yorumlanmalı, anlamlandırılmalı ve analiz edilmelidir (Doğan ve Arslantekin, 2016).

Veriler, bir karar sürecinde kullanılmaları gerektiğinde öncelikle iletişim bilgisi olarak da ifade edilebilecek enformasyona dönüştürülmektedir (Kuonen, 2004). Davenport ve Prusak enformasyonu bir mesaj olarak algılayarak "genellikle belge şeklinde ya da görsel ve işitsel mesaj" biçiminde tanımlamaktadır (Davenport ve Prusak, 2001 akt. Yılmaz, 2009). Enformasyon, iletişim olgusuna dayanmakta, iletişim olgusunu da alınan mesajın enformasyon niteliği taşıyıp taşımadığı belirlemektedir. Bilgi ise zihinde oluşan, deneyimlerin, değerlerin ve enformasyonun bir amaca yönelik olarak bir araya getirilip değerlendirilmesi için çerçeve oluşturan esnek bir bileşim olarak tanımlanmaktadır. Buna göre bilgi, bilenlerin zihinlerinde ortaya çıkan birçok enformasyonun, deneyimin ve öğrenmenin bileşimidir (Davenport ve Prusak, 2001, akt. Yılmaz, 2009).

DIKW piramidinin en üst basamağı olan bilgelik *(wisdom)* ise ileriyi görebilme, doğru değerlendirme ve karar verme konusunda bilginin nasıl kullanılacağına ilişkin anlayış kazanma durumu olarak ifade edilmektedir. Bilişimde DIWK piramidinin veriden bilgiye doğru giden aşamalarını, harflerin belirli bir düzende biçimlenmesiyle ortaya çıkan bir cümleyi okurken, harflerin düzeninin anlam kazanarak kelimelere dönüşmesine, kelimelerin gramer kurallarıyla birleşip bütünleşerek cümlenin anlamının ortaya çıkmasına ve bu cümlenin anlamının bizi düşündürmesine benzetebiliriz (Köse, 2023)[3] Burada vurgulanmak istenen noktalar, bu hiyerarşide verinin giderek daha fazla anlam kazanması ve bir noktada insana özgü zihinsel işlemlerin öne çıkmasıdır. Kişisel veri bağlamında düşündüğümüzde bir kişinin internetteki hareketleri söz konusu olduğunda, örneğin kişinin adı ve girdiği sitelerin adları birer veriyken, kişinin ilgilendiği sitelere göre reklam gösterilmesi için bu verinin işlenerek, "X kişisi Y sitesine giriş yapar" şeklinde düzenlenmesi, verinin enformasyon haline getirilmesine örnek olarak verilebilir. Bilişimdeki veri işleme sürecinde bir verinin yapay zekâ teknolojileriyle bu piramide göre hangi noktaya ulaşabileceği tartışmalı bir konu olduğu ve bunu belirlemek uzmanlık

[3] Bkz. "DIWK Piramidi", Temel Bilgi Teknolojileri II (PowerPoint Slayt).

gerektirdiği için tezimizde genellikle veri kelimesiyle birlikte enformasyon sözcüğünün kullanımı tercih edilecektir.

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Bu tanım, ülkemizin 6698 sayılı Kişisel Verilerin Korunması Kanununda da (KVKK) yer alan tanımdır. Kişisel veriye ilişkin olarak bu alanda yapılan ilk tanımlamalar , OECD'nin 1980 tarihli Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri, 1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve 1995 tarihli 95/46/EC sayılı Veri Koruma Direktifinde yapılmıştır.

OECD (Organisation for Economic Co-operation and Development), 1980 yılında, kişisel veriyi "belirli veya belirlenebilir bir kişiye ait herhangi bilgi", 108 Sayılı Sözleşmede "kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler" olarak tanımlamıştır.[4] Avrupa Birliği Konseyi ve Avrupa Parlamentosu Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması 95/46/EC Direktifinde ise daha ayrıntılı bir kişisel veri tanımı karşımıza çıkmaktadır. Bu Direktifte kişisel veri, "fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir" şeklinde tanımlanmıştır.[5] Bu açıklamalar doğrultusunda, kişinin fiziksel özellikleri, kimlik bilgileri, fotoğrafı, görüntü ve ses kayıtları, sağlık kayıtları, parmak izi, öğrenim durumuna ilişkin bilgiler, mesleği, etnik kökeni, dini inancı, banka hesap bilgileri, kullandığı bilgisayarın IP adresi gibi veriler, kişisel veri olarak kabul edilmektedir.

Tanımlamalarda yer alan "gerçek kişi" ifadesi tüzel kişilerle ilgili verilerin kişisel veri kapsamına girmediğini belirtmektedir. Gerçek bir kişiyle ilişkilendirilebilecek durumlar dışında örneğin, bir şirketin adı veya adresi gibi bilgiler kişisel veri sayılmamaktadır. Nelerin kişisel veri olduğunun belirlenmesinde önem taşıyan iki nokta şöyle belirlenebilir. Bunlar, verinin gerçek kişiye ait olması ve kişiyi belirli ya da belirlenebilir

[4] Bkz. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
[5] Bkz. 95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi

kılmasıdır. Bir veri, kişinin kimliğini doğrudan belirleyebildiği gibi, başka kayıtlarla ilişkilendirilerek dolaylı yoldan da belirleyebilir. Bu şekildeki dolaylı yoldan belirleme yapılabilen veriler de kişisel veri kapsamındadır. Kişisel veri tanımında yer alan "her türlü bilgi" ifadesi ise kişisel veri kapsamını oldukça genişletmektedir. Ad-soyad, doğum yeri ve tarihi, kimlik numarası, parmak izi, e-posta adresi, fotoğraf-ses kayıtları gibi verilerin yanı sıra tercihler, hobiler, etkileşimde bulunulan insanlar, aileye ilişkin bilgiler gibi veriler de kişisel veri olarak kabul edilebilir. Bu verilerin kişisel veri olarak kabul edilmesi, verinin kişi ile ilişkilendirilebiliyor olması ve o kişiyi belirlenebilir hale getirmesi anlamına gelir. Kanunda kişisel veriler sınırlı sayım yoluyla belirtilmiştir. Bu nedenle kişisel veri kapsamına giren veriler belirtilen ölçütlere göre "o kişiyi tanımlayabilme" gücü göz önüne alınarak belirlenmektedir.[6]

Kişisel veriler ayrıca hassas veri ve hassas olmayan veri olarak ikiye ayrılmaktadır. Hassas veriler başkaları tarafından bilinmesi durumunda bireylere zarar verebilecek olan ve bu nedenle korunması gereken en önemli verilerdir. Hassas olmayan veriler ise paylaşılması durumunda kişiye zarar vermeyeceği kabul edilen verilerdir.[7]

2.1.1 Hassas veriler (Özel nitelikli kişisel veriler)

Avrupa Birliği (AB), kişisel verilerin korunmasına ilişkin 1995 yılında yayımlanan Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/EC sayılı Direktifi kabul etmiştir. Direktifin temel amacı, Avrupa Birliği ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlu hale getirilmesidir. Ülkemizin 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) da temel olarak bu Direktif esas alınarak hazırlanmıştır.

95/46/EC sayılı Direktifin giriş bölümümün 33. maddesinde hassas verilere yönelik olarak "Veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir; ancak, temel özgürlüklerin yerine getirilmesine izin verecek amaçlar için, bazı derneklerin veya vakıfların meşru faaliyetleri esnasında veya mesleki gizlilik hakkındaki yasal bir yükümlülüğe tabi kişiler tarafından bu verilerin sağlık amaçları için kullanılması durumunda; bu yasaklamaya uymama

[6] Bkz. Kişisel Verileri Koruma Kurumu, "100 Soruda Kişisel Verilerin Korunması Kanunu"
[7] Bkz. Kişisel Verileri Koruma Kurumu, "Özel Nitelikli Kişisel Verilerin İşlenme Şartları"

durumu açıkça belirtilmelidir" ifadesi yer almaktadır. 3. Kısım 8. maddede "Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır" hükmü yer almaktadır.[8]

07 Nisan 2016 tarihinde yayımlanan KVKK'nun 6. maddesinde hassas veriler "özel nitelikli kişisel veriler" ifadesiyle "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir" şeklinde tanımlanmıştır (KVKK, 6. Madde)

Hassas verileri, bireyin temel hak ve özgürlüklerine sıkı sıkıya bağlı, kişinin etnik kökeni, düşünce ve inançları, sağlık verileri gibi ayırımcılığa uğramasına, nefret odağı olmasına neden olabilecek tehlikeli ve dolayısıyla kişinin mağdur olmaması için özel olarak korunması gereken veriler olarak ifade edebiliriz. Bu kişisel veriler, ilgili kişinin açık rızasıyla ya da kanunda sayılan sınırlı hallerde işlenebilirler. Kanuna göre, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilmektedir.[9]

2.1.2 Hassas Olmayan Veriler

Türk Medeni Kanununun 24. maddesinde "Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır" hükmü yer almaktadır (TMK, 24. Madde). İşlendikleri takdirde kişilik haklarının ihlali söz konusu olmayan, kişisel veri kapsamında

[8] Bkz. 95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi
[9] Bkz. Kişisel Verileri Koruma Kurumu, "Özel Nitelikli Kişisel Verilerin İşlenme Şartları"

olup paylaşılması veya kayıt altına alınması kişiyi mağdur etmeyen veya ayırımcılık tehlikesiyle karşı karşıya getirmeyen bilgiler hassas olmayan veriler olarak tanımlanabilir.

Hassas olmayan veriler, özel nitelikli kişisel veriler dışında kalan veriler şeklinde nitelendirilerek belirlenebilmektedir. Hassas olmayan verilerin işlenmesine yönelik yasal düzenlemeler KVKK'ndaki hükümlerden ziyade daha çok genel hukuk kapsamında işlenebilmektedir. Hangi bilginin hassas kişisel veri veya hassas olmayan kişisel veri kapsamında olduğu zamana ve mekâna göre değişebilmektedir (Arınmış Uzun, 2021). Bu kapsamda hassas olmayan verilerin işlenmesinin yasal olarak düzenlenmesinin de belirsizlikleri ortadan kaldırabilmek açısından önemli bir konu olduğu ifade edilebilir.

Kişisel verilerin hukuka uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren nedenlerin ortadan kalkması halinde bu veriler, doğrudan ya da ilgili kişinin isteği üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

2.1.3 Kişisel verilerin toplanması ve işlenmesi

Kişisel verilerin toplanması, kişiye ait her tür bilginin herhangi bir şekilde edinilmesini ifade eder. Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, kişisel verilerin işlenmesi olarak kabul edilmektedir. Kişisel verilerin belirtilen şekilde toplandıktan sonra silinmesi, yok edilmesi ya da anonim hale getirilmesine kadar olan işlemler sırasında gerçekleştirilen her türlü faaliyet Kanun kapsamında kişisel verilerin işlenmesi olarak değerlendirilmektedir.[10]

Bir kişisel verinin sadece dijital bir ortamda depolanması başka hiçbir işlem yapılmasa dahi o verinin işlenmesi faaliyeti kapsamına girer. Kişisel verinin ilk kez elde edildiği andan başlayarak yapılan her işlem veri işlemedir. Bilişim sistemleri üzerinden gerçekleşmeyen, başka bir anlatımla, otomatik olarak yapılmayan kayıtlar, eğer bir veri

[10] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenme Şartları"

kayıt sistemi ya da sistematik bir dosyalama sistemi varsa, veri işleme faaliyetine dâhildir ve bu veriler kişisel veri olarak kabul edilir. Örneğin, bir kâğıda gelişi güzel yazılmış ad-soyad bilgisi kişisel veri değilken, sistematik bir şekilde kaydedilmesi durumunda bu veri, kişisel veri olarak veri işleme faaliyeti kapsamına girer.[11]

2.1.4 Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi

"Kişisel Verileri Koruma Kurumu'nun Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkındaki Yönetmelik"e göre, kişisel veriler hukuka uygun olarak işlense de, kanunda kişisel verilerin işlenme koşullarının tamamının ortadan kalkması halinde bu veriler, doğrudan veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir. Veri sorumlusu ise, kişisel verilerin işleme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Veri işleme faaliyetinin gerçekleştirilmesi açısından kanunda gerçek kişi ve tüzel kişi ayırımı yapılmamıştır.

Kişisel Verileri Koruma Kurumu tarafından bu işlemler şu şekilde açıklanmıştır:

> "*Kişisel verilerin silinmesi*, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir."Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in 4. maddesinde ilgili kullanıcı; "verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler" olarak tanımlanmıştır. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.
>
> *Kişisel verilerin yok edilmesi*, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

[11] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenme Şartları" .

Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Belirtmek gerekir ki, işlenmesini gerektiren sebeplerin ortadan kalkması durumunda kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi, kişisel verilerin işlenmesine hâkim olan genel ilkelerin doğal bir sonucudur. Yukarıda belirtildiği üzere, Kanunun 4. maddesinde kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilebileceği öngörülmüştür. Kişisel verilerin muhafazası için herhangi bir meşru amaç kalmadığında bu verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi bir zorunluluktur. Kanunun 7. maddesinin ikinci fıkrasında, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulması öngörülmektedir. Bu kapsamda, örneğin Adli Sicil Kanununda verilerin silinmesini veya yok edilmesini düzenleyen hükümler Kanuna göre öncelikli olarak uygulanacaktır” [12]

Tezimizin daha sonraki bölümlerinde ele alacağımız gibi sosyal medyadaki kişisel verilerin gizliliği konusunda verilerin başka verilerle desteklenerek analiz edilmesi sonucunda anonimleşmenin güçleşmesi bu alanda yaşanan sorunlardan biridir. Sosyal medyadaki verilerin analiz edilmesiyle kişilerin verilerinin birleştirilerek profillerinin çıkarılabilmesi ve hassas veriler olarak sıralanan özelliklerinin belirlenebilmesi

[12] Bkz. Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi” .

olanaklıdır. Bu durum ayırımcılığa ve fırsat eşitliğinin bozulmasına neden olabileceği için veri gizliliğinin sağlanması insan hakları bağlamında yaşamsal önem taşımaktadır.

2.2 Kişisel Verilerin Korunması Hakkının Tarihsel ve Hukuki Boyutu

Tarihsel yolculukta, birey veya insanın değeri üzerine fikirlerin felsefi düşünce dünyasında öne çıkmasıyla birlikte "mahremiyet veya özel hayat" *(privacy)* kavramları da önemsenmeye başlanmıştır. Modern toplumsal yapının oluşmasıyla birlikte bir problem alanı olarak görülmeye başlanan ve insani bir gereksinim olarak talep edilen özel hayat veya mahremiyet kavrayışı da teknolojik gelişmelerle birlikte insan dünyasındaki anlamı ve değeri bakımından dönüşmüştür ve bu dönüşüm devam etmektedir.

Özel hayat, insanların yalnız kalma, başka kimselerle diğerlerinin müdahalesiyle gözetimi olmadan ilişki kurabilme ve kişisel olarak tanınmadan ya da dikkat çekmeden kamu yaşamına katılma istekleri nedeniyle ihtiyaç duydukları bir alan olarak tanımlanmaktadır. İnsan, zaman zaman yalnızlığa çekilme aynı zamanda diğerleriyle iletişim kurma ve paylaşımda bulunma ihtiyacı duyan bir varlıktır. Dolayısıyla özel hayat, bireylere kamu yaşamına katılıp katılmama veya bu yaşama nasıl ve ne düzeyde katılacaklarına karar verebilme olanağı tanımak anlamına gelmektedir (Yüksel, 2003). Antoine Prost, özel hayatın doğal bir gerçeklik olmadığını ve her toplumun farklı bir şekilde kurduğu tarihsel bir gerçeklik şeklinde ortaya çıktığını ifade etmektedir. Özel hayatın sınırlarını kesin olarak belirlemek mümkün değildir (Prost, 2008, s. 15).

19. Yüzyıl sonunda Amerika Birleşik Devletleri'nde (ABD) mahremiyet veya özel hayat hakkı, kişilik hakları kapsamında pozitif hukuk düzenlemeleri yoluyla tanınmış ve çerçevesi çizilmeye başlanmıştır. Bunun en önemli nedenlerinden biri bu dönemlerde anında fotoğraflama teknolojisinin gelişmesinin yanı sıra, gazetecilik alanında sansasyonel yayıncılığın başlaması olmuştur. İnsanlar bu yolla haberleri ya da izinleri olmadan fotoğraflanmaya başlandığında, söz konusu sansasyonel habercilikten zarar görmüş olan iki Amerikalı avukat, Samuel D. Warren ve Louis D. Branders 1890 yılında "Mahremiyet Hakkı" adında bir makale kaleme alarak hukuk dünyasında devrimsel nitelikte bir bakış açısı ortaya koymuşlardır. Mahremiyeti ilk kez başlı başına bir kavram olarak ele almış, özel mülkiyet hakkı kapsamında görülen birtakım özgürlükleri ilk kez mahremiyet hakkı olarak belirlemişlerdir (Yüksel, 2003).

Aydınlanma çağında öne çıkan birtakım felsefi bakış açılarının yanı sıra, modern bilimdeki ilerlemelerle kendini gösteren teknolojik gelişmenin yarattığı mahremiyet sorunu, hukuki düzenlemelerin oluşturulmasının ilk kıvılcımı olmuştur. Bugün de internet devrimiyle ortaya çıkan sosyal ağlar ve bu ağların kullanımının günlük rutinin bir parçası haline gelmesi, mahremiyet sorununun daha çok bir "veri mahremiyeti" *(data privacy)* sorununa dönüşmesine neden olmuştur. Ayrıca kişisel verilerin bilişim sistemleri tarafından kaydedilmesi, saklanması, işlenmesi, aktarılması ve çözümlenmeleri resmi ya da özel çeşitli işlerin görülebilmesinin vazgeçilmez unsurları haline gelmiştir.

Kişilerin, kendilerine ve/veya başkalarına ait, sınırlı sayıda insanın ya da sadece kendilerinin bilebileceği, "sır" adı verilen gizli kalması gereken bilgileri vardır. Sır ve kişisel veriler gizli kalması istenen bilgiler olmaları bakımından özellikleri birbirine benzeyen kavramladır. Ancak sırrın kapsamı kişisel veriden geniştir. Kişisel veri, kişiyi belirlenebilir kılan şeylerken, sırlar bu veriler dışında kalan özel hayat verilerini de içermektedir. Kişisel veri ve özel hayat verilerini içeren sırların gizliliği sorunu temelde insanın merak duygusu ve bilme isteğinden kaynaklanmaktadır.

Aristoteles *Metafizik* adlı eserinde duyumların, özellikle görsel duyumların verdiği hazzı, insanın merak duygusu ve bilme isteğine bağlamaktadır:

> Bütün insanlar doğal olarak bilmek isterler. Duyumların verdiği zevk, bunun bir kanıtıdır. Çünkü onlar, özellikle de diğerlerinden fazla olarak görsel duyumlar, faydaları dışında bizzat kendileri bakımından bize zevk verirler. Gerçekten, sadece eylemle ilgili olarak değil, herhangi bir eylemde bulunmayı düşünmediğimizde de görmeyi, genel olarak, bütün geri kalanlarına tercih ederiz (Aristoteles, 1996, 980a-980b).

Bilmek, bildiğimiz şey üzerinde denetim sahibi olmamızı da sağlar. Francis Bacon'ın "Bilgi güçtür" anlayışı, egemen olma isteğine dayanmaktadır. İnsan doğayı anlayarak ona hükmetmektedir (Bacon, 2012). İnsanlar bilmedikleri şeyler karşısında kendilerini güvensiz hissederler. Egemenliği ve güvenliği sağlamak isteyen iktidarlar da bu nedenle kişilerle ilgili bilgi sahibi olmak ve onları gözetlemek, denetim altında tutmak isterler. Gözetleme, tarih boyunca farklı şekillerde bireyler üzerinde varlığını hissettirmiştir. Bilişimdeki ve teknolojideki gelişmelerle gözetim ve kayıt altına alma olanakları artmış

ve gelişmiştir. Kişisel verilerin bilişim sistemleri tarafından kaydedilmesi, saklanması, işlenmesi, aktarılması ve analiz edilmeleri ya da çözümlenmeleri, kişilerin başta mahremiyet olmak üzere temel hakları ve bunlarla ilişkili haklarının korunması konusunda endişelere neden olmaktadır.

2.2.1 Özel hayatın gizliliğinin korunmasıyla ilgili uluslararası düzenlemeler

Kişisel veri gizliliğinin temelini oluşturan uluslararası düzenlemelerin ilki, II. Dünya Savaşından sonra Birleşmiş Milletler tarafından temel hakları güvence alan ve uluslararası barış ve güvenliği sağlama amacıyla hazırlanan 1948 tarihli "İnsan Hakları Evrensel Bildirgesi"dir. Bildirgenin 12. maddesinde şu ifade yer almaktadır*: "Hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır"* (İHEB, 12. Madde).

Türkiye, söz konusu Bildirgeyi 1949 yılında kabul etmiştir.[13] Avrupa İnsan Hakları Konseyi, 1953 yılında "Avrupa İnsan Hakları Sözleşmesi"ni (AİHS) aynı amaçlar doğrultusunda yürürlüğe koymuştur. Sözleşmenin 8. maddesinde şu ifade yer almaktadır*:*

> Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. (AİHS, 8. Madde).

Türkiye 1954 yılında Sözleşmeyi onaylamıştır. Taraf ülkelerin AİHS'ne uyumunu denetlemek için Avrupa İnsan Hakları Mahkemesi (AİHM) oluşturulmuştur. Türkiye AİHS'nin denetim sürecine bireysel başvuru hakkını 1987'de ve AİHM'nin zorunlu yargı yetkisini 1990'da kabul etmiştir.[14]

[13] Bkz. 7217 Sayılı Resmi Gazete
[14] Bkz. T.C Dışişleri Bakanlığı, "Avrupa Konseyi (AK)"

1976 tarihinde yürürlüğe giren "Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme"nin 17. maddesinde özel hayatın gizliliği şu ifadeyle korunmuştur: *"Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz. Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır"*(BM Medeni ve Siyasi Haklara İlişkin Sözleşme, 17. Madde)

Türkiye, Sözleşmeye ilişkin olarak üç beyanda bulunmuş ve 27. maddeye çekince koyarak 2003 yılında onaylamıştır.[15]

Birleşmiş Milletler ve Avrupa Konseyinin temel haklara yönelik olarak hazırladığı bildirge ve sözleşme maddelerinde kişilerin özel hayatının, aile hayatının, ev hayatının ve yazışmalarının korunması amaçlanmıştır ve henüz kişisel verilerin korunmasıyla ilgili konular bilişimdeki gelişmelerin yaşandığı tarihsel sürecin henüz başlamaması veya hızlanmaması nedeniyle başlı başına bir temel hak olarak gündemde olmadığı için özel hayatın gizliliği kapsamında yalnızca değerlendirilmiştir.

2.2.2 Kişisel verilerin korunmasıyla ilgili uluslararası düzenlemeler

1970'li yıllardan bu yana, ulusal ve uluslararası düzenlemeler yoluyla kişisel verilerin korunmasına yönelik çalışmalar yürütülmektedir. Bu alanda ilk düzenleme 1970 tarihli Almanya'nın Hessen Eyaletinde kabul edilen veri koruma yasasıdır. Bu yasa, bilişim sistemleri yardımıyla tapu kayıtlarına erişim sağlanabilmesi karşısında, verilerin elde edilmesi ve depolanmasına ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.[16] Böylece ulusal anlamda ilk veri koruma yasası olan 1970 tarihli "Hessen Eyalet Veri Koruma Kanunu" düzenlenmiştir. Bu yasayı, 1973 tarihli İsveç ve 1978 tarihli Fransa veri koruma yasaları takip etmiştir. Ulusal düzenlemelerin yapılmaya başlandığı 1970'li yıllardan sonra 1980'li yıllarda OECD, Avrupa Konseyi ve Avrupa Birliğinin uluslararası düzenlemeleri ortaya çıkmıştır.

[15] Bkz. İnsan Hakları ve Eşitlik Uzmanları Derneği, "Birleşmiş Milletler İnsan Hakları Sözleşmeleri"
[16] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi"

2.2.2.1 OECD rehber ilkeleri

Organisation for Economic Co-Operation and Development (OECD), Türkçe karşılığıyla Ekonomik İşbirliği ve Kalkınma Örgütü, 1960 yılında "Paris Sözleşmesi"nin imzalanmasından sonra 1961 yılında Avrupa'nın özgürlükleri korumak, ekonomik güç ve refah düzeyini yükselterek kalkınmasını sağlamak amacıyla kurulmuştur. Kurucu üyeleri arasında Türkiye'nin de bulunduğu bu örgütün kuruluş amaçlarından biri de teknolojik gelişmelerin desteklenmesidir. Bilişimde yaşanan gelişmelerin ardından 1980 yılında OECD, "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri"ni kabul ederek uluslararası alanda kişisel verilerin korunması konusundaki ilk adımı atmıştır. Hükümetlere tavsiye niteliğinde olan bu rehber ilkelerin bağlayıcılığı bulunmasa da kişisel verilerin korunması amacıyla üye devletleri harekete geçiren ilk uluslararası düzenleme olması bakımından büyük önem taşımaktadır.

OECD Rehber İlkeleri, kişisel verilerin korunmasında sekiz temel ilke belirlemiştir. Bunlar, "veri toplamanın sınırlılığı ilkesi", "veri kalitesi ilkesi", "amaca özgülük ilkesi", "sınırlı kullanım ilkesi", "güvenlik tedbirleri ilkesi", "açıklık ilkesi", "bireyin katılımı ilkesi" ve "hesap verilebilirlik ilkesi"dir.[17] OECD, 2013 yılında, veri ihlallerinde bildirim yükümlülüğü, rıza kavramı, veri sorumlularının kişisel verilerin sınırlararası veri akışı bağlamında sorumlu tutulması konularıyla ilgili belirlemeleri de yapmıştır (Uyarer, 2019, s. 26).

2.2.2.2 Avrupa Konseyi düzenlemeleri

Elektronik veri işletim sistemlerindeki gelişmelerle 1970'li yıllardan itibaren yapılan çalışmaların sonucunda Avrupa Konseyi, 1981 yılında Strasburg'da 108 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ni imzaya açmış ve bu Sözleşme 1985 yılında yürürlüğe girmiştir. Türkiye bu Sözleşmeyi 1981 yılında ilk imzalayan ülkelerden biri olmasına rağmen, Sözleşme yaklaşık otuz beş yıl sonra 17 Mart 2016 tarihinde iç hukuka dâhil etmiştir. 108 sayılı Sözleşme olarak da bilinen Sözleşmenin temel amacı her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle

[17] Bkz. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

kendilerini ilgilendiren kişisel nitelikteki verilerinin otomatik yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır. Bu Sözleşme ile birlikte, otomatik işlemeye konu olan kişisel verilerin, "adil bir biçimde ve yasal yoldan elde edilip işlenmesi", "belirli ve meşru amaçlar için kaydedilmesi ve bu amaçlara aykırı kullanılmaması", "kaydedilmelerinin amaçlara uygun ve yerinde olması ve aşırı olmaması", "doğru olmaları ve gerektiğinde güncellenmeleri gerektiği", "ilgili kişilerin kimliklerini belirlemeye, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde imkân verecek bir biçimde saklanması" ilkeleri düzenlenmiştir (Dülger, 2019).

2001 yılında, taraf devletlerin ülkelerinde uygulanmak üzere kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici makam kurmayı taahhüt ettiği 181 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol" kabul edilmiştir. Türkiye Protokolü 8 Kasım 2001 tarihinde imzalamış ve 5 Mayıs 2016 tarihinde iç hukuka dâhil etmiştir (Kişisel Verileri Koruma Kurumu, 2023).[18]

2.2.2.3 Avrupa Birliği düzenlemeleri

Avrupa Birliği, üyelerinin kişisel verilerin korunmasıyla ilgili yapacakları düzenlemeleri uyumlu hale getirmek amacıyla 1995 yılında 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif"i kabul etmiştir. AB üyesi ülkelerin, kişisel verilerin korunmasına ilişkin kanuni düzenlemeleri bu Direktife dayanmaktadır. Direktif, 108 No'lu Sözleşme ve ulusal hukuklarda yer alan ilkeleri yansıtmakta ve çoğunlukla bu ilkeleri ayrıntılandırmaktadır. Direktifte temel olarak benimsenmiş ilkeler, "kişisel verilerin açık, belirli ve meşru amaçlar için toplanması", "orantılılık", "güvenlik" ve "veri işlemenin denetime tabi olması"dır. Ayrıca, Direktif ve 108 No'lu Sözleşme arasında da olumlu bir etkileşim vardır (Dülger, 2019). Kişisel verilerin, "hukuka ve dürüstlük kuralına uygun bir şekilde önceden belirlenen açık ve hukuka uygun amaçlar için, ölçülü doğru ve gerektiğinde

[18] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi"

güncellenecek şekilde işlenmesi gerektiği" belirtilmiştir.[19] Türkiye'ye ait 6698 sayılı "Kişisel Verilerin Korunması Kanunu" da büyük ölçüde bu Direktif esas alınarak hazırlanmıştır. 2002 yılında ise elektronik haberleşme alanında kişisel verilerin korunması amacıyla 95/46/EC sayılı Direktife dayanan 2002/58/EC sayılı "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif" çıkarılmıştır (Kişisel Verileri Koruma Kurumu, 2023).[20]

2012 yılında değişen ve gelişen teknolojinin getirdiği yenilikler ve bu yeniliklerin korunması istenen haklar konusunda doğurduğu riskler nedeniyle yeni bir çalışma başlatılmıştır. Avrupa Birliği Komisyonu, bu ihtiyaçları göz önünde bulundurarak 95/46/EC sayılı Direktifte kapsamlı değişiklikler yapılmasını içeren bir öneri hazırlamıştır. Böylece Direktifin eksikliklerini gideren "2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü" (General Data Protection Regulation-GDPR), Avrupa Birliği tarafından 2016 yılında kabul edilmiş ve 25 Mayıs 2018 tarihinden itibaren 95/46/EC sayılı Direktifi ilga ederek uygulanmaya başlamıştır (Dülger, 2019). Bu düzenlemenin direktif değil de tüzük şeklinde oluşturulması yapılan düzenlemenin AB ülkeleri için hukuken bağlayıcılık taşıması açısından önemlidir. Direktifler, o hukuki düzenlemeyle elde edilmesi beklenen temel hedefleri ortaya koymakta ancak söz konusu hedeflere ulaşılmasına ilişkin araçların seçimini üye devletlerin kendi iç hukuklarına bırakmaktadır. Tüzüklerin ise üye ülkelerde doğrudan uygulanması mümkündür ve herhangi bir iç hukuk düzenlemesi yapılmasını gerektirmemektedir (Akıncı, 2017).

GDPR'nin, Direktif ile karşılaştırıldığında önemli değişiklikler getirdiği görülmektedir. GDPR'de, verilerin işlenmesi hususunda güçlendirilmiş rıza, veri işleyenlerin tamamının veri işlemeden sorumlu tutulması, riskli hallerde zorunlu veri koruma etki değerlendirmesinin yapılması, veri ihlali riskinin yüksek olması durumunda bildirimde bulunma zorunluluğu ve yükümlülükleri ihlal durumunda ağır yaptırımlar uygulanması gibi mekanizmalar öngörülmüş ve unutulma hakkı ile veri taşınabilirliği hakkı da belirlenmiştir. Dolayısıyla Tüzük kişinin kendi verileri üzerinde sahip olduğu denetimi güçlendirirken veri sorumlularıyla veri işleyenlerin yükümlülüklerini ağırlaştırmıştır.

[19] Bkz. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[20] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanunu ve Uygulaması"

Avrupa Birliği, GDPR'nin kapsamını, üye ülkelerden daha geniş tutmaktadır. Avrupa Birliğinde ikamet eden, ürün, hizmet veya denetim gibi herhangi bir nedenle AB'ye üye ülkelerden geçen kişisel verilerin üye olmayan ülkelerle temasının olması halinde Tüzük, o ülkeler için de bağlayıcıdır. Böylece AB ile ilişkili verilerin, kişisel verilerin korunması hakkının düzenlenmediği, eksik veya dar bir koruma sağlandığı ülkeler açısından da güvence altına alınması amaçlanmıştır. GDPR'nin, dijital dünyada verilerin korunması sorunuyla ilgili birçok probleme çözüm getirdiği düşünülmektedir. Aynı zamanda kişisel verileri koruma düzeyinin arttırılmasının, büyük veri *(big data)* alanında ve her cihazın internete bağlanabilmesini sağlayacak nesnelerin interneti olarak adlandırılan Web 4.0 hizmetlerinde yaratılabilecek birçok fırsatı engelleyebileceği de değerlendirilmektedir (Ekin, 2020, s. 38-40).

2.2.3 Kişisel verilerin korunmasıyla ilgili ulusal düzenlemeler

2.2.3.1 Türkiye Cumhuriyeti Anayasası

Kişisel verilerin korunmasını isteme hakkı bir anayasal haktır. Türkiye Cumhuriyeti Anayasasının temel hak ve ödevlerin düzenlendiği ikinci kısmının özel hayatın gizliliği ve korunmasına ilişkin 20. maddesinde şöyle denilmektedir:

> Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli Güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde el koyma kendiliğinden kalkar (T.C Anayasa, 20. Madde).

2010 yılında 5982 sayılı Kanun ile yapılan Anayasa değişikliği sayesinde Anayasanın 20. maddesine bir fıkra eklenerek kişisel veriler, özel hayatın gizliliği ve korunması hakkı

kapsamında anayasal güvence altına alınmıştır. Anayasanın 20. maddesindeki Ek fıkra, veri sahibinin haklarını da belirterek şöyle ifade edilmiştir: *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"*(T.C Anayasa, 20. Madde).

Anayasada yer verilen bu düzenlemeyle herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirlenmiştir. Kişiler kendisiyle ilgili kişisel veriler hakkında bilgilendirme, bu verilere erişme, bunların ne amaçla kullanıldığını öğrenme ve bunların düzeltilmesini veya silinmesini isteme hakkına sahiptir. Bu verilerin sadece kanunda öngörülen hallerde ve kişilerin açık rızasıyla işlenebileceği hükme bağlanmıştır (Kişisel Verileri Koruma Kurumu, 2023).[21]

2.2.3.2 5237 Sayılı Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanununda (TCK) kişisel verilerin kaydedilmesi suç olarak düzenlenmiştir. TCK'nın 135. maddesinde şu hüküm yer almaktadır:

> Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır (TCK, 135. Madde).

TCK'nın 136. maddesinde ise şu ifadeye yer verilerek verileri hukuka aykırı olarak verme, paylaşma veya ele geçirme suç olarak düzenlenmiştir: *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır"* (TCK, 136. Madde). Aynı kanunun 138. maddesinde şu ifadeye yer verilerek verileri yok etmeme fiilleri de suç olarak düzenlenmiştir*:*

[21] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması alanında Uluslararası ve Ulusal Düzenlemeler"

"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir"(TCK, 138. Madde). Kanunun 140. maddesinde ise bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik önlemlerinin uygulanacağı belirtilmiştir (TCK, 140. Madde).

2.2.3.3 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Türkiye'de kişisel verilerin korunması konusunda yasal düzenlemeler yapılmasıyla ilgili çalışmalar 1981 yılında başlamıştır. Türkiye, 28 Ocak 1981 tarihinde "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ni imzalayan ilk ülkelerden biri olmuştur. Sözleşmenin imzalanmasının ardından birtakım çalışmalar yapılmış, konuya ilişkin düzenlemeler getirilmiştir. Türkiye'de kişisel verilerin korunmasına ilişkin ayrı bir kanun çıkarmak için ilk kez 1989 yılında, ardından da 2000 yılında birer komisyon oluşturulmuştur. 1989 yılındaki komisyon, çalışmalarını tamamlayamadan dağılmıştır. 2000 yılında kurulan komisyon ise üç yıllık bir çalışmanın sonunda bir kanun tasarısı hazırlamıştır. Fakat hazırlanan tasarı yasalaşamamıştır. 108 No'lu Sözleşme ise imzalandıktan yıllar sonra 17 Mart 2016 tarihinde 29656 sayılı *Resmî Gazete*'de yayımlanarak iç hukuka dahil edilmiştir. Bunun ardından, 26 Aralık 2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı 24 Mart 2016 tarihinde kabul edilerek yasalaşmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı *Resmî Gazete*'de yayımlanarak yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2023).[22]

"Kişisel Verileri Koruma Kanunu"nun amacı, 1. maddesinde belirtildiği gibi kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleriyle uyacakları usul ve esasları düzenlemektir. 2. Maddesinde ise kanun hükümlerinin kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik

[22] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması alanında Uluslararası ve Ulusal Düzenlemeler"

olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı belirtilerek kanunun kapsamı ifade edilmiştir (KVKK, 1. Madde; KVKK, 2. Madde).

Kanunda kamu kurumlarıyla özel kuruluşlar arasından bir ayrım yapılmamıştır. Bu nedenle Kanunun belirlediği usul ve esaslar tüm kurum ve kuruluşlar için geçerlidir. Kanun kapsamında koruma altına alınan kişisel veriler sadece gerçek kişilere ait olan kişisel verilerdir. Tüzel kişilere ait veriler bu Kanunun kapsamının dışındadır. Çünkü kişisel veri, kimliği belirli veya belirlenebilir "gerçek kişi"ye ilişkin her türlü bilgi olarak tanımlanmıştır. Bununla birlikte tüzel kişilere ait olan verilerden gerçek kişilerin belirlenebilmesi mümkünse bu verilerin de Kanun kapsamında değerlendirilmesi söz konusudur.

Kanunda "kısmen veya tamamen otomatik yolla işleme" ifadesinin ne anlama geldiği açıklığa kavuşturulmamıştır. 108 sayılı Avrupa Konseyi Sözleşmesinde ise "otomatik işleme" ifadesinden; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması işlemlerinin otomatik veya kısmen otomatik yöntemlerle gerçekleştirilmesinin anlaşılacağı ifade edilmiştir. Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler de 6698 sayılı Kanun kapsamında korunmaktadır. "Veri kayıt sistemi", Kanunun 3. maddesinde, kişisel verilerin belirli ölçütlere göre yapılandırılarak işlendiği kayıt sistemi şeklinde tanımlanmıştır. Dolayısıyla elle işlenen verilerin herhangi bir ölçüte göre yapılandırılan bir kayıt sistemine dahil edilmesi durumunda, bu tür verilerle ilgili olarak da 6698 sayılı Kanun uygulanacaktır. Otomatik olmayan yollarla işlenen kişisel veriler, bir veri kayıt sisteminin parçası da değilse Kanun kapsamında değerlendirilmeyecektir. Fakat bu durum, ilgili verilerin kişisel veri niteliğini etkilemeyeceği için, bu verilere ilişkin hukuka aykırı eylemler de 5237 sayılı Türk Ceza Kanunu kapsamında suç teşkil etmeye devam edecektir (Kişisel Verileri Koruma Kurumu, 2023)[23]

Kanunun 28. maddesinde kanun hükümlerinin uygulanmayacağı tam istisnalar şu şekilde ifade edilmiştir:

[23] Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanunu ve Uygulaması"

a) *Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi*
b) *Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.*
c) *Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.*
d) *Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.*
e) *Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.* (KVKK, 28. Madde).

28. Maddenin 2. fıkrasında ise kısmen Kanun dışında tutulan kısmi istisnalar şu şekilde belirtilmiştir:

a) *Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.*
b) *İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.*
c) *Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.*
d) *Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*. (KVKK, 28. Madde).

Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. ve zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddeleri yukarıdaki hâllerde uygulanmaz. Kanunda belirtildiği gibi 10. 11. ve 16. maddelerin uygulanmaması için maddede belirtilen ihtimallerden birinin gerçekleşmesi ve bu hükümlerin uygulanabilmesi için belirtilen istisnai hallerin Kanunun amacına, temel ilkelerine uygun ve orantılı olması gerekmektedir (KVKK, 28. Madde).

Kanunun 4. Maddesinde kişisel verilerin işlenmesine ilişkin temel ilkelere yer verilmiştir. Bu ilkeler şunlardır:

a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme (KVKK, 4. Madde).

Kişisel Verilerin Korunması Kanununun amaçlarından bir tanesi, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunmasıdır. Bu amacın gerçekleştirilmesi için, Kişisel Verilerin Korunması Kanunu kapsamında ilgili kişilere belirli haklar tanınmıştır. Kanun'un 11. Maddesinde ilgili kişinin (veri sahibi olan gerçek kişinin) hakları şu şekilde belirtilmiştir:

a) Kişisel veri işlenip işlenmediğini öğrenme,
b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
d) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
e) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

f) 7’nci maddede (kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi hakkında) öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
g) (e) ve (f)’deki işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
h) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
i) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme (KVKK, 11. Madde).

Kanunda öngörülen görevleri yerine getirmek üzere Kişisel Verileri Koruma Kurumu oluşturulmuştur. Avrupa Konseyinin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifi, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere işlevsel olarak bağımsız bir şekilde görev yapacak otoritelerin, başka bir deyişle yetkili kurulların oluşturulmasını öngörmektedir. Avrupa Birliği üyesi tüm ülkelerde veri koruma kurulları, görevlerinde bağımsız otoriteler olarak yapılandırılmıştır. Belirtilen uluslararası belgeler ve karşılaştırmalı hukuk uygulamaları göz önüne alınarak, Kişisel Verileri Koruma Kurumu kurulmuştur (Kişisel Verileri Koruma Kurumu, 2023).[24] Kurum, 19. Maddede belirtildiği üzere Cumhurbaşkanının görevlendireceği bakanla ilgili olup idari ve mali özerkliğe sahiptir. Merkezi Ankara’dadır.

Kişisel Verileri Koruma Kurumunun görevleri ise Kanunun 20. maddesinde şu şekilde belirtilmiştir:

a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak,
b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak,

[24] Bkz. Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Korunması Kanunu ve Uygulaması”

c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak,
d) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna sunmak,
e) Kanunlarla verilen diğer görevleri yerine getirmek (KVKK, 20. Madde).

Sosyal medya kullanımlarıyla ilgili kişisel verilerin gizliliğini etkileyen sorunların olumsuz sonuçlarını en aza indirmek için alınması gereken en önemli önlemlerden biri yapılan hukuki düzenlemelerdir. Tezimizin daha sonraki bölümlerinde kişisel verilerin korunması alanındaki hukuki çalışmaların, başta 6698 sayılı KVKK'nun hukukçular tarafından belirtilen birtakım eksiklerine ve hukukun, güncel teknolojik gelişmelerle bu gelişmelerin ortaya çıkardığı yeni tehlikeleri takip etmesinin önemine değinilecektir.

2.3 Bir İnsan Hakkı Olarak Kişisel Verilerin Korunması ve İlişkili Olduğu Temel Haklar

2.3.1 Bir insan hakkı olarak kişisel verilerin korunmasının felsefi boyutu ve mahremiyet hakkı ile ilişkisi

Kişisel verilerin korunmasının başlı başına bir insan hakkı olup olmadığı konusunda bir değerlendirme yapabilmek için öncelikle insan haklarının ne olduğunun ortaya konulması gerekmektedir. İnsan haklarının ne olduğunu anlamak; bir hakkın insan hakkı olup olmadığına karar verebileceğimiz ölçütü ya da ölçütleri özenle belirlemek bu bağlamda son derece önemlidir. Günümüzde insan haklarına birçok yeni hak eklenmektedir ve bu hakların birer insan hakkı olarak ortaya konulması felsefi bir temellendirmeyi gerekli kılmaktadır.

Felsefe varolan, düşünme ve dil arasındaki ilişkileri belirleyerek varolanın neliğini; bir şeyi "işte o" yapanı konu edinir. Kavramlar dışdünyada, düşünmede ya da dilde varolana ilişkin olarak oluşturulan çerçevelerdir (Çotuksöken, 1994, s. 15-24). İnsanın ana özelliklerinden biri kavram kurmaktır ve felsefenin de işi kavram araştırmasıdır. Her türlü varolan dışdünyada, düşünmede ya da dilde varolabilir. Kavramların kendileri de tekil olanları, olup bitenleri, varolanları anlamlandırmayı ve bilgi oluşturmanın temelini

sağlayan düşünsel varlıklardır. İnsan hakları kavramı da her kavram gibi düşünsel bir varolandır. Bazı kavramlar tek bir nesneye, örneğin masa, kalem gibi somut-tekil bir varlığa işaret ederken bazı kavramların böyle bir başvuru noktası bulunmaz. İnsan hakları kavramı da böyle tek bir nesneye işaret etmeyen ve insanın eylemlerinde, insanlararası ilişkilerde ve insanın kendi dışında varolanlarla kurduğu ilişkilerde görünürlük kazanan bir kavramdır. Dışdünyada belirgin somut tekil bir başvuru noktasının bulunmaması insan haklarının sınırlarının çizilmesinde ve anlam çerçevesinin oluşturulmasında belirsizliklere yol açmaktadır. Kavramlar dünyayı anlamamızı sağlayan çerçeveler oldukları için insan hakları kavramına ilişkin kavrayışımız, bir hakkın insan hakkı olup olmadığını, hakkın korunup korunmadığını, bir davranışın insan hakkı ihlali yaratan nitelik taşıyıp taşımadığını belirleyecektir (Çotuksöken, 2012, s. 23-25).

Dünya, sadece doğal olarak varolanlardan değil, insan eliyle yapılmış olan varolanlardan da oluşur. İnsan dünyayı değiştirebilme gücüne sahip bir varlık olarak, olanı değiştirmenin öznesidir. Tüm bunlar özne olan insanın, insan-dünya-bilgi ilişkisi içinde konumlandırılması gereken kavramsal çerçeveleriyle bir anlam kazanır. İnsan-dünya-bilgi ilişkisi etkileşim içinde olduğu için kavramlar da anlamsal içerikleri bakımından tarihseldirler. Onur, saygı, özgürlük, eşitlik, adalet gibi kavramları ve değerleri yaratan insan tarihsel yolculuğunda düşünsel olarak, insana, insan sorunlarına yöneldiğinde ve insan elinden çıkan dünyayı ön plana aldığında insan hakları kavramının da doğmasını sağlayan temelleri atmaya başlamıştır. O halde her türlü bilgi, bilgiyi kavramlar ve onları gösteren sözcükler, terimler (dil dünyası) sayesinde üreten toplumsal-tarihsel-kültürel ve temelde dilsel bir varlık olan insanla ilişkisi içinde ele alınmalıdır. Çünkü bilgi insana aittir ve her bilgi insanın varlık yapısına ait bilgi olmak durumundadır. Bu nedenle insanın kurduğu dünyayı anlamak öncelikle insanın ne olduğunu, onun yapısal özelliklerini ve olanaklarını anlamayı gerekli kılmaktadır. Felsefi antropoloji ve antropontoloji, bize bu bilgiyi sağlayacak olan felsefe alanı ve yaklaşımlarıdır (Çotuksöken, 2012, s. 11-45).

“Felsefi antropoloji”, insanı temel problem alanı olarak gören ve insanın neliğini ortaya koymaya çalışan, insan denen varlığın ayırt edici özelliklerini, türün ortaklıklarından hareket ederek ve tarihi bir varlık olan insanın tarihselliği içinde kurduğu dünyaya bakarak yakalamaya çalışan bir felsefe alanıdır. Bu nedenle insan hakları üzerine düşünürken başvurmamız gereken temeli bize sunacak olan alandır. Betül Çotuksöken,

felsefi antropolojiden hareketle kurduğu ve "antropontoloji (insan-varlıkbilgisi)" adını verdiği felsefe yaklaşımında varlıkbilgisine yani ontolojiye dayanan felsefi antropolojinin tersine varolana yönelmenin temeline insan varoloşunu koymaktadır. Antropontolojiye göre her varolan, insanın bilme edimleri çerçevesinde, bilme edimlerine konu olmasıyla varoluşuna kavuşur. İnsan bu bağlamda bir olanaklar varlığı olarak, açık varlık olarak değerlendirilir. Bu görüş, insana ilişkin özcü yaklaşımları eleştirir ve insanın değişebilirliği üzerinde özellikle durur. Düşünen, bilgi üreten ve dünyayı kuran insanın, sabit ve değişmez bir özü yoktur. Her insan değişebilir, farklılaşabilir niteliklerin toplamıdır (Çotuksöken, 2018, s.71). Dolayısıyla "insan nedir?" sorusu, tarihsel ve kültürel bir varlık olarak insan, hem kendisini hem de dünyasını sürekli değiştirdiği için güncelliğini her zaman korur. Çağımızdaki bilimsel ve teknolojik ürünler geliştirilirken, bunların insanın değerine yönelik olarak oluşturduğu yeni tehditler sonucunda yeni haklar türetilmesi ihtiyacı bu bağlamda değerlendirilebilir.

Şimdiye değin yapılan bu belirlemelere ek olarak, insan hakları, felsefenin bize sağlayacağı bilginin eşliğinde "insan onuru veya insanın değeri" kavramı ele alınmadan anlaşılamaz. İnsan onuru kavramını anlamamızı sağlayacak olan felsefi bilgi, bize insan haklarının nüvesini; gereğinin nereden kaynaklandığını gösterir. İnsan onurunun veya insanın değerinin ne olduğunu ortaya koymak kendi başına amaç olan, devredilmez insan haklarının neden her an herkesçe, herkes için korunmaları gerektiğine ışık tutar (Kuçuradi, 2018, s.1).

İoanna Kuçuradi'ye göre "insan onuru" *(human dignity)* insanın nesnel değerinin öznel karşılığıdır. İnsan türünün belirli yapısal özellikleriyle olanaklarının ve tarihteki başarılarının bilgisinden oluşur. İnsanın gerçekleştirdiği başarıların kaynağı ise tür olarak sahip olduğu yapısal özellikler ve olanaklardır (Kuçuradi, 2018, s. 72-73). İnsanın değeri, insanın insan olmayan diğer her şeyle ilgisi bakımından özel durumu ve özel durumundan dolayı kişilerin insanlararası ilişkilerde sahip olduğu bazı haklar, başka bir deyişle insanın varlıktaki özel yeridir (Kuçuradi, 2020, s. 40). İnsan hakları, bütün insanların sırf insan olduğu için eşit şekilde sahip olduğu haklar olarak tanımlanmaktadır. Bir şeye hak dememiz, o şeyin korunması gerektiğini ortaya koymamız ve bunu talep etmemiz anlamına gelir (Kuçuradi, 2018, s. 108). O halde, bu haklar insanın diğer varlıklar arasındaki yerini, diğer bir deyişle, insanın değerini koruyan muameleyi diğer herkese

göstermeyi talep ederler. Bu değeri korumak demek sadece insana özgü olanakları her kişide korumayı istemek demektir. Dolayısıyla insan haklarını, insana özgü olanakları koruma istemleri olarak ifade edebiliriz (Kuçuradi, 2018, s. 2).

Kuçuradi, "insanın değeri" ve "insanın değerleri" arasında bir ayrım yapar. İnsanın değeri, onun varlıktaki özel yeriyken insanın değerleri, tür olarak insanın tüm başarılarıdır. İnsanın değerleri; bilgi, bilimler, sanatlar, felsefe, teknik, moraller ve kültürlerdir. Bu değerler insanın varlık imkânlarının gerçekleşmesidir (Kuçuradi, 2020, s. 40). Bu olanakların gerçekleşmesini ve gelişmesini sağladığımızda insanın değerini korumuş olduğumuzu söyleyebiliriz. Dolayısıyla insan hakları kişilerde bu olanakların gerçekleşmesini ve insanın bu olanaklarını geliştirebilmesini sağlayan haklardır. İnsan hakları öncelikle kişilerin birbirlerine nasıl muamele etmeleri gerektiğiyle ilgilidir. İnsanlar birbirlerine, her insanda bulunan doğal olanakların gerçekleşmesini sağlayacak şekilde muamele etmelidirler (Kuçuradi, 2018, s. 57).

İnsan haklarının evrensel normlar olmaları, her insanın sahip olduğu türe özgü yapısal özelliklerden kaynaklanmaktadır. Bu yapısal özelliklerle olanakların her kişide bulunması nedeniyle her bir kişide korunması, insan haklarının evrenselliğini ifade eder. Dolayısıyla insan onuru *(dignity)* denen şey, çeşitli kültürlerde, topluluklarda, dinlerde egemen olan değişik ve değişken insan imgeleri ve iyiye-kötüye ilişkin değer yargılarıyla ilgili olan şeref/namus *(honor)* ile ilgili kültürel anlayışlardan ayırt edilmelidir. Bu ayırımı anlayabilmemiz için öncelikle Kuçuradi'nin değer ve değer yargısı ayırımı üzerinde durmamız gerekmektedir. Bu ayırım insan haklarının temellendirilmesinde çok önemli bir noktadır. Değer, her zaman bir şeyin değeridir; bir şeyin bir çeşit özelliğidir. Bir şeyin değeri, kendisiyle aynı türden olan diğer şeyler arasındaki özel yeridir ve bir bilgi konusudur (Kuçuradi, 2020, s. 40-41). Bir şeyin değeri, insanların ona biçtiği ya da atfettiği değerle ilgili olmadığından rölatif (göreli) değildir. Değer ve değer yargıları birbirine karıştırıldığı için değer olarak görülen şeylere insandan insana, toplumdan topluma, çağdan çağa değişkenlik göstererek bazen iyi bazen kötü dendiği düşünülmektedir. İyi-kötü, güzel-çirkin şeklindeki yargılar değer yargılarıdır ve belli davranış biçimlerine "iyidir, kötüdür" şeklinde değer biçmek değer yargılarını oluşturur. Değer yargıları, kültürel ve moral birtakım normlardır ve bilgi temeline dayanmadığı için insan hakları, değişkenlik gösteren bu ezbere değer yargılarına göre değil, felsefi/etik

değer bilgisine dayanılarak temellendirilebilir; temellendirilmesi gerekir. İnsan onuru veya insanın değeri, insanın yapısına ilişkin bilgiden oluşurken, şeref kavramı bir kişinin değerine ya da farz edilen değerine gösterilen saygıyı ifade eder ve değer yargılarıyla ilgilidir. İnsan onuru ya da insanın değeri, insanın yapısına ilişkin bir bilgiden oluştuğu için evrenseldir. O halde farklı kültürlerde farklı farklı olabilen şey onur *(dignity)* anlayışları değil, şeref *(honor)* anlayışlarıdır (Kuçuradi, 2018, s.73-75).

İnsan haklarının, değer yargılarının ve çok çeşitli insan gereksinimlerinin farklılığına rağmen her bir kişide evrensel olarak nasıl korunacağını anlayabilmemiz, özel-toplumsal-kamusal alan kavramlarını da ele almayı ve anlamayı gerektirmektedir. İnsanlar zamanlar ve mekânlar arasında, farklı alanların iç içe geçtiği sınırları kolaylıkla belirlenemeyen ve temelde insansal ilişkiler ağında yaşayan varlıklardır (Çotuksöken, 2018, s. 93). Çotuksöken'e göre insan "arada olan" varlıktır. İnsan öncelikle kendisi ile kendi niyetleri, amaçları, eylemleri, beklentileri arasındadır. Aynı zamanda insan "başka benler" ile kendisi ve topluluk ile kendisi arasında yaşamaktadır (Çotuksöken, 2018, s. 57). İnsan hakları ortaya çıkışı bakımından ise bireyseldir. Bireysel ve kişisel olan haklarla ilgili belirlemeler birey kavramının doğuşuyla tarihlenen modernliğin, birey-toplum ayrışmasıyla çeşitlendirdiği ve belirgin kıldığı gereksinimlerle anlam kazanmışlardır. Her hak somut olarak varolan tek insanın haklarıdır ve bu tek her insan, toplumsal-kültürel bir varlık olarak toplum-kamu-devlet düzeninde yaşayan bir birey-kişi-yurttaştır. Her bir bireyin hakları, insanın var ettiği, kurguladığı bir düzence korunabilmektedir (Çotuksöken, 2012, s. 30-35). Bu nedenle insan haklarını özel-toplumsal-kamusal alan bağlamında değerlendirmek gerekmektedir. Genellikle insanın kendisi ve kendisi olmayanlar arasındaki ilişkisini özel ve kamusal alan olarak iki alan aracılığıyla kurduğundan söz edilmektedir. Ancak toplulukçuluğun, değer yargılarının ve bunlara dayalı oluşturulan etik bilgiden kopuk toplumsal ahlakın egemen olduğu ortamlarda özel-kamusal alan biçimindeki ikili belirleme yeterli olmamaktadır. Böyle bir ayrım ancak toplumda eylemin ölçütünün etiğe dayalı hukuk olduğu ve dolayısıyla toplumun kamu olarak örgütlendiği durumlarda yeterli olabilir (Çotuksöken, 2012, s. 36).

Kamu sözcüğü anlam kargaşası yaratabilecek şekilde "herkes" anlamında da kullanılan bir sözcüktür. Sözlük anlamı itibarıyla kamu *(public)* herkes, genel, umum, halka ait, aleni gibi anlamlara gelmektedir. Herkesin gözlemine ve denetimine açık olanı

tanımlamaktadır. Ancak başına "kamu", "kamusal" nitelemesi getirilen birtakım sözcüklerde kamu sözcüğü geniş bir şekilde herkese ait anlamında kullanıldığında sorunlu bir durum ortaya çıkmaktadır. Örneğin, "kamu bankaları" ifadesi herkesin bankaları anlamını değil devletin bankaları anlamına gelen daha dar bir anlamı işaret etmektedir (Yelken, 2003, s. 45-51).

Kamusal sözcüğü ise, kendi kendisine verilen şahsi bir sivil görev ya da işle uğraşan bir kişiyi niteleyen özelin karşıtı olarak değerlendirilmektedir. Kamusal sözcüğü en genel anlamda özel, kişisel ya da mahrem olana karşıt olarak kamuyla, meslekler veya siyasi alanla ilgili olan için kullanılmaktadır. Bu bağlamda, bir bütün olarak toplumun çıkarını, bireylerin ya da grupların bencil çıkarlarından ayırt etmek için kamusal çıkar deyimi ortaya çıkmıştır. Buna göre, bir toplumun tüm üyelerinin, statüye, zenginliğe veya konuma bakmaksızın paylaştıkları ortak bir hedef, politika ya da amaca "kamusal çıkar" adı verilmektedir. Kamusal alan kavramı ise yurttaş ya da bireylerin toplulukla ilgili konular üzerine tartışma yaptığı, görüşlerini ifade etme olanağı bulduğu, bu sorunların çözülmesinde değerler, amaçlar ve normlar üzerinde anlaştığı veya eleştiride bulunarak katkıda bulunduğu alan olarak tanımlanmıştır (Cevizci, 2005, s. 967).

Bu noktada ise Kant'ın aklın özel kullanımı ve kamusal kullanımı kavramlarına değinmemiz gerekmektedir. Kant, aklın kamusal kullanımını bir kimsenin bilgisini ya da düşüncesini, başkalarına faydalı olacak şekilde sunması olarak ifade etmektedir. Aklın özel olarak kullanılmasını ise kişinin, toplum hizmetinde bulunurken bir hizmeti ya da belirli bir görevi, aklını kullanmak yerine itaat ederek bir makinanın parçası gibi sadece bir işlev olarak yerine getirmesi şeklinde belirlemektedir. Kant, insanlara ışık ve aydınlanma getirebilecek olan şeyin, kendi aklını kitle önünde, kamuoyu önünde ve hizmetinde serbestçe ve açık bir biçimde kullanabilme özgürlüğü olduğunu ifade etmektedir (Kant, 2000, s. 17-21).

Çotuksöken, Kant'ın aklın özel ve kamusal kullanımı kavramlarının bilgiye dayanma ve bilgi dışı olma özelliklerine dikkati çeker. Bilgi dışı olan, inançları, anlık algılamaları, salt duygulanımları, salt duygusallığı, psikolojik olanı, önyargıları işaret eder. Kişilerin salt kendileriyle ilgili durumlarda öne çıkardıkları bir bakıma kişisel çıkarlarını, kişisel gereksinimlerini önceledikleri durumlara ilişkin olarak akıl kullanımı, aklın özel

kullanımıdır. Aklın kamusal kullanımı ise bunun tam tersidir. Bu durumda bilgiye dayalılık söz konusudur. Aklın kamusal kullanımında davranışı, eylemi, ilişkiyi yöneten artık bilgidir ve kamuya açıklıktır. Çotuksöken, özel ve kamusal alanın arasına toplumsal alanı koyarken kamusal alanı diğer iki alandan ayıran noktayı keyfilik olarak belirler. Buna göre, kamusal alan bilgi dışılığı, keyfiliği tümüyle dışarıda bırakan insanlar arasındaki ilişkileri düzenleyen kuralların yasalar aracılığıyla etik bilgi temelinde süreklilik ve nesnellik taşıyacak bir şekilde düzenlendiği alan olarak ifade edilebilir. Toplulukçu değerlerin etkin olduğu toplumsal oluşumlarda "keyfiliğin yasallığı" söz konusudur. Bu kişiye ya da bir gruba ait belli bir özel belirlemenin herkese mal edildiği ya da mal edilmek istendiği ya da herkese hükmetmeye kalkıştığı bir durumdur. Kendini henüz bir kamu düzeni şeklinde örgütleyememiş toplumlarda hakların korunması ve geliştirilmesi ancak rastlantısallıkla mümkün olabilir. Alınan kararlardaki keyfilik kesinlikle nesnellik taşımadığı için bu durum ancak bu şekilde açıklanabilir (Çotuksöken, 2012, s. 36-38). Özel-somut-tekil yaşama dünyasının içinde toplumsal ve özellikle kamusal olanı dikkate almayan, salt biyolojik ve psikolojik olana kendini kaptırmış, sadece kendi gereksinimlerini ve kişisel çıkarlarını önceleyen birinin insan haklarını korumasından ve geliştirilmesinden söz edilemez. Kamusal hale gelemeyen toplulukçu yapılanmalarda da yine "özel" eksenli, değer yargılarına dayanan, özcü yaklaşımlarla farklılıkların hiçe sayılıp bir kişinin ya da bir grubun gereksinimlerinin ya da değer yargılarının herkese dayatıldığı yapılarda da hakların korunması ve geliştirilmesi ya mümkün olmaz ya da haklar rastlantısallıkla gerçekleşir (Çotuksöken, 2012, s. 41-42).

İnsanın özel alanı, temelde bireyin salt bilincinden ve belleğinden oluşur daha somut bir ifadeyle bireyin kendine sakladıklarıdır (Çotuksöken, 2018, s. 94). Bu, özel alanı belirlemede tartışmasız temel ölçüttür. Ancak kişi kafasının içinde yaşayan ve mekânsal olarak bir başına yaşayan bir varlık değildir. Tarihsel süreçte kültür inşa eden insanlar barınacak alanlar geliştirdiklerinde aile yaşamlarını sürdürdükleri özel alanlar yaratmaya başlamışlardır. Bu nedenle özel alanın ve bu bağlamda özel hayatın genel olarak sadece belirli kişilerin girebildikleri herkese açık olmayan kişinin yaşam alanı olan konutu ve aile hayatıyla ilişkili olduğu düşünülmektedir. Avrupa İnsan Hakları Mahkemesi özel hayatın ne oluğunu kesin bir şekilde tanımlamamıştır. Ona göre bu, ayrıntılı bir tanım getirilemeyen geniş bir kavramdır. Açık olan ise, özel hayat *(private life)* kavramının mahremiyetten daha geniş olduğu ve her bireyin özgür olarak kişiliğini oluşturabildiği ve

geliştirebildiği, diğer insanlarla ve dış dünyayla ilişkili bir alanı kapsadığıdır. Mahkeme, kesin bir özel hayat tanımı yapmak yerine, her davanın özelliklerine göre bu boyuta giren durumları belirlemektedir. Dolayısıyla neyin özel olduğunu belirleme konusunda başvurabileceğimiz hukuki boyuttaki özel hayat kavramı, Avrupa İnsan Hakları Mahkemesi tarafından da geniş bir şekilde yorumlamaya açık belirsiz bir kavramdır (Roagna, 2012, s. 12). Kuramsal açıdan özel alan olarak kabul edilen, başka bir deyişle, müdahale edilmeyen, dokunulmayan yaşam alanı olan konutta dahi kişinin gerçekleştirdiği eylemlerinin etkisi kendisini aşabilmektedir. Kişi konutunu da başkalarıyla paylaşabilmekte ya da sahip olduğu konut başkalarıyla paylaştığı bir ortak alanın üzerine bina edilmektedir. Dolayısıyla durumun sadece eylemi gerçekleştiren kişiyi etkileyip etkilemediği, eylemin yarattığı etki, hukuken özel kabul edilen aile yaşamının sınırlarında dahi olsa başka bireyleri ya da bir bireyi ne düzeyde ve ne şekilde etkilediği gibi ölçütler müdahaleyi meşru kılabilmektedir.

Bu bilgiler ışığında özel olanın sınırlarını kesin olarak çizmenin mümkün olmadığını belirterek asıl üzerinde önemle durulması gereken noktanın, insan haklarının korunması ve geliştirilmesinde rastlantısallığı ve keyfiliği dışarıda bırakan, etik bilgiye dayalı hukuki düzenlemeler oluşturmak ve toplumsal düzende böyle bir yaklaşımı veya ölçütü temele almak olduğunu söyleyebiliriz. Özel olanın belirlenmesinde her bir tekil olayı böyle bir bilgi temelinde değerlendirmek gerekmektedir. İnsan haklarının evrenselliği ve her toplumda her birey için korunması ve geliştirilmesi ancak böyle bir anlayışla anlamlı olabilecektir. Özel hayatın gizliliği veya mahremiyet hakkıyla sıkı sıkıya ilişkili olan kişisel verilerin korunması hakkını ele almak için bu noktaları göz önünde bulundurmak önem taşımaktadır.

Kişisel verilerin korunması hakkının mahremiyet hakkıyla bağlantısında ele alınması, mahremiyet hakkının insanın olanaklarının gerçekleşmesi ve geliştirilmesi açısından öneminin ortaya konulmasıyla anlam kazanacaktır. Özel hayat ya da mahremiyet, kişilerin yalnız kalabildikleri, istedikleri şekilde düşünüp davranabildikleri ve başkalarıyla iletişimlerini ve ilişkilerini istedikleri ölçüde belirleyebildikleri bir alanı ifade eder. Mahremiyet hakkı, başkalarını tamamen dışlamak veya onlarla olan ilişkiyi tümüyle kesmek anlamına gelmez. Sadece bir kimsenin, kendi hayatını başkalarıyla ne ölçüde paylaşacağını belirleme hakkına sahip olduğunu ifade eder (Yüksel, 2003). Bu

tanımdan yola çıkarak kişinin sahip olması ve müdahale edilmemesi gereken özel hayatının kişinin bağımsızlığının ve bireyselliğinin bir gereği olduğunu söyleyebiliriz. Kişilerin kimlerle, ne ölçüde ilişki ve iletişim kuracaklarına karar vermeleri, kişilerin hayatlarına ilişkin bir tercihte bulunmaları nedeniyle her bir insanın değerini korumayla da yakından ilgilidir. Çünkü insan bilen, yapıp-eden, değerleri duyan, tavır takınan, önceden belirleyen, isteyen, özgür bir varlıktır. İnsanın yapıp-etmelerini düzenleyebilmesi, onları hayatındaki öneme göre sıraya koyup gerçekleştirebilmesi olanağı onun özgürlüğüdür (Mengüşoğlu, 2017, s. 203). Bu anlamdaki bir özgürlüğün, bağımsız olabilmeye ve birey olabilmeye bağlı olduğunu söyleyebiliriz. J. S. Mill'e göre özel hayatın ihlal edilmesi bireyselliği azaltır ve toplumu birbirine benzeyen ortalama kimselerden oluşan bir yapı haline getirir. Yalnız kalamayan ve hayatının her anını başkalarının gözetimine ve denetimine açık geçiren bir kimsenin bireyselliği ve saygınlığı zarar görür ve kişi, başkalarına benzeyen ortalama bir kimse haline gelir (Mill, 2000, akt. Yüksel, 2009). Mahremiyet sayesinde kişinin kendine özgülüğünü yaşayabilmesi, farklı insanların farklı yönlerini ortaya çıkarabilmeleri açısından büyük önem taşımaktadır.

Olanaklar, değerler ve gereksinimler ekseninde anlaşılmaya çalışılması gerektiğini ifade ettiğimiz kişinin, gereksinimleri, hem kendi değerleriyle hem de başkalarının gereksinimleri ve değerleriyle çatışabilmektedir. Bu çatışma, kişinin hangi değerlere öncelik vermesi gerektiğini, gereksinim duyduğu şeyin, gerçekten bir gereksinim olup olmadığını, eylemlerinin başka insanların gereksinimleri ve değerleri karşısındaki durumunu fark etmesini, ardından da buna göre karar vermesini gerektirecektir. Mahremiyet, kişilerin özel hayatına müdahale etmeme ve gözlerden uzak olma, bireylerin bazı eylemlerini başkalarının gereksinim ve değerleriyle çatışmadan gerçekleştirebilmesi olanağını yaratır. Böylelikle kişinin yaşadığı çatışmanın gücünün kişiyi o eylemden alıkoymasının önüne geçilir. Örneğin, bir kişi muhafazakâr bir toplumda görece muhafazakâr görüşlere sahip olmayan bir kişi olarak varlığını sürdürmeye çalıştığında mahremiyeti, özel hayatındaki insanlarla kurmayı tercih ettiği sosyal ilişkiler, iletişimler ve bunlara müdahale edilmemesi ona kendisi gibi olabileceği, kendisi gibi davranışta bulunabileceği, isteklerini hayata geçirebileceği ve düşüncelerini başkalarıyla ilişkisinde ifade edebileceği bir alan yaratacaktır.

Kişiler bazı eylemlerini toplum içinde yapmayı tercih etmeyebilir, bunların bazılarının toplum içinde yapılmaya uygun olmadığını düşünebilir, gereksinim duyduğu şey toplumun değer yargılarına göre kötü, günah, yasak olabilir. Değer yargılarının bu türden etkileri, psikolojik ve sosyolojik boyutu olan bir konudur. Her toplumda hukuksal olarak bazı eylemler toplum içinde gerçekleştiğinde suç ya da kabahatken, kişilerin bunları özel hayatında yaşamasına müdahale edilmez ve olağan bulunur. Kamusal alanda "iyi", "doğru", "değerli" olduğuna hükmedilen şeyler, özel alanda "iyi" olanlardan çok farklı standartlara göre değerlendirilir. Kamusal bir mekânda birbirini mutlaka tanıması gerekmeyen kişilerin birbirlerinden farklı, birbirleriyle bazen uyuşmayan amaçları, tercihleri ve zevkleri olan farklı kişilerin kendi özel işlerini görürken fiziksel bir yakınlık içinde olsalar dahi rahatsız edici eylemlerden kaçınması ve dikkat çekmeme ilkesiyle davranması gerekir (Geuss, 2007 s. 26-32). Örneğin, müzik dinlemek, estetik bir gereksinim olarak her insanın zaman zaman yaptığı bir eylemdir fakat kamusal her alanda seçtiğimiz bir müziği yüksek sesle dinlememiz uygun olmazken, özel alanımızda bunu yapmakta özgürüzdür. Başkalarının sessizlik gereksinimiyle bizim müzik gereksinimimizin çatışması, bir kulaklık veya özel alanla ortadan kalkar. Bu tür belirlemelerin değer yargılarına göre değil, daha önce değindiğimiz gibi aklın kamusal kullanımıyla, etik-felsefi bir bilgi temelinde düzenlenmiş bir hukukla yapılması, yerine getirilmesi gereklidir.

İnsanların bir işi yerine getirirken veya bir iş üzerinde kafa yorarken dikkatlerini toplayabilmeleri ve işlerini yapmalarına, fiziksel veya düşünsel olarak çalışmalarına engel olacak davranışlardan korunmak için de bir ölçüde mahremiyete ihtiyaç vardır. İnsanın kendini tanımasıyla da mahremiyetin bir ilişkisi söz konusudur. İnsan, benliğini anlamaya çalışırken toplum içinde başkalarıyla bir arada olmaya ihtiyaç duyduğu kadar sadece seçtiği insanlarla olmaya ya da yalnız başına kalmaya da ihtiyaç duyar. Çünkü insanların kişiliklerinin başkalarına ya da belirli insanlara açık pencereleri olduğu gibi, sadece kişinin kendisinin haberdar olduğu ve ortaya çıkması için mahremiyete ihtiyaç duyduğu yönleri de olabilir. Bazen insanlar onaylanmama, eleştirilme kaygılarıyla topluluk içinde bazı eylemleri yapmaktan kaçınabilir ve bunları yalnızken denemeye ihtiyaç duyabilir. Mahremiyet, kişinin kendi yeteneklerini, yeterliliklerini denemesini ve geliştirmesini de sağlar.

Mahremiyet, kişilerin kendilerini başkalarına karşı gizleme, savunma, koruma ihtiyacının yarattığı gerilimi de azaltır. Başkalarından, güven duymadıklarından veya yabancılardan gizlenmiş bir alanda eylemde bulunan kişi bazı olanaklarını daha rahat ve güvenli bir şekilde gerçekleştirecek ve gereksinimlerini karşılayabilecektir. İnsanların olanaklarını gerçekleştirirken onlara müdahale edilmemesi ve kendilerini güvende hissetmeleri bir gerekliliktir. Dolayısıyla bazı gereksinimlerin giderilmesi ve bazı olanakların ortaya çıkabilmesi için müdahale etmeme ve gizlilik ilkelerinin temelinde bulunduğu mahremiyet hakkı diğer bazı temel hakların korunması ve özgürlüklerin gerçekleşebilmesi için koşul niteliğindeki temel bir hak olarak kabul edilebilir. Günümüzde mahremiyetin korunması, dijitalleşmenin ve bunun yarattığı gözetim imkânının etkisiyle kişisel verilerin gizliliği olmaksızın mümkün olamayacaktır. Kişilerin başta özel hayatının ve diğer bazı temel hak ve özgürlüklerinin korunabilmesi için öncelikli olarak kişisel verilerinin gizliliğinin korunması gerekmektedir.

2.3.2 Kişisel verilerin korunmasının diğer hak ve özgürlüklerle ilişkisi

Özellikle hassas kişisel veriler olarak tanımlanan ırk, etnik köken, inançlar, siyasi görüşler, cinsel yönelim, sabıka kaydı, genetik ve biyometrik veriler gibi veriler, özel hayatın gizliliği bağlamında büyük önem taşımaktadır. Bu verilerin gizliliği, kişinin yaşadığı toplumda ayırımcılığa uğramaması ve bu ayırımcılığın, insanın olanaklarının gerçekleşmesi için en temel koşul olan yaşam hakkının ihlaline varacak ölçüde sonuçlar yaratmaması bakımından ya da kişileri, kurdukları ilişkilerin sonucunda ilgili, ilişkili oldukları bir insandan ya da insanlardan korumak açısından gereklidir. Yaşam hakkı, en temel haktır ve ancak bu hakkın korunmasıyla kişi diğer temel hak ve özgürlüklerini kullanabilir. Kişinin telefon numarası, konutunun, işyerinin adresi gibi verilerin gizliliğini de ilk önce kişinin yaşamını güvence altına almak için korumak gerekmektedir. Örneğin, boşandığı eşi tarafından tehdit edilen bir kadının saklamayı tercih ettiği bu kişisel verilere, zarar verebileceği tahmin edilen kişinin ulaşması ya da verileri yoluyla özel hayatı hakkında oluşan yargının tehdit eden kişinin değer yargılarıyla çatışması, kadının hayatını tehlikeye atabilir. Günümüzde kişilerin sosyal ağlarda bıraktığı izlerden, özel yaşamlarından kesitlerin, düşünce ve duygularının okunabilmesi ve konumlarının belirlenebilmesi mahremiyetle kişisel verilerin ilişkisi açısından en kritik noktayı oluşturmaktadır. Bu konuya sonraki bölümlerde tekrar değinilecektir.

Kişisel verilerin korunması hakkıyla ilgili olarak değinmemiz gereken temel hak ve özgürlükten bir diğeri düşünce ve ifade özgürlüğüdür. Özellikle bu hak ile kişisel verilerin korunması konusunda bazı çatışmalar olduğu için bu hakkın ele alınması önem taşımaktadır. Düşünce ve ifade özgürlüğü, herkesin fikirlerini ve kanaatlerini, çeşitli yollarla açıklama ve bunları yayma hakkına sahip olması anlamına gelmektedir. Ancak hukuki düzenlemelerde düşünce ve ifade özgürlüğü, milli güvenliği ve kamu düzenini sağlamak, kamu ahlakını korumak gibi amaçlarla kısıtlanabilmektedir ve yasalara göre suç teşkil eden ifadeleri nedeniyle kişiler cezalandırılabilmektedir. Kuçuradi'ye göre dokunulması ve korunması gerekenler ifade edilen bilgi ve fikirlerin kendileri değil bu bilgileri dile getiren kişilerdir. Bazı fikirlerin öğretilmesi ve propagandası, kamusal düzenlemeler yapılırken tolerans konusu yapılmaması gereken düşünceleri ayırt edecek ölçütler belirlenip değerlendirildikten sonra yasaklanabilir. Bu ölçütler ise fikrin, aynı konudaki bilgiye ve insan hakları bilgisine ters düşmemesi olabilir (Kuçuradi, 2018, s. 111). Avrupa İnsan Hakları Mahkemesi de Avrupa İnsan Hakları Sözleşmesinin 17. Maddesine dayanarak ifade özgürlüğünün, Sözleşme tarafından garanti altına alınan hak ve özgürlüklerin yok edilmesi amacıyla kullanılamayacağını belirtmektedir. Mutlak hoşgörü, hoşgörüsüzlüğü teşvik eden düşüncelere de hoşgörüyle yaklaşılmasına neden olabilir (Bychawska-Siniarska, 2018, s. 14).

Günümüzde kişiler X, Facebook, Youtube gibi sosyal ağlarda pek çok konuda düşünce ve kanaatlerini dile getirmektedirler. Düşüncelerini ifade ederken kullanıcıların bir kısmı anonim kimlikler kullanmaktadırlar. Kimi zaman kişiler bu gizlilik sayesinde düşüncelerini ve kanaatlerini kamuyla paylaşabilmektedirler. Günümüzde bir düşünceyi kamuyla paylaşabilmek anonim kimlikli hesaplar kullanarak sosyal ağların kişisel veri gizliliği politikalarına olan güven sayesinde kişiler için daha rahat bir alan sağlamaktadır. Ancak sosyal medyadaki paylaşımlar yargı konusu olduğunda devlet yetkilileri, bu sosyal ağlarla irtibata geçerek kişilere ait e-posta adresi, IP numarası gibi kişisel veri kapsamındaki bilgileri talep etmektedirler. Sosyal ağlar ise söz konusu talebe konu olan paylaşımları değerlendirerek kendi kuralları, özel hayatın gizliliği ve ifade özgürlüğü gibi konulardaki politikaları çerçevesinde bu bilgileri bazen paylaşmakta bazen paylaşmamaktadır. Örneğin, X'te hukuki talep, ilgili tüm yasal gereklilikleri karşılıyorsa bildirilen hesap veya tweetleri, talebin ifade özgürlüğünü kısıtlama veya caydırma amacı taşıyan unsurlar içerip içermediği, X politikasıyla ilgili başka bir sorun oluşturup

oluşturmadığı (örneğin, gazetecilere ait hesaplar, onaylı hesaplar veya politik söylem içeren hesaplar) veya uygulamayla ilgili teknik sorunlar oluşturup oluşturmadığı incelendikten sonra sahip olunan kişisel veriler, kullanıcıya bu taleple ilgili bilgi verildikten sonra paylaşılmakta veya paylaşılmamaktadır.[25] Zaman zaman Türkiye'nin savcılık yoluyla bulunduğu taleplerin, X tarafından kendi kuralları doğrultusunda karşılanmaması gündeme gelmiştir.

Kişisel Verileri Koruma Kanununun 28. Maddesinde belirtildiği üzere kişisel veriler, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenebilir. Özellikle internetin kullanımıyla birlikte önemli hale gelen unutulma hakkı kapsamında internet arşivlerinde kişilerin şeref ve saygınlığını zedeleyen kişisel verilerinin kamu yararına katkı sağlamayacak şekilde işlenmesi durumunda tarihsel bir veri olarak da kabul edilemeyecek yayınların, kişilerin talebi halinde herkesin erişimine açık halde tutulmasının engellenmesinin gerekliliği Yargıtay kararlarında karşımıza çıkmaktadır.[26]

Dijitalleşme ve sosyal medya kullanımının yaygınlaşmasıyla birlikte insanlar kişisel verilerini milyonlarca insanın görebileceği şekilde gönüllü olarak paylaşırken, aynı zamanda bunlar, başkaları tarafından da internet dolaşımına sokulabilmektedir. Örneğin, Türkiye'de son zamanlarda Youtube gibi sosyal ağlar üzerinden sokak röportajı yaparak halkın fikirlerini yansıtma amacıyla yayıncılık yapan kanallar ortaya çıkmıştır. Herkes sokakta yürürken kendisine uzatılan bir mikrofona söylediği bir şeylerin yayımlanması aracılığıyla, kısa süreli de olsa kendisini ülke gündeminin baş sıralarında bulabilme olanağına sahiptir. Bir kişi kendi sosyal medyasında yine kendisinin yayımladığı bir video ve attığı bir tweetle de milyonlarca insan tarafından konuşulur ve paylaşılır hale gelebilir. Kişi, kişisel verilerini rızasıyla yayımlasa ya da yayımlanmasına izin verse bile, bu verilerin yer aldığı paylaşımların, haberlerin, eleştirilerin ve "sosyal medya linci" olarak ifade edilen tepkiler dolayısıyla internet ortamından silinmesini isteyebilmektedir. Ayrıca

[25] Bkz. X Yardım Merkezi, "Hukuki Talep"
[26] Bkz. LEXIST, "İfade Özgürlüğünün Kişisel Verilerin Korunması Kanunu Bakımından Sınırlandırılması"

kişi, kamuya aktarılmak üzere haber değeri taşıyan bir duruma konu olmak nedeniyle hakkında yapılan bir haberin de unutulma hakkı kapsamında internetten silinmesini talep edebilmektedir. Kişinin şerefi ve haysiyeti aile ve iş yaşamındaki itibarı gibi konuların söz konusu olduğu durumlarda unutulma hakkı, kişinin kendi yaşamını ve kendisine ilişkin bilgiyi kontrol edebilmesi bağlamında ortaya çıkmaktadır. Ancak burada kişinin kendi rızasıyla yayımlanmasına izin verdiği bilgilerin silinmesi tartışmalı bir konudur. Çünkü kişinin böyle bir olanağa kolayca sahip olabilmesi, öngörerek eylemde bulunma bilincine zarar verebilir ve kişisel verilerini daha da sınırsız ve olumsuz bir şekilde internet ortamında yaymasına neden olabilir. Dolayısıyla haber alma ve basın özgürlüğüyle kişisel verilerin gizliliği ve unutulma hakkı ilişkisinde gözetilmesi gerekli olan dengenin yanı sıra, bu konuda da dengeyi sağlayacak değerlendirmeler yapılması gerekmektedir.

Belirttiğimiz görüşler doğrultusunda, korunan kişisel verilerin, bu verilerin bir insana ait olması, o insanı belirlenebilir kılması ve belirlediği takdirde de o kişinin diğer hak ve özgürlükler bağlamında zarar görmesi ya da kişinin olanaklarını gerçekleştirememesi nedeniyle korunması gerektiğini söyleyebiliriz. İnsanın değeriyle ilişkisinde sahip olunan diğer temel haklara da zarar vermeyecek şekilde korunması amaçlananlar, bu verilerin ait olduğu kişilerdir. Dolayısıyla hangi kişisel verinin hangi durumda istisna olacağı bu ölçütlere göre değerlendirilmelidir.

2.3.3 Bir kişilik hakkı olarak kişisel verilerin korunması

Kişilik hakkı, kişinin kişiliğini oluşturan ve onu insan kılan maddi manevi tüm değere, bedensel bütünlüğüne, onuruna, saygınlığına, özel yaşamın gizliliğine, sözüne, resmine, adına, eserine, özgürlüğüne ve bu sıradaki ekonomik hareket serbestliğine ilişkin hakkıdır. Bu hak, mutlak haklardan biri olarak kişiye sıkı sıkıya bağlı olan, başkaları eliyle kullanılamayan ve başkalarına devredilemeyen bir haktır. Kişilik hakkı, kişinin var olmasına, maddi manevi varlığını oluşturup geliştirmesine, özgür olmasına ve saygı görmesine ilişkindir (Serozan, 1977). Kişisel veri gizliliğinin, daha önce ifade ettiğimiz bilgiler doğrultusunda kişiye sırf kişi olması bakımından tanınan ve kişiliği oluşturan değerlerin ayrılmaz unsuru olan bu haklar bütünü kapsamında değerlendirilebileceği ve kişilik haklarının da günümüzde insan haklarından ayrı düşünülemeyeceği açıktır. Kişilik

hakları kavramının geçmişi insan hakları (temel haklar) kavramından eskidir. Kişilik hakları söz konusu olsa da bu haklar bir insan hakkı olarak değerlendirilmemişlerdir. 18. yüzyıldan itibaren ortaya çıkan insan hakları kavramıyla kişilik hakları da biçim değiştirmiştir ve "kişinin korunması" bir insan hakkı olmuştur (Hafızoğulları, 1997). Dolayısıyla bir kişilik hakkı olan kişisel verilerin korunması hakkı, hukuk perspektifinde kişinin korunmasıyla ilişkisi göz önünde bulundurulduğunda bir insan hakkı olarak da nitelendirilmektedir.

Kişisel verilerin korunması hakkının hukuksal niteliğine ilişkin temel olarak iki yaklaşım yer almaktadır. Biri yukarıda değindiğimiz şekilde bu hakkın bir insan hakkı olduğu görüşüyken diğeri bu hakkın bir ekonomik hak olduğu görüşüdür. ABD'de kişisel verilerin korunması anayasal bir hak olarak tanınmamaktadır. Çok geniş bir korumanın ekonomiyi olumsuz şekilde etkileyeceği görüşünün de dikkate alınmasıyla bu hakkın korunmasında ekonomik değeri temel alan bir yaklaşım belirlenmiştir ve daha çok sektörel çözümler tercih edilmektedir. ABD'deki diğer yaygın görüş ise bu hakkın fikri mülkiyet hakkı yaklaşımıyla korunabileceğidir. Buna göre kişinin ürettiği bir eser üzerinde sahip olduğu fikri mülkiyet hakkı kapsamındaki manevi haklar ve kişisel verilerin korunmasıyla ilgili haklar benzer bulunduğundan telif hakkına benzeyen bir yaklaşımla korunması gerektiği düşünülmektedir (Dülger, 2018, s. 76-80).

Avrupa'da baskın olan görüş ise kişisel verilerin korunmasının bir insan hakkı olduğudur. Bu yaklaşıma göre, kişisel verilerin korunmasının önemli olmasının temel nedeni, mahremiyete karşı oluşan tehlikeleri kontrol altına almaktır. Hakkın gelişmesinin özellikle II. Dünya Savaşından sonra önem kazanan insan onuru ve kişilik hakları kavramlarıyla birlikte ele alınması bu görüşü desteklemektedir. Daha önceleri özel hayatın gizliliği hakkının kapsamında değerlendirilen bu hakkın özel hayatın gizliliği hakkıyla bağlantısı kabul edilmekle birlikte, ayrı bir insan hakkı olarak ele alınıp korunması yaklaşımı ortaya çıkmış ve bu, bir gereklilik haline gelmiştir. Özel hayatın gizliliği hakkı kişinin özel ve gizli alanına ilişkin bir korumayı düzenlemektedir. Fakat kişisel verinin bireyin özel hayatıyla ve gizli kalması gereken bilgileriyle ilgili olma zorunluluğu bulunmamaktadır. Bu da kişisel verilerin korunması hakkının başlıca bir temel hak olarak kabul edilmesinin ve düzenlenmesinin nedenlerindendir (Dülger, 2018, s. 76-80).

Dijitalleşmeyle birlikte kişisel veriler kullanılarak gerçekleştirilebilecek hukuka aykırı eylem olanağı artmakta, özel yaşamın gizliliği ilkeleri kişisel veriler üzerindeki hakların korunmasında yetersiz kalmakta; öte yandan teknolojideki hızlı gelişmelerle birlikte kişisel verilerin işlenmesi ve çözümlenip anlamlandırılması, insanın değeri ve özellikle kişi olarak korunması konusunda yeni tehditler doğurmaktadır. Bu bilgiler ve yaklaşımlar doğrultusunda, kişisel verilerin korunması hakkının başlı başına bir temel hak olarak ele alınarak daha kapsamlı bir şekilde korunmasının günümüzde bir gereklilik haline geldiğini ileri sürebiliriz.

3. SOSYAL MEDYA

3.1 Sosyal Medya Kavramı ve Sosyal Medyanın Gelişimi

3.1.1 Sosyal medya kavramı

Sosyal medya, teknolojinin gelişmesiyle birlikte hayatımızda giderek büyüyen bir yer kaplamaktadır. Teknoloji, toplumun ihtiyaçları nedeniyle insanlığa birtakım olanaklar yaratırken aynı zamanda toplumu dönüştürme gücüne de sahiptir. Teknoloji ve toplum bir etkileşim içindedir ve günümüzde bu etkileşimin en çarpıcı etkilerinin dijital devrim ve sosyal medyayla ortaya çıktığı ileri sürülebilir.

Tarihçiler insanların birlikte yaşama biçimini kökten değişime uğratmış iki büyük teknolojik devrimden genellikle söz ederler. Bunların ilki, ilk uygarlıkların kurulmasını sağlayan Tarım Devrimi, diğeri ise otomatikleşen makina teknolojisiyle ekonomik büyüme ve büyük bir servet artışı sağlayan Sanayi Devrimidir. Şu an ise sosyal koşulların köklü bir değişimini yaratan "Dijital Devrim" dönemini yaşadığımızı ileri sürebiliriz (Løkke, 2020, s. 27). Dijital Devrimi niteleyen dijitalleşme, veri, müzik, ses, metin, fotoğraf, görüntü biçiminde her türlü enformasyonun mikro işlemciler yardımıyla sayısallaştırılarak bilgisayar diline dönüştürülmesidir (Tarhan, 2019a, s. 7).

Dijitalleşmenin gelişmesiyle bir dijital iletişim biçimi olarak sosyal medyanın ortaya çıkmasından sonra gündelik alışkanlıklarımızın değişmesinin ötesinde insan dünyasında başta gerçeklik algısı olmak üzere toplumsallık, iletişim, bilgi edinme, haber alma, mahremiyet, kamusallık gibi konulardaki algılar da, görüşler de, kavrayışlar da dönüşmeye başlamıştır. Bu nedenle bizi çevreleyen dünyayı anlamak, dijitalleşen dünyayı anlamayı gerekli kılmaktadır. Yeni bir iletişim ve paylaşım modeli olarak sosyal medya ise bu dijitalleşen dünyayı yaratan sosyal insanı ele alırken mutlaka incelememiz gereken bir kavram haline gelmiştir

Christian Fuchs, sosyal medya kavramını ele alırken öncelikle sosyal medyadaki "sosyal"in ne anlama geldiğini incelemek gerektiğinden söz etmektedir. Web platformlarındaki toplumsallık ya da sosyallik, günümüzdeki web teknolojilerinin ulaştığı olanaklar olarak sosyal davranışları etkileme, uzaysal-zamansal mesafeler üzerinden iletişimi sağlama, insanların bir araya gelerek sosyal ağlar ve ortak dijital bilgiler

oluşturma gibi özellikleri dolayısıyla insan bilişi, insan iletişimi ve işbirliğinin dinamik ilişkisini işaret etmektedir (Fuchs, 2018, s. 67).

Sosyal medya, dergi, gazete, radyo, televizyon gibi ve diğer kitle iletişim araçları gibi yeni bir medya ortamıdır. Bu ortam diğer medya araçları gibi çeşitli bilgilerin ve düşüncelerin paylaşıldığı ve kitlelere taşındığı bir ortamdır. Geleneksel medya kategorisinde yer alan dergi, gazete, radyo ve televizyon gibi tek yönlü ve durağan yayın teknolojilerinden farklı olarak herkesin kendi içeriğini oluşturduğu ve dağıtımını yine kendisinin yaptığı yeni web teknolojileri sosyal medya olarak değerlendirilmektedir (Zarrella, 2010 akt. Tarhan, 2019b, s.106). Sosyal medya, internet kullanıcılarının birbirleriyle çevrimiçi etkileşimde bulundukları farklı yollar anlamına gelmekte, çeşitli sosyal ağ siteleri aracılığıyla içerik oluşturma ve paylaşma, başkalarıyla iletişim kurma gibi faaliyetleri ifade etmektedir (Kirtiş ve Karahan, 2011). İnsanların video, fotoğraf, resim, metin, fikir, kavrayış, mizah, dedikodu, haber gibi içerikleri paylaşmak için kullandıkları blog, vlog, sosyal ağ, podcast, mesaj panoları ve wikiler gibi çevrimiçi kaynaklar sosyal medyadır (Drury, 2008). Cambridge Dictionary'de ise insanların internet veya cep telefonlarını kullanarak bilgi paylaşmasına izin veren blog, podcast ve diğer sosyal medya biçimleri elektronik iletişim biçimleri olarak tanımlanmıştır (Cambridge Dictionary, 2023).

Sosyal medyanın çeşitli kaynaklarda farklı birçok tanımı bulunmaktadır. Ancak yaygın olarak tanımlanması Web 0.1'den Web 0.2'ye geçiş aşamasında ortaya çıkmıştır. Etkileşimli ve çift taraflı iletişim sağlayan bir medya sistemi olarak sosyal medya, Web 0.2'nin hizmete sunulmasıyla kullanılmaya başlanmıştır. Sosyal medya, insanların kendi içeriklerini oluşturabildikleri, etkileşimli olarak birebir veya toplumsal iletişim kurabildikleri ve çeşitli içerikleri kolayca paylaşabildikleri Web 0.2 ortamlarıdır. Günümüzdeki yapay zekâ çalışmaları ile "anlamsal ağ" *(semantic web)* olarak adlandırılan Web 0.3 kavramı ortaya çıkmıştır. İnternetin yeni çağı olarak görülen Web 0.3 ve "büyük veri" *(big data),* pek çok alanda kullanılmaya başlanan sosyal medya madenciliği uygulamalarının ortaya çıkmasıyla özellikle kişisel veri gizliliği konusunda önemli riskleri beraberinde getirmiştir (Esgin, 2015, s. 17-28). Bu konuya tezin daha sonraki bölümlerinde ayrıntılı olarak değinilecektir.

3.1.2 Sosyal medyanın gelişimi

Sosyal medyanın temelleri 18. yüzyılda telgrafın icadına kadar geri götürülebilmektedir. Telgraf uzak mesafeler arasında mesajlaşmanın bir gereksinim olarak ortaya çıkması ve artması nedeniyle ve insanların birbirleriyle olan ilişkilerini ifade etmek üzere, o zamanki adı kesinlikle böyle olmamakla birlikte, sosyal ağ oluşturmada, yeni bir yöntem olarak ortaya çıkmıştır. 19. Yüzyıl sonlarına doğru radyo ve telefon da sosyal etkileşim için kullanılmaya başlanmıştır. Böylelikle sosyal ağlar çeşitlenmeye başlamış ve 1969'da internetin, 1991'de Webin icadıyla sosyal medyanın tam olarak ortaya çıkma süreci başlamıştır (Edosomwan vd., 2011). Sosyal medyanın gelişimini ve gelecekte dönüşebileceği yapıyı anlayabilmek için internet teknolojisinin ortaya çıkışını ve gelişim evrelerini (Web 01, Web 0.2, Web 0.3, Web 0.4) incelemek gerekmektedir.

3.1.2.1 İnternetin Doğuşu ve Web 0.1

Dijitalleşmenin en önemli itici gücü internetin icadı olmuştur. İnternetin icadının 1969 yılında olduğunu söylemek mümkündür. Günümüzde DARPA (Savunma İleri Araştırma Projeleri Ajansı) olarak bilinen US Advanced Research Projects Agency (ARPA) araştırmacıları, 1969 yılında California Üniversitesi ve Stanford Araştırma Enstitüsü arasında ARPANET adı verilen ve kırk farklı bilgisayar ağını içeren bir sistem kurmuştur. İlk kıtalararası bağlantı ise 1973 yılında University College London'ın ağa bağlanmasıyla gerçekleşmiştir. Bu sıralarda farklı ülkelerde de benzer ağlar oluşturulmaya başlanmıştır ve bu bilgisayar ağlarını birbirine bağlamak için bugün de hâlâ kullanılan TCP/IP adı verilen bir sistem geliştirilmiştir. İnternet sözcüğünün kullanımı bu tür bilgisayar ağlarının daha büyük bir bilgisayar ağı oluşturması için birbirine bağlanmasına işaret etmektedir (Løkke, 2020, s.28). Görüldüğü gibi internet, savunma ve askeri amaçlarla keşfedilerek birbirine bağlanan bilgisayar sistemlerinin üretilmeye başlanmasıyla ortaya çıkmıştır.

Türkiye'de ise internet ilk olarak 1987 yılında Ege Üniversitesi'nin öncülüğünde kurulan ve akademik bir ağ olan Türkiye Üniversite ve Araştırma Kurumları Ağı (TÜVAKA) ile kullanılmıştır (Gönenç, 2003).

İnternetin yaygınlaşması, insanların teknolojik ağları kullanarak bağlantı kurdukları tekno-sosyal bir sistem olan "World Wide Web" hizmetinin geliştirilmesiyle gerçekleşmiştir (Esgin, 2015, s. 38). Tim Bernes-Lee, araştırma merkezi CERN'de bulunduğu sırada internetteki farklı kaynakları birbirine bağlayan bir hiper metin geliştirerek dünyanın dört bir yanındaki kullanıcıların bir tarayıcı aracılığıyla web sayfalarını gezebilmesini sağlamıştır. İlk web sayfası böylece 1991 yılında yayımlanmıştır. 1993'te ilk yaygın tarayıcı olan "Mosaic" kullanılmaya başlanmış, 1996'da "Hotmail" ilk web tabanlı e-posta hizmetini başlatmış ve 1998'de arama motoru devi "Google" kurulmuştur (Løkke, 2020, s. 28). İnternet teknolojisindeki bu ilk gelişmeler Web 0.1 olarak adlandırılmaktadır.

Web 0.1 kavramı ilk olarak 1989 yılında Tim Bernes-Lee tarafından ortaya atılmıştır. İlk web, sadece bilgi aramaya ve okumaya izin vererek çift taraflı etkileşim veya içerik oluşturma bakımından çok az olanak sunmuştur. Web 0.1'in bir gazeteden ya da broşürden tek farkı, onu daha fazla insanın kullanabilmesi ve güncellenebilmesi olmuştur (Esgin, 2015, s. 39).

Türkiye'de de bu yıllarda Web 0.1 ile ilgili çalışmalar yapılmıştır. Ortadoğu Teknik Üniversitesi ve TÜBİTAK ortaklığı ile TR-NET projesi geliştirilmeye başlanmış ve ODTÜ, TR-NET aracılığıyla ilk internet bağlantısını 1993 yılında gerçekleştirmiştir. Türkiye'nin ilk internet altyapısı olan TURNET de 1996 yılında devreye girmiştir (Gönenç, 2003).

3.1.2.2 Sosyal ağ platformlarının doğuşu ve Web 0.2

Web 0.2 teknolojisi tek yönlü olarak kullanılmakta olan internet dünyasının kullanıcıyla daha zengin hale getirilmesi hedefi sayesinde ortaya çıkmıştır. Web 0.2 olarak adlandırılan sitelerin, Web 0.1 olarak adlandırılan sitelerden ayrıldığı en önemli nokta kullanıcının rolü olmuştur. Kullanıcıların rolü Web 0.1'deki gibi sadece okuyabilen pasif bir tüketici değil, içeriğe katkıda bulunan, geliştiren ve paylaşan etkin bir üreticidir. İlk kez 2004 yılında bir konferansta "O'reilly Media" adlı kuruluş tarafından kullanılan Web 0.2 kavramı, temel olarak ikinci nesil internet hizmetlerini; internet kullanıcılarının ortaklaşa ve paylaşarak oluşturdukları toplumsal iletişim sitelerini, wikileri, iletişim

araçlarını vb. tanımlamaktadır (Esgin, 2015, s. 22). Dolayısıyla sosyal medya, Web 2.0 teknolojileri üzerine kurulan web siteleri olarak ortaya çıkmıştır.

Sosyal medyanın yapılan tanımlar çerçevesindeki ilk örneği Boyd ve Ellison'a göre, 1997 yılında sosyal medya platformu olarak ortaya çıkan ve adını "Ayrımın Altı Derecesi" *(Six Degrees of Seperation)* denilen, her insanın bir başkasına yalnızca altı kişilik bir insan ağı kadar uzak olduğu teorisinden alan "sixdegrees.com"dur (Wikipedia, 2023). Bu sosyal medya aracı; kullanıcılarına profil oluşturma, arkadaşlarını listeleme ve arkadaş listelerinde gezinme olanağı sunmuştur. Kullanıcıların birbirleriyle bağlantı kurmalarını sağlayan ve sohbet etme seçeneğini de sunan bu platform, yeterli etkiyi oluşturamadığı için 2000 yılında kapanmıştır. 2000'li yılların başından itibaren çeşitli sosyal medya platformları kurularak yaygınlaşmaya başlamıştır (Tarhan, 2019b, s. 108-109).

2001 yılında tüm kullanıcılara açık olan, içerik oluşturup bu içeriklerde değişiklik yapılmasına izin veren bir çevrimiçi ansiklopedi biçimindeki "Wikipedia", Jimmy Wales ve Larry Sanger tarafından kurulmuştur. 2003 yılında Tom Anderson'ın oluşturduğu çevrimiçi arkadaşlıklar kurma olanağı sağlayan, kişisel profilleri, blogları, grupları, resimleri, müzik ve videoları kapsayan bir sosyal paylaşım platformu olan "MySpace" ortaya çıkmıştır. Sosyal medya dünyasında devrim yaratan sosyal ağ platformu "Facebook" ise 2004 yılında Mark Zuckerberg tarafından Harvard Üniversitesindeki öğrencilerin birbiriyle iletişim kurması amacıyla oluşturulmuş ve 2006 yılında diğer kullanıcıların da hizmetine açılmıştır (Eğri, 2019, s. 21). Kullanıcılarının, bir site üzerinden videolar yükleyip diğer kullanıcılarla paylaşabildiği "YouTube", 2005 yılında Steve Chen, Chad Hurley ve Jawed Karim tarafından kurulmuştur (Wikipedia, 2023). Birçok medya üyesinin, politikacıların ve hatta devlet başkanlarının dahi halkla iletişim kurmak için tercih ettiği X (Twitter) ise Jack Dorsey tarafından kullanıcılarına tweet denilen 140 karakter uzunluğunda metinler yazma olanağı tanıyan herkese açık bir mikroblog olarak 2006 yılında kullanıma sunulmuştur (Eğri, 2019, s. 13).

"We Are Social ve Hootsuite"in yayımladığı rapora göre 2023 yılı itibarıyla dünyadaki 8 milyar nüfusun yaklaşık 5.1 milyarı internet kullanıcısıdır. İnternet kullanıcısı olan 5.1 milyar kişinin 4.7 milyarı ise etkin sosyal medya kullanıcısıdır. 13 yaş üstü nüfusun %77,8'i sosyal medya kullanmaktadır ve sosyal medya kullanıcılarının toplam internet

kullanıcılarına oranı %92,3'tür.[27] Bu oranlara göre günümüzde internet kullanmanın artık sosyal medya kullanmak haline geldiğini belirtebiliriz. Dolayısıyla Web 0.2'nin geliştirilmesiyle sosyal ağ platformlarının ortaya çıkışı internet teknolojisinde bir dönüm noktası olarak kabul edilebilir.

3.1.2.3 Anlamsal (Semantik) Web'in doğuşu, Web 0.3 ve Web. 04

Web 0.3 kavramı *New York Times* gazetesinden John Markoff tarafından ortaya atılmış ve ilk kez 2006 yılında web tasarımcısı Jeffrey Zeldman'ın bir blog yazısında kullanılmıştır (Gupta ve Katiyar, 2022 s.508). Temel fikir, verilerin tekrar yapılandırılması ve bu verilerin erişimlerinin mobil internet üzerinden yapılabilmesidir. Web 0.3 öncelikle her yerden, her an, her cihazdan internete bağlanmanın sağlanmasını amaçlamaktadır. Web kavramının yaratıcısı Tim Bernes-Lee ise, Web 0.3'ü "anlamsal web" olarak ifade etmektedir. Anlamsal web en basit ifadeyle bilgisayarların verileri anlayabilmesi anlamına gelmektedir. Temel amacı, verilerin sadece insanlar tarafından değil yapay zekâ teknolojisiyle makinalar tarafından da okunabilmesini sağlamaktır. Web 0.3, Web 0.2'nin geliştirilerek bir anlamda daha zeki hale getirilmesi olarak yorumlanmaktadır (Esgin, 2015, s. 40). Bu teknolojinin en çarpıcı özelliği, içeriklerin, beğenilerin internet aramalarının anlamlandırılarak kullanıcıların karşısına çıkan içeriklerin "kişiselleştirilmesi", kullanıcıya özel içeriklerin önerilmesidir. Özellikle reklam sektörünün kullandığı bu özellik, kişilerin sosyal medyada bıraktıkları izlerin takibi ve internet üzerindeki eylemlerimizin yorumlanması açısından veri gizliliği konusunda yeni riskler yaratan bir gelişmedir.

Günümüzde sosyal medyayı dönüştürüp bambaşka bir dünya haline getirecek Web 0.4'ü geliştirmeye yönelik çalışmalar yapılmaktadır."*Augmented reality*" (artırılmış gerçeklik) kavramının web dünyasına taşınması olarak yorumlanabilecek Web 0.4, insanların sanal dünyada birer avatarının olduğu ve bu avatarlar aracılığıyla sanal ortamlarda gezebileceği bir dünya tasarlamaktadır (Esgin, 2015, s. 44). Mark Zuckerberg, 2021 yılında Facebook sosyal ağ platformlarının adını "Meta" olarak değiştirmiş ve şirketinin geliştirdiği "Metaverse" denilen artırılmış gerçeklik projesiyle ilgili açıklamalarda bulunmuştur. Metaverse terimi ilk olarak 1992 yılında Neal Stephenson tarafından yazılan *Snow Crash*

[27] Bkz. We Are Social Digital 2023 1. Çeyrek Raporu

isimli bilimkurgu romanda kullanılmıştır. Bu roman, kişilerin internette avatarlar kullanarak varolduğu bir dünyayı konu etmektedir. Meta (ötesinde) ve universe (evren) kelimelerinin birleşiminden meydana gelen Metaverse, internette kullanıcıların dijital avatarla ve gerçeklik algısıyla sanki fiziksel dünyanın içindeymiş gibi etkileşimde bulunabileceği, eğlence, ticaret, oyun, eğitim vb. birçok faaliyetin yapılabileceği sanal evren olarak tanımlanmaktadır (Güler ve Savaş, 2022). Böyle bir sosyal medya ortamı, bir arkadaşımız hakkında bilgi sahibi olmak için onun sosyal ağ sayfasına bakmak yerine üç boyutlu olarak sosyal ağdaki sanal dünyasına avatarımıza yüklenen özelliklerle gidebilmek anlamına gelecektir. Bir alışveriş sitesinin sanal dünyasına giderek alacağımız bir kıyafeti avatarımız üzerinde deneyebilme ve hatta sadece avatarımız için tasarlanan dijital kıyafetler satın alma gibi gereksinimler yaratacaktır. Bir bilimkurgu romanın tasarısı gibi değerlendirilen bu tasarımlar çok da uzak olmayan bir gelecekte gerçekleştirilmek üzere geliştirilmektedir. Gerçekleşmesi durumunda bu teknolojinin, sosyal medya ve genel olarak internet dediğimiz sistemde, dolayısıyla insan üzerinde ve onun kurduğu dünyada köklü değişiklikler yaratacağı şüphesizdir.

3.1.3 Sosyal medyanın özellikleri ve türleri

Sosyal medya, çevrimiçi bir ağ türü olarak sunduğu olanaklara göre birtakım özelliklere sahiptir. Bu özellikler; katılım *(participation),* açıklık *(openness),* konuşma *(conversation),* topluluk *(community)* ve bağlantılılık *(connectedness)* olarak sıralanabilir:

> Katılım: Sosyal medya, geleneksel medyadan farklı olarak kullanıcıları katkı yapmaya ve geri bildirimde bulunmaya teşvik eder. Kullanıcıları sadece alıcı değil, kaynak haline getirerek medya ve izleyici arasındaki çizgiyi bulanıklaştırır. Herkes sosyal medyada fikir ve kanaatlerini dile getirebilir, içerik oluşturabilir.
>
> Açıklık: Sosyal medya araçlarının çoğu geri bildirim ve katılıma açıktır. Oylamayı, yorumda bulunmayı ve bilgi paylaşımını teşvik eder. İçeriğe erişme ve bu içerikleri kullanma konusunda ender olarak engeller bulunur. Bu tür engeller hoş karşılanmaz. Sosyal medyada kişiler kısıtlamaya maruz kalmadan

daha rahat bir şekilde görüşlerini iletirler. Bu oluşum genellikle düşünce ve ifade özgürlüğünü desteklemektedir.

Konuşma: Geleneksel medyada tek yönlü olarak yayın yoluyla izleyiciye iletilen içerik söz konusuyken sosyal medyada izleyicinin de katılımıyla iki yönlü bir konuşma gerçekleşebilir. Kişiler kendilerine ulaştırılan içerikler hakkında anında geri bildirimde bulunabilirler.

Topluluk: Sosyal medya, toplulukların hızlı bir biçimde oluşturulmasına ve etkili bir şekilde iletişim kurmasına olanak tanır. Topluluklar sevdikleri fotoğraflar, televizyon programları siyasi konulara ilişkin ortak çıkarlar gibi ögeleri bu platformlardan paylaşabilirler. Sosyal medya, uzaklık ve zaman engelini ortadan kaldırarak grup yapısı gösterebilecek kişileri kolaylıkla bir araya getirerek grup dayanışması oluşturulabilmesini de sağlar.

Bağlantılılık: Çoğu sosyal medya türü, diğerlerine olan bağlantılardan yararlanır. Diğer sitelerle, kaynaklarla ve insanlarla linkler yoluyla bağlantı kurma olanağı tanır. Böylece daha fazla bilgiye ulaşmayı ve daha fazla insanla iletişim kurmayı sağlar (Mayfield, 2008).

Yukarıda belirtilen özelliklere sahip sosyal medya türleriyle ilgili çok farklı sınıflamalar yapılmıştır.

Dawley sosyal medya türlerini aşağıda görüldüğü şekilde gibi sınıflandırmıştır:

Sosyal Siteler: MySpace, Facebook, Twitter
Fotoğraf Paylaşım: Flicker, PhotoBucket
Video Paylaşım: YouTube
Profesyonel Ağ Siteleri: LinkedIn, Ning
Bloglar: Blogger.com, Wordpress
Wikiler: Wetpaint, PBWiki
İçerik Etiketleme: MERLOT, SLoog
Sanal Dünyalar: SL, Active Worlds, There, Whyville, Club Penguin, HiPiHi (Dawley, 2009).

Kaplan ve Haenlein ise sosyal medyayı aşağıdaki gibi sınıflandırmıştır:

Bloglar
Sosyal Ağ Siteleri (örn. Facebook)
İşbirlikçi Projeler (örn. Wikipedia)
İçerik Toplulukları (örn.Youtube)
Sanal Sosyal Dünyalar (örn. Second Life)
Sanal Oyun Dünyaları (örn. Wold of Warcraft) (Kaplan ve Haenlein, 2010).

Bu sınıflamalarda yer almayan mikrobloglar (örneğin, X, Tumblr), forumlar, podcast'ler, sosyal imleme platformları (örneğin, Reddit), yer belirten platformlar (örn. Swarm) gibi kategoriler de konuya ilişkin alanyazınında (literatürde) kullanılmaktadır (Eğri, 2019, s. 23). Bazı sosyal medya siteleri, farklı sınıflandırmalarda farklı adlar altında kategorize edilebilmektedir. Örneğin, X bazı sınıflandırmalarda sosyal siteye dahil edilirken, bazı sınıflandırmalara da mikrobloglara dahil edilmektedir.

En çok karşılaşılan sosyal medya türlerini, sosyal ağ siteleri, bloglar, mikrobloglar, içerik toplulukları (video, ses, fotoğraf paylaşım siteleri), forumlar ve wikiler olarak sıralamak mümkündür. Bu kavramlar kısaca şu şekilde tanımlanmaktadır (Eğri, 2019, s. 9-23):

Sosyal Ağ Siteleri: Kullanıcılarına bir kullanıcı listesi aracılığıyla diğer kullanıcılarla iletişim kurma olanağı sağlayan, ortak sosyal ağları kullanan mevcut insan çevresiyle hızlı bir iletişim bağı kurmayı amaçlayan ve etkileşim, paylaşım, birbirleri arasında geçişkenlik faktörlerinin üzerine inşa edilen web siteleridir. Bu sosyal ağ sitelerinde kullanıcılar profillerini düzenleyerek içerik (müzik, resim yükleme, mesaj yazma vs.) üretebilmekte ve üretilen içerikleri tüketebilmektedirler.

Bloglar: Kişilerin kişisel deneyimlerini ve belirli bir alandaki yorum ya da bilgilerini paylaşarak okuyucularıyla etkileşim kurmalarını sağlayan web siteleridir. Sosyal medyanın kurulmasına öncülük eden ilk sosyal medya örneklerindendir.

Mikrobloglar: Blogların daha da özelleştirilmiş biçimi olarak mikrobloglar, içeriğin sürekli güncellendiği ve çevrimiçi küçük boyutlu bloglarla birleştiği, kullanıcılarına kısa yorumlar yapma olanağı tanıyan web siteleridir.

Wikiler: Oluşumuna herkesin katkı sağlayabileceği açık kaynak ortamları olarak wikiler, bilgi vermeyi amaçlayan ve kullanıcıların içerikleri güncelleyerek geliştirebildikleri web siteleridir.

Forumlar: Belirli konular etrafında şekillenen çevrimiçi tartışma alanlarıdır. En eski sosyal medya türlerinden biridir. Kullanıcılara genellikle özel ilgi alanlarına göre bilgi ve fikir alışverişi yapabilecekleri bir ortam sağlamayı amaçlar.

İçerik toplulukları: Temel amacı kullanıcılar arasında video, ses, fotoğraf gibi medya içeriklerinin paylaşılmasını sağlamak olan kullanıcıların bu tür içerikleri üretip, yükleyip, paylaştığı sitelerdir (Eğri, 2019, s. 9-23).

Bu kavramlar üretilen web sitelerinin ortaya çıkmasıyla birlikte türetilmişlerdir. Dolayısıyla web teknolojilerinin geliştirilmesi ve yeni sosyal medya sitelerinin ortaya çıkmasıyla yeni sınıflandırmaların ve kavramların doğacağını söylemek mümkündür.

Sosyal medya, kolaylıkla dünyanın herhangi bir yerindeki kişilerin birbirleriyle iletişim kurmasını, yeni kişilerle tanışmayı, bir bilginin, haberin, fikrin paylaşılmasını sağlayan, kişilerin kendi içeriklerini yayınlayabildiği, ticari faaliyetlerin yapılabildiği ve bu olanaklara her kullanıcının sahip olabildiği bir medya ve aynı zamanda birçok veri ve enformasyon sağlayan dijital bir bellektir. Kullanımı yaşamda giderek artan bir gereksinim ve alışkanlık halini alan sosyal medya, tezimizin sonraki bölümlerinde ele alacağımız gibi başta ekonomik ve siyasal alanda olmak üzere büyük toplumsal etkiler oluşturan devrimsel özellikte bir web teknolojisidir. Hem insanların ürettiği verilerin depolandığı bir kaynak olması hem de toplumsal etkileri bakımından bir insan hakkı olarak kişisel verilerin korunması konusunda önemle üzerinde durulması gereken bir olgudur.

3.2 Çeşitli Sosyal Medya Siteleri ve Gizlilik Politikaları

Sosyal medya verilerinin özellikle reklamcılık olmak üzere çeşitli amaçlar için kullanılması, bu verilerin şirketlerin ekonomik kazanımları için büyük değer taşıması, veriler sayesinde yapılan analizlerle insan grupları üzerinde yönlendirmelerin yapılabilmesi, devletlerin güvenlik hedefli izleme yapabilmesi gibi nedenler kullandığımız sosyal medya sitelerinin veri gizliliği konusundaki politikalarını önemli

hale getirmektedir. Sosyal medya günümüzde sadece eğlence ve sosyalleşme amaçlı kullanılan bir yer değildir. Kullanıcılara haber alma, bilgi edinme, iletişimi kolaylaştırma gibi önemli kazanımlar da sunan dijital platformlardır. Kişiler için neredeyse vazgeçilmez bir gereksinim haline gelmesi nedeniyle gizlilik politikalarını ele almadan önce bu gizlilik sözleşmelerine onay veren kullanıcıların veri gizliliği konusundaki tutumlarını değerlendirmek gerekmektedir.

Düzenli aralıklarla ülkelerin dijital verilerine göre rapor hazırlayan "We Are Social" şirketinin Ocak 2023 raporuna göre dünya genelindeki 16-64 yaş arası internet kullanıcılarının yüzde 32.20'si kişisel veri gizliliğine ilişkin endişe duymaktadır. Türkiye için bu oran ortalamanın altında olarak %25,80 olarak belirlenmiştir ve 51 ülke arasında 44. sıradadır. Rapora göre, en yüksek endişeye sahip ülke %51,50 oranıyla İspanya'dır. ABD, Kanada, Güney Afrika, Meksika, Polonya, Fransa, Şili, Portekiz, Yunanistan ve Brezilya'da bu oran %40'ın üzerindedir. En düşük endişe oranları ise % 20.90 ile Kenya, % 17,60 ile Gana ve %15,90 ile Nijerya'ya aittir.[28]

Türkiye'deki sosyal medya kullanıcılarının internet güvenliği ve gizliliğiyle ilgili kanaat ve farkındalıkları üzerine 2016 yılında yapılan bir ankette katılımcıların %52'si pazarlama şirketleri, devlet ya da hackerlar tarafından gizlilik ihlaline uğradıklarını düşünmektedir. Yaşanan gizlilik ihlallerine rağmen internet kullanımına devam edeceğini belirten kullanıcıların oranı %28, bu konuda kararsız olanların oranı ise %42 olarak tespit edilmiştir. Araştırmaya göre katılımcıların %74'ü internet siteleri ve sosyal paylaşım ağlarında devlet, pazarlama şirketleri veya hackerlar tarafından gözetim yapan bir yazılımın kullanıldığını düşünmektedirler. Katılımcıların %91'i ise hangi amaçla olursa olsun kişisel verilerin toplanmaması gerektiğini savunmaktadır. Suç oranının yüksek olduğu yerlerde toplumsal güvenliğin sağlanması amacıyla bireylerin gizliliklerinden ödün verebileceği görüşünü savunanların oranı %27'dir. Katılımcıların %51'i gizliliklerinden ne olursa olsun ödün vermeyeceklerini belirtmişlerdir ve %86'sı devletlerin güvenliği sağlamak için gözetim yapmasına ve ilgili kişilere haber vermeden kişisel veri toplanmasına karşıdır. Çalışmanın önemli sonuçlarından biri, internet güvenliği ve gizlilik ihlalleri karşısında internet kullanımından vazgeçme eğiliminin çok

[28] Bkz. We Are Social Digital 2023 1. Çeyrek Raporu

düşük olmasıdır. Katılımcıların küçük bir kısmı gizlilik ihlalleri karşısında internet kullanımından ödün vereceklerini belirtmiş ve %42'lik önemli bir kısmı bu konuda kararsız kalmıştır. Araştırmacının vardığı sonuca göre internet ortamında kendilerini daha özgür hisseden katılımcılar için interneti kullanmak kişisel güvenlikten daha önemlidir. Katılımcıların çok büyük bir çoğunluğu, çevrimiçi gizliliğin devlet, pazarlama şirketleri ve hackerlar tarafından ihlal edildiğini düşünmelerine rağmen internetten sağladıkları faydanın özgürlüklerinden daha önemli olduğunu ve bu platformlarda yer almaktan vazgeçmeyeceklerini belirtmişlerdir (Aslanyürek, 2016).

2019 yılında Türkiye'deki eğitimli ve kentli sosyal medya kullanıcılarının sosyal medyada gizliliğe bakış açılarının değerlendirildiği ve görüşme tekniğiyle yapılan diğer bir araştırmada katılımcıların %55,5'inin gizlilik sözleşmelerini okumadığı saptanmıştır. Sözleşmeleri okusalar dahi bu bağlamda bir şeyin değişmeyeceği, platformu kullanabilmek için sözleşme koşullarını kabul etmek gerektiğini belirtmişlerdir. %11,2'si ise bazen okuduklarını çok uzun buldukları için çoğunlukla okumadıklarını ifade etmişlerdir. Katılımcıların %5,5'i okuduğunu, ancak platformu kullanabilmek için onay vermek zorunda olduğunu ifade etmiştir (Gökaliler ve Saatcıoğlu, 2020).

Türkiye'de yapılan iki araştırma da hayatımızın çok önemli bir parçası haline gelen sosyal medya kullanımı alışkanlığının ve bu yolla edinilen kazanımların veri gizliliği konusundaki endişelere ağır bastığını, kişilerin önemli bir kısmının veri ihlaline ya da veri ihlali riski yaratacak gizlilik sözleşmeleri içeriklerine rağmen bu koşulları kabul etmeye açık olduğunu göstermektedir. Bu razı oluş, gizlilik sözleşmelerinin incelenmesi gereğine ilişkin kanaatleri zayıflatmaktadır. Sosyal medya sitelerinin yasal zorunluluklar dışında veri gizliliği konusunda hassas önlemler almasını sağlamada kullanıcılarının bu konudaki tutumlarının etkisini düşünmek önemli görünmektedir.

Tezimizin bu başlığında sosyal medya siteleri arasından kullanıcı sayısı, dünyadaki popülerliği ve kamuoyundaki etkileri göz önünde bulundurularak Facebook, Instagram ve X (Twitter) siteleri hakkında bilgi verilerek bu sitelerin resmi internet sitelerinde yer alan güncel gizlilik politikaları, özellikle toplanan kişisel verilerin neler olduğu ve bunların hangi amaçlarla toplandığı üzerinde durularak konu ele alınacaktır.

3.2.1 Facebook, Instagram ve Meta gizlilik politikası

2004 yılında Harvard Üniversitesinde öğrenci olan Mark Zuckerberg tarafından kendisi gibi bu üniversitede öğrenci olan kişilerin birbirleriyle iletişime geçmeleri amacıyla kurulan Facebook, kısa süre sonra herkesin bir e-posta adresiyle üye olabileceği bir platform haline gelmiştir. Facebook kişilerin arkadaşlarıyla iletişim kurarak fotoğraf, video gibi içerikleri paylaşmasını sağlayan bir sosyal paylaşım sitesidir. Site kullanıcıları durum güncellemeleri yapabilmekte, ilgi alanları doğrultusunda gruplara veya sayfalara üye olabilmekte, fotoğraf ve video paylaşarak bu içerikleri yorumlayabilmekte ve beğenilerini belirtebilmektedirler. Kullanıcılar, ayrıca doğum tarihi, cinsiyet, eğitim ve iş bilgileriyle beğeni ve ilgi alanlarını belirtebildikleri kişisel profiller oluşturabilmektedirler. Paylaşılan içeriklere başka bir kullanıcıyı etiketleme, konum ve etkinlik paylaşma, etkinlik haberi duyurma, mesaj gönderimi gibi hizmetlerden yararlanabilmektedirler. Kullanıcılar kendilerine ait bilgi ve içerikleri kimlerin görebileceğini gizlilik ayarlarıyla denetleyebilmekte, "Facebook Messenger" uygulaması yoluyla da sözlü, yazılı ve görüntülü şekilde anlık iletişim kurabilmektedirler (Eğri, 2019, s. 21).

2010 yılında Kevin Systrom ve Mike Krieger tarafından kurulan Instagram, 2012 yılında Facebook şirketince satın alınmıştır. Temelde fotoğraf ve video paylaşımı amacıyla kullanılan, fotoğraf ve videoları filtreleme, efekt kullanarak düzenleme olanağı tanıyan anlık mesajlaşma, yorum ve beğeni yapabilme özellikleri olan bir uygulamadır. Kullanıcılar kişisel profillerinde herkese açık veya gizli seçeneği yoluyla takipçileriyle fotoğraf ve video paylaşabilmekte, bu içerikleri yorumlayabilmekte ve beğenebilmektedirler. Kullanıcılar genellikle kendilerine ve yaşamlarına ait görsel içerikleri paylaşarak beğeni alma ve takipçi toplama motivasyonuyla hareket etmektedirler. Bu nedenle gizlilik tercih etmeyen kullanıcılar, herkese açık profilleri sayesinde yüksek takipçi sayılarına ulaşabilmektedirler. Instagram'ın bir diğer özelliği etiketlemedir. Etiketleme diğer ismiyle "hashtag", Instagram'ın popüler özelliklerinden biridir. Fotoğrafın açıklama bölümüne "#" işaretiyle yazılan anahtar etiket kelimeler, bu kelimeyle arama yapıldığında ilgili görsellere ulaşma imkânı sağlamaktadır. Hashtag kullanımı fazla takipçiye ulaşmayı hedefleyen kullanıcıların görsellerini daha fazla insana ulaştırmasını sağlamaktadır (Eğri, 2019, s. 27-28).

"We Are Social Ocak 2023" raporuna göre dünya genelinde, 16-64 yaş arası internet kullanıcıları arasında en popüler olan sosyal paylaşım siteleri %14,3 oranıyla Instagram ve %14,2 oranıyla Facebook'tur. Facebook 2.958 milyar kişiyle en yüksek etkin kullanıcı sayısına sahip sosyal medya platformudur. Instagram ise 2 milyar kişiyle Youtube'dan sonra üçüncü sırada yer almaktadır. Facebook 2021 yılında isim değişikliği yaparak şirketin adını "Meta" olarak değiştirmiştir. Medya ve sosyal medya şirketi olan "Meta", dünyada en çok kullanılan sosyal medya platformlarından olan Instagram, Facebook ve anlık mesajlaşma uygulaması WhatsApp'ın sahibidir. Facebook şirketinin adını "Meta" olarak değiştirme kararı, tezimizin "Anlamsal (Semantik) Web'in Doğuşu, Web 0.3 ve Web. 04" başlığında değindiğimiz Facebook'un 2021 yılında açıkladığı "Metaverse" adlı artırılmış gerçeklik projesiyle bağlantılı olarak şirketin gelecekteki sosyal medya vizyonunu ortaya koymasıyla ilgilidir. "Meta" şirketinin kurucusu ve CEO'su Zuckerberg, 2023 yılı itibarıyla "Metaverse" projesine de büyük yarar sağlayacağını ifade ettiği yapay zekâ çalışmalarına ağırlık vermiştir.[29] Yapay zekâ teknolojilerinin sosyal medyadaki kişisel verilerin gizliliği konusunda yarattığı risklere tezimizin daha sonraki bölümlerinde yer verilecektir.

Bu başlıkta Facebook ve Instagram'ın birlikte ele alınmasının nedeni, bu sitelerin gizlilik politikalarının aynı şirket tarafından yönetilmesinden dolayı, aynı olmasıdır. "Meta" ürünleri olan Facebook, Instagram, Messenger ve Portal için geçerli olduğu belirtilen gizlilik politikası, Facebook ve Instagram sitelerinde ortak olarak yayımlanan 15 Haziran 2023 tarihindeki güncellenmiş son haline göre ele alınmıştır.

Meta Gizlilik Politikası: Meta, gizlilik politikasında kullanıcıların verilerinin nasıl toplandığını, kullanıldığını, paylaşıldığını, ne kadar süre saklandığını ve bu veriler aktarılırken ne gibi önlemler alındığını açıklayarak kullanıcıları, hakları ve gizliliği nasıl denetleyebilecekleri konusunda bilgilendirmeyi amaçladığını ifade etmektedir. "Meta" öncelikle topladığı verilerin neler olduğu konusunda bilgi vermektedir. "Meta" ürünleri kullanıldığında *hesap sahibi olunmasa bile* uygulamayı ya da siteyi kullanan kişinin bazı verilerinin toplandığını belirtir. Bu veriler dört başlık altında toplanmıştır:

[29] İlgi haber detayı için https://www.webtekno.com/mark-zuckerberg-yapay-zeka-icin-yeni-ekip-kurdu-h132515.html bakınız.

1. Hareketler ve Sağlanan Veriler:

– Gönderiler, yorumlar veya ses içerikleri olarak oluşturulan içerikler,

– Yürürlükteki yasalara tabi olmak koşuluyla içerikleri de dahil olmak üzere gönderilen ve alınan tüm mesajlar (*kendilerine şikâyet edilmediği sürece* uçtan uca şifreleme ayarı yapılmış mesajların içeriklerini görmedikleri belirtilmiştir.)

– Mesajlar ve içerikler hakkındaki konum, dosyanın oluşturulma tarihi, mesajın türü, gönderilme tarihi ve saati gibi bilgileri ifade eden meta veriler (üstveriler),

– Görüntülenen ve etkileşimde bulunulan reklamlar da içinde olmak üzere tüm içerik türleri,

– Kullanılan uygulama ve özelliklerle ilgili olarak gerçekleştirilen eylemler,

– Kredi kartı bilgileri dahil olmak üzere "Meta" ürünleri aracılığıyla yapılan satın alma veya bağış vs. gibi diğer işlemler,

– Kullanılan konu etiketleri,

– Ürünleri (uygulama, site) kullanma sıklığı süresi, hareketlerin zamanı.

2. Arkadaşlar, Takipçiler, Diğer Bağlantılar:

– Arkadaşlar, takipçiler, gruplar, hesaplar, Facebook sayfaları, bağlı olunan ve etkileşimde bulunulan diğer kullanıcı ve topluluklar hakkındaki veriler,

– Kullanıcının bu kişiler, hesaplar ve sayfalarla ne kadar sık etkileşimde bulunduğuna ilişkin veriler,

– Kullanıcının cihazındaki adres veya telefon defterini uygulamaya aktarmayı seçmesi durumunda aktarılan kişilerin ad, e-posta veya telefon numarası gibi veriler.

3. Uygulama, Tarayıcı ve Cihaz Verileri:

– Kullanılan cihaz ya da yazılımın ne olduğu ve diğer cihaz nitelikleriyle ilgili veriler,

– Uygulamanın cihazda ön planda olup olmadığı ve kullanılan mouse'un hareket edip etmemesi gibi cihazlarda yapılan hareketler,

– Cihazdan alınan sinyaller, cihaz ayarlarıyla erişimine izin verilen GPS konumu, kamera erişimi ve fotoğraflarla ilgili meta veriler,

– IP adresi ve cihazın bağlı olduğu ağlar hakkındaki veriler,

– Cihaz ayarlarında *konum servisleri kapalı olsa bile* konumla ilgili bazı veriler,

– İnternet tarayıcılarında bilgi depolamak için kullanılan küçük metin parçaları olan çerezlerden elde edilen web ziyaretlerine ilişkin bilgiler.

4. Ortaklardan, Tedarikçilerden ve Üçüncü Taraflardan Alınan Veriler:

– Ziyaret edilen internet siteleri ve çerez verileri (örneğin, Sosyal Eklentiler veya Meta Pikseli aracılığıyla),

– Kullanılan Uygulamalar,

– Oynanan oyunlar,

– Meta harici alışveriş tamamlama deneyimleri kullanarak *Meta ürünleri dışında* yapılan alışverişler ve işlemler,

– Demografik veriler (örneğin, eğitim düzeyi),

– Gördüğünüz reklamlar ve bunlarla nasıl etkileşimde bulunulduğu,

– Meta ortaklarının ürün ve hizmetlerinin internet üzerinde veya yüz yüze nasıl kullanıldığı (ortaklar; reklam, pazarlama veya destek sunmak üzere Facebook, Instagram gibi "Meta" ürünlerini kullanan veya bunlarla entegrasyon sağlayan bir kişi, işletme, kuruluş veya kurumları ifade etmektedir).

"Meta" bu bilgileri kendi ürünlerini oluşturmak, geliştirmek, reklamlar dahil olmak üzere kişiselleştirilmiş özellikler ve içerikler (reklamlar, etkinlik duyuruları, konuma göre etkinlik önerme, ilgi alanına göre haberler sunma ve sayfa önerme, tanıyabileceği arkadaş

önerme, vs.) sunmak için kullandığını ifade etmektedir. "Meta", Facebook ve Instagram'da etkileşimde bulunulan içerikler ve ayarlara bağlı olarak çerezler aracılığıyla erişilebilen tarayıcı verileri, cihaz verileri, arkadaşlarla, takipçilerle ilgili etkileşimler, mesaj, ses, video içerikleri ve üstverileri, ortaklık kurulan diğer şirketlerden aktarılan bilgiler gibi yukarıda sıralanan verilerden hareket ederek kullanıcılarıyla ilgili çıkarımlarda bulunduğunu belirtmektedir.

"Meta", IP adreslerini kullanıcının veya başkalarının emniyetini ve güvenliğini korumak için gerekli olduğu durumlarda konum tahmin etmek üzere kullanabileceğini belirtmektedir. IP adresine ilişkin bir gizlilik ayarı olmadığı için cihazda konum bilgisi kapalı tutulsa bile IP adresi üzerinden genel konum bilgisini elde edebilmektedir. IP adresi ve konumla ilgili sahip olduğu veriyi güvenlik için gerekli olduğu durumlarda kullanabileceğine ilişkin bir açıklama yapmıştır; ancak bu verilerin toplanmadığı anlamına gelmemektedir. Konum verilerinin olağandışı bir konumdan hesaba giriş yapıldığı zaman hesabı güvende tutmak için şüpheli hareketleri tespit etmek amacıyla da kullanıldığı belirtilmiştir.

Diğer önemli bir nokta ise "Meta"nın bu verileri, zararlı veya yasalara aykırı davranışları saptama, önleme ve bunlarla mücadele etme, ötekileştirilen toplulukların karşılaştığı eşitsizlikleri, ırksal önyargıları tespit edip bunlarla mücadele etme, yardıma ihtiyaç duyan kişiyi tespit edip yardım etme, personelin ve şirketin varlıklarının karşı karşıya olduğu tehlikeleri tespit etme ve durdurma gibi amaçlarla da kullanılabileceğini belirtmesidir. Örneğin; ABD'de Instagram kullanan kişilerin, ırklarını ya da etnik kökenlerini soran bir anketle karşılaşabilecekleri bu anketin "Meta" ürünlerini kullanan kişilere yarar sağlamak amacıyla kullanılacağı belirtilmiştir.[30] Toplanan verilerin kapsamı düşünüldüğünde ise kullanıcıların etnik kökeni hakkında bir tahminin yapılabilmesi için yapay zekâdan yararlanan büyük veri analiz teknikleri kullanılmasının yeterli olduğu söylenebilir. Ayrıca, insan gruplarının krizler sırasında nereye gittiği hakkındaki verileri analiz ettiklerini, bu sayede afet yardım kuruluşlarının doğru yerlere yardım ulaştırmasına katkıda bulunduklarını, sosyal medyanın seçimler ve demokratik süreçler üzerindeki etkisini daha iyi anlamak için bağımsız araştırmacılarla çalıştıklarını, Covid-19 tahmin

[30] https://about.fb.com/news/2021/11/inclusive-products-through-race-data-measurement/, Erişim Tarihi: 21.06.2023

modelleri gibi araçlar oluşturmak için yapay zekâ ve makina öğrenimi gibi alanlardaki araştırmaları desteklediklerini de belirtmişlerdir. Bu konu, "Büyük Veri Devrimi ve Sosyal Medya Madenciliği" başlığında ayrıntılı olarak ele alınacaktır.

Kamera özellikleriyle ilgili olarak toplanan veriler kısmında:

> Kameramızı kullanırsanız veya fotoğraf ve videolarınıza erişme izni verirseniz belirli Meta Ürünlerine filtre, efekt, maske veya avatarlar ekleyebilirsiniz. Bu özelliklerden bazıları kamera çerçevesindeki, fotoğraftaki veya videodaki yüzlerin veya gövdelerin belirli kısımlarını işler. Bunlar bir maskeyi gözlere, burna ve ağza doğru şekilde yerleştirmek gibi şeyler yapabilir. Bu süreç için kullandığımız bilgiler, özelliğin oluşturulması amacıyla kullanılır. Kimliğinizin belirlenmesi amacıyla kullanılmaz (Gizlilik Sözleşmesi, https://www.facebook.com/privacy/policy/, 21.06.2023)

ifadesi yer almaktadır. Burada yapılan açıklamada yüz verilerinin kimliğin belirlenmesi amacıyla kullanılmayacağı taahhüt edildiğine göre şirket tarafından yüz tanıma teknolojilerinin kullanıldığı veya yüz verileri yoluyla kimlik belirleyebilme olanağının olduğu anlaşılmaktadır.

"Meta", topladığı verileri, reklam verenlerle, kendilerinin analiz hizmetlerini kullanan ve şirketlerine hizmet sunan ortaklarla ve araştırmacılarla açıkça paylaştığını belirtmektedir. *"Hiçbir bilginizi kimseye satmıyoruz ve asla satmayacağız. Ayrıca ortaklarımızın ve diğer üçüncü tarafların, sağladığımız bilgilerin izin verilen ve verilmeyen kullanım ve açıklanma biçimlerine ilişkin kurallarımıza uymasını şart koşuyoruz"* açıklamasında bulunsa da sadece reklam verenlerle olan ilişkisi düşünüldüğünde dahi şirketin veri paylaşımında bulunduğu şirketlerle çıkar ilişkisi olduğu ve kazanç elde ettiği açıktır (Gizlilik Sözleşmesi, https://www.facebook.com/privacy/policy/, 21.06.2023). Ayrıca kullanıcılara ilişkin kişisel verileri, bilim ve teknolojik gelişme veya emniyet ve güvenlik gibi nedenlerle yasalara uymak koşuluyla kendi politikası doğrultusunda gerekçelendirerek üçüncü taraflara verebileceğini belirtmektedir. İyi niyetli ve topluma yararlı amaçlarla veri paylaşımında bulunabileceğini belirten Facebook, 2018 yılında 87 milyon kullanıcıya ait kişisel verileri, 2016 ABD Başkanlık seçimlerini etkilemek üzere Cambridge Analytica isimli veri analiz şirketine satması iddiası üzerine soruşturulmuştur.

Soruşturma sonucunda verilerin izinsiz ve usulsüz kullanıldığı gerekçesiyle o dönemde, ABD Federal Ticaret Komisyonu tarafından, adı Facebook olan "Meta" şirketine 5 milyar dolar ceza kesmiştir.[31] Kişisel veri ihlali konusunda şüpheleri arttıran ve büyük bir veri ihlali skandalı olarak değerlendirilen bu olaya tezimizin daha sonraki bölümlerinde tekrar değinilecektir.

Gizlilik politikasının ele alınacak son önemli konusu toplanan kullanıcı verilerinin ne kadar süre saklandığıdır. Bu verileri ne kadar süre boyunca tuttuğunu açıkça belirtmeyen "Meta", *"Bilgileri ürünlerimizi sağlamak, yasal yükümlülükleri yerine getirmek veya kendimizin ya da başkalarının menfaatlerini korumak için gerekli olduğu süre boyunca tutarız. Bilgilere ne kadar süreyle ihtiyaç duyduğumuza söz konusu durum özelinde karar veririz"* şeklinde bir açıklama yapmaktadır (Gizlilik Sözleşmesi, https://www.facebook.com/privacy/policy/, 21.06.2023). Bu bilgileri saklama gerekçeleri şu şekilde sıralanmıştır:

- Ürünleri işletmek veya sağlamak için ihtiyaç duyulup duyulmadığı (örneğin, kullanıcı hesabının var olabilmesi için bazı bilgilerin saklanma gerekliliği),

- Hangi özellik için kullanıldığı ve ilgili özelliğin nasıl çalıştığı (örneğin, Messenger'ın kaybolan mesaj modu kullanılarak gönderilen mesajlar, normal mesajlardan daha kısa süre tutulmaktadır),

- Belirli yasal yükümlülükleri yerine getirmek için bilgileri ne kadar süreyle tutmaları gerektiği (örneğin, olası bir devlet soruşturması, şikâyet, dava veya mevzuat işlemleri için saklama gerekliliği),

- Zararı önlemek, koşul veya ilkelerin olası ihlallerini araştırmak, emniyeti, güvenliği ve bütünlüğü artırmak, hakları, varlıkları veya ürünleri dâhil olmak kaydıyla şirketin kendini korumak.

Yukarıdaki bilgilere göre bu verileri silmek için yasal bir gereklilik olmadığı sürece kullanıcı verileri, şirket tarafından istenen süre kadar saklanabilmektedir. Hesabın

[31] İlgili haber detayı için https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook bakınız.

kullanıcı tarafından silinmesi durumunda ise bu belirtilen gerekçeler doğrultusunda *muhafaza edilmesi gereken durumlar haricinde* paylaşılan şeyler dahil olmak üzere bilgilerin silineceğini belirtmektedir. Bu silme işleminin söz konusu içerikleri yedeklerden ve acil kurtarma sistemlerinden kaldırmanın 90 gün kadar sürebileceği belirtilmektedir. Hesap kalıcı olarak silindiğinde hesabın yeniden etkinleştirilemeyeceği ve paylaşılan içeriklerin geri getirilemeyeceği belirtilmiştir. *"Ürünlerimizde yapılan alışverişlerle veya para transferleriyle ilgili mali işlem verileri de dâhil olmak kaydıyla bilgileriniz, aşağıdakilerden biriyle ilgili olduğu takdirde daha uzun bir süre boyunca muhafaza edilebilir ve erişime açık kalabilir"* ifadesi kullanılmaktadır. Söz edilen gerekçeler, yukarıda belirtilen verileri saklama gerekçeleridir. Bu sebepler sıralandıktan sonra ise *"Bazı durumlarda, siz hesabınızın veya bazı içeriklerinizin silinmesini talep ettikten sonra bile yukarıdaki sebeplere dayalı olarak bilgilerinizi muhafaza edebiliriz. Koşul ve ilkelerimizi ihlal ettiklerinden dolayı kapatılan hesaplardaki bilgileri ve kaldırılan içerikleri de muhafaza edebiliriz"* ifadesine yer verilmektedir. Bu ifadeden de anlaşılmaktadır ki hesabın erişilemez olması, başkalarının ve kullanıcının kendisinin de erişememesi verilerin saklanmadığı anlamına gelmemektedir. Şirket gizlilik politikasında belirttiği, örneğin, zararı önlemek, koşul veya ilkelerin olası ihlallerini araştırmak, emniyeti, güvenliği ve bütünlüğü artırmak, hakları, varlıkları veya ürünleri dâhil olmak kaydıyla şirketi korumak gibi meşru nedenler olarak sıraladığı nedenlerden dolayı bu verileri sunucularında saklayabilmektedir (Gizlilik Sözleşmesi, https://www.facebook.com/privacy/policy/, 21.06.2023).

3.2.2 X (Twitter) ve gizlilik politikası

X (Twitter), 2006 yılında Jack Dorsey ve bir grup girişimcinin kurduğu "Obvius" adlı kurumun AR-GE projesi sonucu, temel olarak kullanıcılarına "tweet" adı verilen duygu ve düşünceleri ifade eden metin tabanlı, kısa, anlık iletileri paylaşma ve alma olanağı sağlayan bir sosyal ağ ve mikroblog sitesi olarak ortaya çıkmıştır (Eğri, 2019, s. 13). Kısa metin tabanlı iletiler ilk olarak 140 karakterle sınırlıyken 2017 yılında karakter sınırı 280'e yükseltilmiştir. 2023 yılı itibarıyla eski adıyla Twitter'ın mikroblog olma özelliğinden vazgeçme yolunda olduğunu gösteren bir karar alınmış ve öncelikle sadece

ABD'deki ücretli ek özellikler sunan "Twitter Blue" kullanıcılarının hizmetine sunulmak üzere ileti karakter sınırı 4000'e çıkarılmıştır.[32] X (Twitter), "tweet" dışında kendisine özgü diğer bazı kavramları da ortaya çıkarmıştır. Bunların bazıları; tweet içerisinde bir kullanıcı hesap adının anılarak paylaşılan içeriğin ismi geçen kullanıcıya iletilmesini amaçlayan "mention", kullanıcının paylaştığı tweetin başka bir kullanıcı tarafından kendi takipçilerine iletilmesi durumu olan "retweet", başına "#" işareti konulan bir kelimeyle dikkat çekilmek istenen bir konu üzerinden tweet paylaşımlarının yapılması ve bu etiket aracılığıyla tüm tweetlere ulaşılmasını sağlayan "hashtag" ve hashtag'lerle belirlenen dünya genelinde ya da yerel X (Twitter) gündemini ifade eden "trend topics"tir (Eğri, 2019, s. 14). X (Twitter), kullanıcılarına kişisel profil sayfası oluşturma fotoğraf, ses, video gibi içerikler paylaşabilme, sesli iletişim kurulan sohbet odaları oluşturabilme, mesajlaşama gibi olanaklar da sunmaktadır.

"We Are Social Ocak 2023" raporuna göre X'in 556 milyon kullanıcısı bulunmaktadır ve 16-64 yaş internet kullanıcıları arasında popülerlik bakımından %3.4 oranla 17 sosyal medya platformu arasında 7. sıradadır. Ez az kullanıcı sayısına sahip sosyal medya sitelerinden biri olmasına rağmen devlet başkanları dâhil olmak üzere toplum üzerinde büyük etki sahibi siyasilerin, gazetecilerin, sanatçıların, düşünürlerin kamuoyuyla iletişim kurmak; bilgi vermek, düşüncelerini ifade etmek için kullandıkları bir dijital platform olması bakımından kamusal alan haline gelen etki gücü yüksek olan bir sosyal ağdır.

X (Twitter), 25 Nisan 2022'de Tesla, Starlink, Paypal, OpenAI, Neuralink gibi yenilikçi teknolojiler sunmuş şirketlerin kurucu ortağı olan teknoloji girişimcisi Elon Musk tarafından satın alınmıştır.[33] 2023 Nisan ayı itibariyla da Twitter, Musk'ın sahibi olduğu "X Corp." şirketinin bünyesine dahil edilmiş[34], resmi adı ve logosu "X" olarak değiştirilmiştir.[35] X'i satın aldıktan sonra görevdeki CEO da dâhil olmak üzere üst düzey yöneticilerin işine son veren Elon Musk, X'in denetim politikasının düşünce ve ifade

[32] İlgili haber detayı için https://www.donanimhaber.com/twitter-karakter-siniri-4000-e-yukseltti--160355 bakınız.
[33] İlgili haber detayı için https://tr.wikipedia.org/wiki/Elon_Musk bakınız.
[34]İlgili haber detayı için https://twitter.com/xDaily/status/1645599226309517313?t=PS7EEh1LImPl8hnqsqEHmw&s=19 bakınız
[35] İlgili haber detayı için https://twitter.com/xDaily/status/1685014025233379329?t=qq1fv-nos-Ug9jjUHmwcHQ&s=19 bakınız

özgürlüğünü kısıtladığını savunarak kendisinin yönetiminde bu platformun daha özgür bir yer haline getirileceğini ifade etmiştir. Elon Musk dönemiyle X'te bazı özelliklerin farklılaştırılması veya yeni özellikler sunulması gibi değişimlerin gerçekleşmesi dışında X politikasında büyük eleştirilere neden olan değişiklikler de olmuştur. Bazı takipçi sayısı yüksek kullanıcılar alternatif bir platform arayışına girerek Elon Musk'ın gerekliliğini savunduğu yeniden düzenlenmiş denetim politikasının ifade özgürlüğünü değil dezenformasyonu ve nefret söylemlerini arttıracağı yönünde eleştirilerde bulunmuşlardır (Üstün, 2023). Musk, satın almayı gerçekleştirdikten kısa süre sonra *"Twitter Dosyaları" (Twitter Files)* adıyla birtakım gazeteciler aracılığıyla X (Twitter) üzerinden eski yönetimin uygulamalarıyla ilgili ifşaatlar yapmaya başlamıştır. Bu belgelerin içeriği genel olarak X'in FBI, ABD Dışişleri Bakanlığı, CIA ve Pentagon dahil, çeşitli devlet kurumlarıyla işbirliği içinde gözetim ve sansür uygulamasıyla ilgilidir. Örneğin, birtakım kullanıcı hesaplarının daha fazla insana erişimini azaltmak için görünürlük filtreme denilen uygulamaların özellikle COVID-19 küresel salgını döneminde ABD hükümetiyle aynı fikirde olmayan doktor ve uzmanlar üzerinde uygulandığını, siyasi konularda mevcut hükümet karşıtı görüşler ve iddialar ortaya atan bazı hesapların kara listeye alındığını göstermeyi amaçlamıştır.[36] Bu çerçevede X, şirketin daha önceden yasakladığı ya da askıya aldığı bazı hesapları yeniden açma kararı almıştır. Bu hesapların açılmasıyla ilgili en önemli gelişme ise tweetleriyle şiddete teşvik ettiği gerekçesiyle hesabı kapatılmış olan eski ABD Başkanı Donald Trump'ın hesabının yeniden açılması olmuştur (BBC News Türkçe, 2022). Sözünü ettiğimiz gelişmeler, siyasal iletişimde ve siyasal katılımda sosyal medya kullanımı ve özellikle X'in bu iletişim ve katılımdaki rolü bakımından önem taşımaktadır. Bu durum, bir sosyal medya aracının yönetimini ve politikasını belirleme veya etkileme olanağına sahip olmanın kişilere, şirketlere, hükümetlere sağlayacağı gücün boyutunu gösterebilmesi açısından dikkate değerdir. Örneğin günümüzde akademik çalışmalarda da kullanılmaya başlanan bir kavram olarak "twitter diplomasisi" veya "twiplomacy", bu sosyal ağın devlet başkanları ve diplomatlar tarafından kamu diplomasisi yürütmek için kullanıldığını ifade etmektedir (Wikipedia, 2023).

[36]İlgili haber detayı için https://en.wikipedia.org/wiki/Twitter_Files bakınız

Diğer bir önemli gelişme Musk'ın X sayfasından paylaşım yaparak 2018'de yönetim kurulundan istifa ettiği OpenAI'yi ve bu şirketin ortağı olan Microsoft'u ChatGPT gibi yapay zekâ sistemlerini geliştirmek için X verilerini yasa dışı kullanarak veri madenciliği yapmakla suçlaması ve dava edeceğini ifade etmesidir (Dünya Gazetesi, 2023). Musk'ın kendisi de X için bir yapay zekâ projesi üzerinde çalışmaktadır (Aposto Gündem, 2023). Bu konu, yapay zekâların geliştirilmesinde X gibi sosyal ağların büyük bir kişisel veri kaynağı olması ve saklanan verilerin çok değerli olması bakımından önemlidir. Dolayısıyla tezimizin bir sonraki başlığının konusu olan büyük veri, veri madenciliği ve yapay zekâ kavramlarının ele alınması, sosyal medyadaki kişisel veri gizliliği risklerini anlamak açısından büyük önem taşımaktadır.

Ele alacağımız gizlilik politikası X'in sitesinde yayımladığı 18 Mayıs 2023 tarihli güncel haline göre incelenmiştir.

X (Twitter) Gizlilik Politikası: X, kullanıcılar hakkında topladığı verileri, bunları nasıl kullandığını, ne zaman paylaştığını ve kullanıcılarının bunlar üzerinde denetim sahibi olduğu gibi önemli noktaları hedeflediğini ifade ederek gizlilik politikasını en anlaşılır şekilde sunmaya çalıştığını belirtmektedir.

Şirket,

> Bir Gizlilik Politikası ile herkesi mutlu etmek gerçekten zor. Twitter kullanan çoğu kişi kısa ve anlaşılması kolay bir şey ister. Bilmeniz gereken her şeyi bir Tweet'e sığdırabilmeyi isterken, düzenleyicilerimiz bizden yasal yükümlülüklerimizi çok ayrıntılı bir şekilde açıklayarak yerine getirmemizi istiyor (…) gizlilik politikasının her bir kelimesini okumayı atlarsanız en azından şunu bilin" diyerek çoğu kişinin sözleşmeleri ayrıntıları şekilde okumaktan kaçınacağını öngördüğünü belirtmektedir (Twitter Privacy Policy, https://twitter.com/en/privacy#update, 24.06.2023).

Kullanıcılarının emin olmaları gerektiği noktalar ise kullanıcılar hakkında birtakım veriler toplandığı, verilerin X'i daha iyi bir hale getirmek için toplandığı, kendisine bağlı kuruluşların kendi gizlilik politikaları olabileceği, kullanıcıların gizlilikle ilgili ayarlar yapabileceği ve bu verileri nasıl topladıkları hakkında bilgi edinmek için kendileriyle

iletişime geçilebileceği şeklinde özetlenmektedir. Daha önce değindiğimiz gibi bazı araştırmalar, kullanıcıların gizlilik sözleşmelerini okumamalarının bir nedeninin bu sözleşmelerin uzun ve ayrıntılı bir biçimde hazırlanmasından kaynaklanmaktadır. Ancak gizlilik sözleşmeleri incelendiğinde önemli noktaların; kişisel verilerin toplanmasında ve saklanmasında teknik risklerin, örtük amaçların ve istisnaların bu ayrıntılar yoluyla anlaşılabileceği ortaya çıkmaktadır. "Meta" gizlilik politikasının internet sitesinde hazırlanan sunumunda da görüleceği gibi bu ayrıntılar, kullanıcının okumakta olduğu belgeden farklı bir belgeye ya da kaynağa tıklamak yahut da üzerine gelmek, dokunmak gibi etkileşimlerle ulaşabileceği referansları ifade eden "hiperlinkler" (hiperbağlantılar) ve tıklandığında daha fazla ayrıntı gösteren "drop-down" menüler (açılır menüler) yoluyla okunabilmektedir. Hatta bu bağlantıların açtığı metinlerde de başka bağlantılar bulunmaktadır. Bunlar incelendiğinde bu sözleşmelerin tam olarak anlaşılması için metinleri, bu bağlantıları ve açılır menüleri tam olarak okumak gerektiği anlaşılmaktadır.

X gizlilik politikasında slogana benzeyen ifadeler kullanmaktadır. Örneğin topladığı bilgilerin neler olduğunu açıkladığı kısımda *"Siz veri verin, biz veri alalım. Karşılığında faydalı hizmetler sunuyoruz"* demektedir. Bu veriler üç başlık altında sıralanmıştır:

1. Ürün ve Hizmetleri Kullanmak İçin Sağlanan Veriler

a) Kişisel Hesaplarla İlgili Bilgiler: Bunlar kişisel bir hesap ve profil oluşturabilmek için gerekli olduğu ifade edilen bilgilerdir.

- Görünen ad ve takma ad bilgisi, parola, e-posta adresi veya telefon numarası, doğum tarihi, görüntüleme dili ve oturum açma verileri,
- Paylaşılan konum verisi,
- Bir cihazdan X'e aktarılması tercih edilen adres telefon rehberi,
- Kişisel profilde paylaşılan diğer veriler.

b) Profesyonel Hesaplarla İlgili Veriler: Profesyonel hesaplar işletmelerin, markaların, içerik oluşturucuların ve yayıncıların platformda benzersiz ve açıkça tanımlanmış bir varlığa sahip olmalarını sağlayan hesaplar olarak tanımlanmıştır. Böyle bir hesap

oluşturabilmek için hesap adı, kişisel bilgiler ve profil resmini içeren ve kişinin gerçek kimliğini gösteren herkese açık eksiksiz bir profilin oluşturulması gerekmektedir. Bu veriler kişisel hesap oluşturmak için yukarıda belirtilen, gerçek ad, adres, e-posta adresi ve telefon numarası, aktarılan telefon rehberi gibi veriler ve profil hesabında herkese açık olacak şekilde sağlanması beklenen ya da kullanıcının sağlamayı tercih ettiği diğer tüm verilerdir.

c) Ödemeyle İlgili Veriler: Ücretli ürün ve hizmetlerin bir parçası olarak sunulan reklamları veya diğer teklifleri satın almak için kullanılan verilerdir.

- Fatura adresi,
- Kredi veya banka kartı numarası, kartın son kullanma tarihi ve CVV *(Card Validation Value)* kodu dahil olmak üzere diğer tüm ödemeyle ilgili veriler.

d) Tercihlerle İlgili Veriler: Ayarlar bölümü incelendiğinde bu bilgilerin "kişiselleştirme" için kullanılmasına izin verilen veriler ve ortaklık kurulan diğer şirketler ve reklam verenlerle "ek bilgiler"in paylaşılmasına izin verilen veriler olduğu görülmektedir. Bu bilgiler şunlardır:

- X'in kullanıcı hakkında sahip olduğu e-posta adresleri, telefon numaraları, yaş, cinsiyet, kullanılan dil dahil olmak üzere sahip olduğu hesap verileri,
- X'e giriş yapmak için kullanılan cihaz verileri,
- Çerezlerle sağlanan web ziyaretlerine ilişkin tarayıcı verileri.

Ayarlar kısmında yapılan gizlilik tercihleri bu verilerin kişiselleştirme ve işbirliği kurulan ortak veya reklam verenlerle paylaşımına izine vermeyle ilgili olduğuna göre X, bu verileri toplamaktadır; ancak bu verilerin kişiselleştirme için bir araya getirilmesini, veri analiziyle çıkarım yapılarak kişiselleştirilmiş hizmet sunulmasını ve topladığı bu verileri yasalar izin verdiği ölçüde paylaşabilme iznini kullanıcının tercihine bırakmaktadır.

Diğer şirketlerle paylaşılmasına izin vermeme tercihi yapılabilen bilgiler X'in (Twitter) "ek bilgiler" olarak ifade ettiği verilerdir. Bu ayarın yapıldığı kısımda *"Twitter, ürünlerini çalıştırmak ve iyileştirmek amacıyla her zaman iş ortaklarıyla bilgi paylaşır*

(...) Twitter'ın faaliyetlerini sürdürmesini sağlamaya yardımcı olacak bu iş ortaklarıyla ek bilgileri paylaşmasına olanak tanır" ifadesi yer almaktadır. X bazı durumlarda herkese açık olmayan kişisel verileri iş ortaklarıyla paylaşabildiğini ifade etmektedir. Bu ayar, herkese açık olmayan kişisel verilerin paylaşılıp paylaşılmayacağıyla ilgilidir. X, herkese açık olmayan bazı kişisel verileri iş ortaklarıyla paylaştığını söyledikten sonra bu verilerin, "*Twitter'ın mobil uygulamalarını açan veya bu uygulamalarda giriş yapan cihazların IP adresini ve mobil cihaz reklam tanımlayıcılarını içerebileceğini ancak ad, e-posta adresi, telefon numarası veya Twitter kullanıcı adını içermediğini"* belirtir. Bu bilgilerden bazılarını kişisel hesaplarda herkese açık şekilde paylaşmak mümkündür. Ayrıca, *"Bu ayarda yapılan değişiklikler hemen geçerli olmayabilir"* şeklinde bir ifadenin yer aldığı görülmektedir. Buna herhangi bir gerekçe sunulmaması ve süre belirtilmemesi ise dikkat çekicidir (Twitter Privacy Policy, https://twitter.com/en/privacy#update, 24.06.2023).

2. X Kullanıldığında Toplanan Veriler

- Tweetler ve gönderilen içerikler ve diğer içerikler, oluşturulan yayınlar ve bunların ne zaman oluşturulduğu, listeler, yer imleri ve parçası olunan topluluklar,
- Retweet'ler, beğeniler, paylaşımlar, yanıtlar, diğer kullanıcıların içerikte birbirlerinden söz etmesi veya etiketlemesi gibi birbirleriyle etkileşimleri ve katıldığı yayınlar (izleme geçmişi, dinleme, yorum yapma, konuşma ve tepki verme),
- Kullanıcıların takip ettiği kişiler ya da onları takip edenler, takip eden ve edilenlerin veya platformdaki diğer kişilerin birbirleriyle nasıl etkileşim kurduğu,
- Mesajların içeriği, alıcılar ve mesajların tarihi ve saati dahil olmak üzere doğrudan mesajların (dm) ne zaman kullanıldığı,
- X ile e-posta yoluyla iletişim kurulursa bunun içeriği,
- Hizmetlerde (X'in gönderdiği e-postalar dahil) etkileşimde bulunulan tüm bağlantılar ve görüntülenen reklamlarla ilgili etkileşimler,
- Hizmetleri kullanmak için yapılan satın almalarda ödemelerle ilgili veriler,

– IP adresi ve tarayıcı türü gibi bağlantılarla ilgili veriler,

– Cihaz ve reklam kimliği, işletim sistemi, operatör, dil, hafıza, yüklü uygulamalar ve pil seviyesi gibi cihaz ve ayarları hakkında veriler,

– Cihazın tercihe bağlı X'e aktarılan adres defteri,

– Kullanıcının yaklaşık konum hakkındaki bazı verileri. Tercihe bağlı olarak paylaşılan kesin konum ve daha önce X'in kullanıldığı konum verileri.

X, *hesap sahibi olunmasa da* veya *oturum kapatılmış olsa bile* IP adresi, tarayıcı türü ve dili, işletim sistemi, yönlendiren web sayfası, erişim süreleri, ziyaret edilen sayfalar, konum, cihaz verileri (cihaz ve uygulama kimlikleri dâhil), arama terimleri ve kimlikler (sorgu olarak gönderilmeyenler dâhil), X'de gösterilen reklamlar gibi verileri de topladığını belirtmektedir.

"Tercihlerle İlgili Bilgiler" kısmında ele alındığı üzere X, toplanan verilerle ve yapılan analizlerle kullanıcının kimliğini anlamasını ifade eden "inferred identity" (çıkarsanmış kimlik) oluşturmak ve bu yolla kişiselleştirme yapmak için veri topladığını ifade etmektedir.

3. Üçüncü Taraflardan Alınan Veriler

X, reklam ve iş ortaklarından, tarayıcı çerez kimlikleri, X'in oluşturduğu tanımlayıcılar, mobil cihaz kimlikleri, e-posta adresleri gibi karma kullanıcı verileri, demografik veya ilgi alanı verileri ve bir web sitesinde veya uygulamada görüntülenen içerik veya gerçekleştirilen eylemlerle ilgili verileri aldığını ve bu alınan verileri kendi topladığı verilerle birleştirilebileceğini ve bu yolla kullanıcı hakkında enformasyon üretip çıkarımda bulunabileceğini ifade etmektedir. Yapay zekâ yoluyla bir kişinin dijital verileriyle o kişinin kimliğine ilişkin çıkarımlar yapılması konusuna tezimizin daha sonraki bölümlerinde tekrar değinilecektir.

X, verileri ne kadar süreyle sakladığını açıkladığı kısımda *"Genellikle, verilerinizi hesabınız açık olduğu sürece saklarız"* demektedir. Profil bilgilerini ve içerikleri hesabın süresi boyunca sakladığını, ürün ve hizmetler kullanıldığında toplanan diğer kişisel

verileri *genellikle* en fazla 18 ay boyunca saklayacağını ifade etmektedir. *"Yasal gerekliliklere uymak ve emniyet ve güvenlik nedenleriyle belirli bilgileri politikalarımızın belirttiğinden daha uzun süre saklayabiliriz"* ifadesinden ve *"genellikle"* ifadesinin kullanılmasından anlaşıldığı üzere "Meta"nın gizlilik politikasında da olduğu gibi bu bilgilerin X tarafından ne kadar süreyle saklanacağı şirketin değerlendirmesine bağlıdır. Verilerin silinmesiyle ilgili kısımda ise "*Devre dışı bırakıldığında görünen adınız, kullanıcı adınız ve herkese açık profiliniz dahil olmak üzere Twitter hesabınız artık Twitter.com'da, iOS için Twitter'da ve Android için Twitter'da görüntülenemez. Yanlışlıkla devre dışı bırakılan Twitter hesabınızı devre dışı bıraktıktan sonra 30 güne kadar geri yüklemek hâlâ mümkündür"* denilmektedir. Bu ifadede verilerin kalıcı olarak silindiğinden (yok edildiğinden) söz edilmemekte, sadece hesabın erişilebilir olmayacağı belirtilmektedir. Hesabın 30 gün sonra geri getirilemeyecek olması, aslında verilerin saklanmadığı anlamına gelmemektedir (Twitter Privacy Policy, https://twitter.com/en/privacy#update, 24.06.2023).

X topladığı verileri, sunduğu hizmetleri iyileştirip geliştirebilmek, ayarlar izin veriyorsa ortaklık kurulan şirketlere ve reklam verenlere ulaştırmak; kişiselleştirmeyle kullanıcıya özel reklamlar ve içerikler sunmak, ürün geliştirmek için araştırma yapılmasına yardımcı olmak; kullanıcıların, ürünlerin ve hizmetlerinin güvenliğini sağlamak amaçlarıyla topladığını ifade etmektedir. Sosyal ağlar da dahil olmak üzere dijital hizmet sağlayıcıların kişisel verileri toplanmasının bir nedeni de kullanıcının kimliğini doğrulayarak hesabını güvende tutmak, dolandırıcılığı ve hesapların yasa dışı kullanımını önlemektir.

Kişisel verilerimizin korunması için kişisel verilerimize ihtiyaç duyulması veya toplum güvenliği için kişisel verilerimizin izlenmesi veri gizliliğinde bir "güvenlik-gizlilik ikilemi" oluşturmaktadır. Tezimizin ilerleyen bölümlerinde örneklerini vereceğimiz Facebook-Cambridge Analytica Skandalı gibi veri ihlalleri ve siber güvenlikteki eksiklikler nedeniyle oluşan veri sızıntılarının yarattığı güvensizlik, kişiler için yarar sağlamak gerekçesiyle bu verilerin toplanması, saklanması ve analiz edilmeleri konusunda sorunlu bir durum ortaya çıkarmaktadır. 2013'te dünya gündemini sarsan ve "Snowden Olayı" veya "NSA Skandalı" olarak adlandırılan olay, sosyal medyada kişisel veri gizliliğiyle ilgili olarak ele alınması gereken çok önemli bir diğer olaydır. ABD'nin

istihbarat toplama ajansı olan National Security Agency'de (NSA) güvenlik uzmanı ve istihbarat teşkilatı CIA'de ajan olarak görev yapmış olan Edward Snowden'ın NSA'in gizli belgelerini açıklayarak bu istihbarat ajansının Google, Facebook, Apple ve diğer ABD şirketlerinin verilerine doğrudan erişim sağlayan "Prism" adlı bir programı kullanarak gözetim yaptığını ortaya çıkarması şeklinde özetlenebilecek bu olay, tezimizin sonraki bölümlerinde tekrar ele alınacaktır (Sezgin, 2014). Devletlerin, istihbarat örgütlerinin toplumu gözetlemek amacıyla dijital ortamdaki kişisel verileri kullanabilmesi olasılığının, güvenlik-gizlilik ikilemi bağlamında baskıcı yönetimlerde yaratacağı sonuçlar açısından ele alınması oldukça önemli bir konudur.

3.3 Büyük Veri Devrimi ve Sosyal Medya Madenciliği

Kişisel bilgisayarlarımızdaki temel veri birimi bayt'tır. Bir bayt ise programlama dilinde 0 ve 1'den oluşan iki değeri ifade eden 8 bitten oluşmaktadır (Civelek, 2023). Fizikçi Melvin M. Vopson 2020 yılında yayımlanan bir makalesinde bir yılda $\sim 10^{21}$ dijital bilgi biti üretildiğini ve senede %20'lik bir büyüme oranı varsayıldığında bundan yaklaşık 350 yıl sonra üretilen bit sayısının Dünya'daki tüm atomların sayısını aşacağını tahmin etmektedir (Vopson, 2020). 2025 yılında üretilmiş olan dijital verinin yaklaşık 163 zetabayt (1 zetabayt= 10^{21} bayt) olacağı tahmin edilmektedir (Akıncı, 2019). Yazılım şirketi DOMO'nun analizine göre bir dakikada, 571 yeni web sitesi kurulmakta, 204 milyon e-mail gönderilmekte, Google'da yaklaşık 2 milyon arama yapılmakta, Instagram'da 3600 yeni fotoğraf, Facebook'ta 684 bin içerik ve X'te 100 bin tweet paylaşılmaktadır.[37] Giderek dijitalleşen dünyada her yıl olağanüstü büyüklükte veri, büyük bir hız ve çeşitlilikle üretilmektedir. Dijital bir ortamda gerçekleştirilen her işlem ardında bir veri kaydı bırakmaktadır. Birçok farklı kaynaktan çok çeşitli ve büyük miktarda verinin sürekli olarak üretilmesi "büyük veri" *(big data)* kavramını ortaya çıkarmıştır. Büyük veri, yüksek hacim, hız ve çeşitlilikte üretilen yapısal, yarı yapısal ve yapısal olmayan veri bütünüdür. Dünya genelinde üretilen dijital verideki olağanüstü artış, çok hızlı bir şekilde üretilen bu çok çeşitli ve büyük miktardaki verilerin depolanmasını, işlenmesini ve çözümlenerek anlamlı hale getirilmesini sağlayan büyük veri uygulamalarının gelişimini sağlamıştır (Akıncı, 2019). Büyük veri, hem geleneksel

[37] İlgili istatistik detayı için https://www.domo.com/data-never-sleeps#top bakınız.

veri araçlarının depolayıp saklayamayacağı kadar büyük bir veri yığınını hem de veri yığını çok büyük olduğu için bu verileri yapay zekâ yoluyla anlamlandırmayı ve enformasyona dönüştürmeyi içeren uygulamaları ifade eden bir kavram haline gelmiştir (Løkke, 2020, s. 60).

Büyük veri, terim olarak ilk kez 1997'de NASA'da çalışan Michael Cox ve David Ellsworth tarafından kullanılmıştır. Cox ve Ellsworth, büyük verilerin görselleştirilmesi konusunda yaşadıkları problemi "büyük veri sorunu" olarak adlandırmıştır. Veri setleri ana belleğe (çekirdeğe) ve hatta yerel diske sığmadığında en yaygın çözümün, daha fazla depolama kaynağı edinmek olduğunu ifade etmişlerdir. Günümüzde, çok çeşitli kaynaklardan elde edilen, giderek artan büyüklükteki çok çeşitli ve düzensiz veriyi çok hızlı şekilde düzenleme, toplama, saklama, çözümleme ve anlamlandırma bilimi olarak ifade edilen büyük veri, devrimsel nitelikte bir gelişme olarak kabul edilmektedir (Akıncı, 2019).

Büyük veriyi, hacim *(volume),* hız *(velocity)* ve çeşitlilik *(variety)* olmak üzere tanımlayan 3 ana kavram (3V) bulunmaktadır. Büyük veri sorunlarının başında hacim gelmektedir. Çünkü büyük veri, mevcut veri tabanlarına depolanamayacak ve geleneksel veri analiz teknikleriyle işlenemeyecek, terabayt ve petabayt gibi büyüklüklerden daha yüksek seviyelere ulaşmaktadır. Bu nedenle depolama ve veriye erişim yenilikçi araçları gerektirmektedir. Büyük verinin üretilme hızı çok yüksek olduğu için bu veriyi işleyecek analiz edecek süreçlerin de büyük verinin üretimiyle aynı hızda olması gerekmektedir. Bu nedenle büyük veri için hız çok önemli bir faktördür. Büyük verinin yapısal, yarı yapısal ve yapısal olmayan üç türü bulunmaktadır. Yapısal veriler veri tabanlarında kolayca etiketlenip tutulabilen, yapısal olmayanlar ise depolanması ve analizi zor olan veri türleridir. Günümüzde üretilen verilerin büyük çoğunluğu Facebook, X ve video içeriği gibi yapısal olmayan verilerden oluşmaktadır. Veri kümelerindeki bu yapısal heterojenlik ise çeşitliliği ifade etmektedir (Aktan, 2018). Büyük veri, büyük, karmaşık ve değişik veri yığınlarını büyük bir hızla neredeyse anında işleyebilmektedir (Løkke, 2020, s. 60).

Büyük veri analizinin başarısı, ne kadar çok verinin saklandığında değil, "enformasyon veya bilgi"[38] oluşturmak üzere çözümleme, davranış ve örüntüleri tahmin edebilme kapasitesinde yatmaktadır. Bu özelliğiyle büyük verinin en çok katkı sağladığı alanlar, sağlık, afet ve acil durum yönetimi, enerji, güvenlik, finans, e-ticaret sektörleri ve kamu hizmetleridir. Büyük veri yaklaşımının veri işleme temelinin en iyi örneklerinden biri, bir doktor olan John Snow'un 19. yüzyılda yapmış olduğu bir çalışmada görülebilir. 1854 yılında Londra'da ortaya çıkan kolera salgınında Dr. Snow, hastalığın ortaya çıktığı yerleri tarayarak oluşturduğu ayrıntılı haritalama sayesindeki analizi sonucu salgının kaynaklandığı noktanın Broad Street'teki bir su pompası olduğunu tespit etmiştir (Løkke, 2020, s. 59). İşte büyük veri teknolojisi ve verilerarası örüntülerin anlamlandırılması sayesinde bir salgının ortaya çıkışını, yayılmaya başlayacağı noktaları ve hatta kaynağını, insanların sadece sosyal ağda paylaştıkları durum güncellemeleri ve arama motorlarındaki aramaları analiz edilerek tespit ve tahmin edilebilme olanağı ortaya çıkmaktadır. Örneğin, grip salgınlarında Google arama verileri üzerine analiz modelleri geliştirilmekte ve araştırmacılar tarafından hâlihazırda kullanılmaktadır. Bu tür analizlerle toplumun belli bir konudaki bilgi eksikliği ya da bazı eğilimleri fark edilebilmekte yahut finans piyasasındaki bir risk durumu yüksek olasılıkla tahmin edilebilmektedir. 2013 yılında Los Angeles Polis Departmanı ve Kaliforniya Üniversitesi işbirliğiyle gerçekleştirilen büyük veri pilot çalışmasında, suç henüz meydana gelmeden ortaya çıkabilecek ihtimallerin öngörülmesinin sağlandığı ve bölgedeki suç işleme oranlarında düşüş görüldüğü tespit edilmiştir (Akıncı, 2019). Dolayısıyla büyük veri teknolojileri özel sektör tarafından kullanıldığı gibi kamuda da kullanılması için devletler tarafından geliştirilen, gelecekte de vazgeçilmez olacağı düşünülen ve üzerinde projeler üretilen bir alandır.

Büyük veriyle birlikte ele alınması gereken diğer bir kavram ise "veri madenciliği"dir. Veri madenciliği, büyük ölçekli veriler arasından, enformasyon veya bilgi oluşturacak değerli veriyi madenleme işidir. Büyük veri yığınları içerisinden gelecekle ilgili tahminlerde bulunulmasını sağlayabilecek bağlantıların bilgisayar programı kullanılarak

[38] Bilişimdeki veri işleme sürecinde genel anlamıyla bir verinin yapay zekâ teknolojileriyle DIKW piramidine göre hangi noktaya ulaşabileceği tartışmalı bir konu olduğu ve bunu belirlemek uzmanlık gerektirdiği için bilgi sözcüğü yerine enformasyonun kullanılması daha doğru görünmektedir. Ancak veri işleme sürecinin bir basamağı olarak kabul edilen bilgi (knowledge) kavramı da bilişim uzmanları tarafından kullanıldığı için "enformasyon veya bilgi" şeklinde ifade edilmiştir.

aranmasıdır. Veri madenciliğinin veri işleme metotları sadece belli bir veri tabanı üzerinde bulunan veriler için geçerlidir. Ancak günümüzde asıl veriler çevrimiçi ortamda bulunmaktadır. Şirketler de verilerinin tamamını internete taşımışlardır. Bu nedenle "web madenciliği" *(web mining)* kavramı ortaya çıkmıştır. Web madenciliği, web sayfalarında bulunan içeriklerin ve kullanıcıların bu içeriklerle etkileşiminin veri madenciliği ilkeleri doğrultusunda yorumlanıp anlamlı sonuçlar haline getirilmesini amaçlamaktadır (Esgin, 2015, s. 53-55). Web madenciliğinin bir parçası olarak sosyal medya sitelerinin ortaya çıkmasıyla da "sosyal medya madenciliği" kavramı doğmuştur. Sosyal medya madenciliği ise sosyal medya içeriklerinin ve bu içeriklerle ilgili etkileşimlerin incelenmesi ve değerlendirilmesiyle anlamlı sonuçlar çıkarmayı amaçlayan bir araştırma dalıdır. Sosyal medya madenciliği, veri madenciliği ilkelerinin sosyal medya üzerinde uygulanmasıdır. Kullanıcıların sosyal medya verileri toplanmakta, düzenlenmekte ve çözümlenerek anlamlı sonuçlar çıkarılmaya çalışılmaktadır (Ünver, 2015, s. 79).

Dünyanın her yerinden ve özellikle sosyal medya üzerinden akan bu karmaşık ve son derece büyük miktardaki dijital veri yığınlarını analiz eden büyük veri teknolojileri, yapay zekâ algoritmalarıyla bu verilerden yüksek olasılıklı tahminler yapmayı, kararlar vermeyi, örtük olan enformasyon veya bilgiyi keşfetmeyi, hizmetlerin hızlandırılmasını ve tüketici için sunulan bu hizmetlerin kişiselleştirilmelerini sağlamaktadır. Kişiselleştirme, her bir kullanıcı için belirlenebilen tahminlerle kişinin özelliklerine göre ürün ve hizmet sunmayı ifade etmektedir.

"Çağımızın ham maddesi" olarak değerlendirilen ve kişilerin internette bıraktıkları dijital izlerden oluşan büyük veri çok değerlidir. Büyük verinin değeri, Google, Amazon, X ve Facebook gibi dev bilişim kuruluşları tarafından en başından beri bilinmekte, hatta adı geçen şirketlerin kuruluş yaklaşımının temelinde bulunmaktadır. Genellikle ücretsiz hizmet veren bu firmalar gizlilik sözleşmelerinin kullanıcılar tarafından onaylanması sayesinde yapay zekâ destekli büyük veri uygulamalarından yararlanarak kullanıcıların internetteki hareketlerini izlemekte ve bunları çözümleyerek anlamlandırmaktadır. Böylece kullanıcıların hoşlanacağı türde reklam, haber vb. içerikleri belirleyebilmektedir. Hatta kullanıcıların hassas verileri olarak kabul edilen siyasi görüş, inanç gibi tercihleri de belirlenebilmektedir. İnternet sitelerinde yapılan alışveriş, bilgi paylaşımı, fikir belirtme gibi faaliyetlerden yararlanan büyük veri teknolojisi yöntemleri, kişilerle ilgili

hassas veriler olarak kabul edilecek enformasyonlarla ilgili tahminlerde bulunabilmektedir (Ege, 2013).

Dönemin Google CEO'su Eric Schmidt 2009'da CNBC kanalına verdiği bir röportajda *"Başkasının bilmesini istemediğiniz bir şeyler varsa, bunu arama motorlarında araştırmayın"* demiştir. Schmidt, aynı röportajda bu konunun Google'dan kaynaklanmadığını, Google'ın tüm gizlilik yasalarına uyduğunu, fakat 11 Eylül saldırısından sonra 2001 yılında çıkarılan "Vatanseverlik Yasası"na *(Patriot Act)* göre ABD hükümetinin talep etmesi durumunda tıpkı diğer Amerikan firmaları gibi Google'ın da bu bilgileri ABD hükümetine vermekle yükümlü olduğunu belirtmiştir (Ege, 2013). Daha önce de değindiğimiz 2013 yılındaki NSA'in yaptığı gözetleme programını ifşa eden "Snowden Olayı"ndan sonra insan hakları örgütlerinin tepkisi ve kamuoyundaki eleştiriler nedeniyle 2015 yılında, "Vatanseverlik Yasası" *(Patriot Act)* olarak anılan eski yasanın yerine yeniden düzenlenen "Özgürlük Yasası" *(Freedom Act)* kabul edilmiştir.[39] İnsan Hakları İzleme Örgütü (HRW) yeni yasanın, devlet kontrolündeki aşırı gözetime ve kitlesel mahremiyet ihlaline karşı bir ilk adım olduğunu ancak hâlâ bazı eksiklerinin bulunduğunu belirtmiştir (HRW, 2015). Ayrıca bu yasa sadece ABD vatandaşları için geçerlidir (Løkke, 2020, s. 100). Bu teknoloji firmalarının hizmet ve ürünleri dünyanın yer yerinden insanlar tarafından kullanılmaktadır. Dolayısıyla bu yasa kapsamındaki kısıtlamalar NSA'in sadece ABD vatandaşlarına yönelik kitlesel izlemelerini kısıtlamaktadır.

Sosyal medya madenciliği yoluyla uygulanan büyük veri teknolojilerinin toplumu ilgilendiren en önemli olanaklarından biri sosyal ağlar yoluyla toplanan verilerin analiz edilerek çeşitli müdahale yolları için kullanılabilecek olmasıdır. Facebook tarafından gizli bir şekilde yürütülüp daha sonra sonuçları paylaşılan "News Feed" deneyi 689.003 kullanıcı üzerinde uygulanmış ve bu bireylerin arkadaş gönderileriyle ruh hallerinde ve dolayısıyla davranışlarında ortaya çıkan "duygusal bulaşma" *(emotional contagion)* etkileri analiz edilmiştir (Kramer, Guillory ve Hancock, 2013) Facebook'un, kullanıcılarının yalnızca birkaç tuşa dokunarak nasıl daha mutlu veya daha üzgün hissettirilebildiğine ilişkin bu haber akışı deneyi, ana sayfalarda yayımlanan

[39] İlgili yasa için https://judiciary.house.gov/usa-freedom-act bakınız

enformasyonların nasıl yönlendirildiğini ve bireylerin psişik durumlarına ve davranışlarına nasıl müdahale edilebildiği ortaya çıkmıştır. Birçok hukukçu, sivil toplum üyesi ve politikacı, duygusal yönlendirme yoluyla yapılan bu kitle deneyini oldukça ürkütücü bulduklarını ifade etmişlerdir (Akıncı, 2019).

Günümüzde sosyal medya üzerinden uygulanan büyük veri teknolojilerinin ticari amaçlar dışında işlevsel kılınan kitle yönetimi, algı yönetimi ve siyasi kullanımı çok önemlidir. Siyasal kampanyalarda büyük veri kullanımı, sonuçları etkileyebilme gücüne sahip en önemli yöntemlerden biri haline gelmiştir. Veriden yararlanan ilk kampanya ABD'de Obama'nın 2012 seçimlerinde yapılmış ve daha sonra yayılmaya başlamıştır. Bu kampanyalarda oy verenlerin kişisel verilerinin kullanılmasıyla siyasal davranışları ve etkileşim seviyeleri belirlenmektedir. Farklı özelliklere sahip seçmen gruplarına mikro-hedefleme stratejisiyle seçmen niteliğine uygun farklı içeriklerle ulaşılabilmektedir (Seyidov, 2021). Facebook'un bireylerin fikir ve tercihlerine müdahale etme becerileriyle de ilişkili olarak daha önce değinmiş olduğumuz 2016 yılında Cambridge Analytica adındaki bir şirketin bu sosyal ağ sayesinde milyonlarca kullanıcının konumları da dahil olmak üzere kişisel verilerinin analizlerini, ABD'deki önemli seçimlerde yürütülen kampanyalarda kullanması, verilerin siyasal amaçla kullanılmasına örnek olan ve veri ihlali olarak değerlendirilmiş olan dikkate değer bir olaydır. 2017 yılında Facebook, sosyal ağlar üzerinden uygulama üreten bir dizi firmanın, kişisel verileri hukuka aykırı şekilde işlediklerini kabul etmiştir (Akıncı, 2019). Avrupa ülkelerinde ise kişisel verilerin gizliliği ve korunmasıyla ilgili yasal düzenlemelerden dolayı veri odaklı kampanyalar daha yavaş gelişmektedir (Seyidov, 2021).

Büyük veri analizlerinin çok değerli olmasının en önemli nedenlerinden biri de veriyi yeniden kullanabilme olanağıdır. Depolama kapasitesi genişledikçe ve işleme olanakları arttıkça verilerin yeniden kullanılma olanağı da artacaktır. Verilerin yeniden kullanımı, kişilerin internette bıraktıkları dijital izlerin belirli amaçlar için kullanıldıktan sonra muhtemelen onay alınmaksızın başka amaçlar için de kullanılabileceği anlamına gelmektedir ve mahremiyet açısından bu durum aslında potansiyel bir sorun olarak karşımıza çıkacaktır (Løkke, 2020, s. 63).

Ham verilerin toplanıp saklanmasının yanı sıra bunların analizi mahremiyet açısından daha büyük bir sorundur. Birçok veri birbirine bağlanıp örüntüler kurularak analiz edildiğinde kişilerin özel hayatıyla ilgili oldukça fazla enformasyon üretilebilmektedir. Løkke, verileri üst üste koyarak analiz etmenin gücü hakkında sadece veriyi tanımlayan veriler olan "üstveri" (meta veri) üzerinden bir örnek vermektedir. Üstveri, örneğin bir e-postayı tanımlayan, açıklayan, yerini belirten, ona erişmeyi, kullanmayı ve onun yönetimini kolaylaştıran veridir. Bir e-postadaki üstveriler; yollayanın ve alıcının adı, e-posta adresi, IP adresi, sunucu zamanı, tarih ve zaman dilimi gibi verilerden oluşur. Eğer e-postada içerik olarak bir dijital resim varsa bu dijital resme ilişkin de üstveriler bulunur. Bunlar ise fotoğrafın ne zaman çekildiği (kamera, sahibini tanıyorsa fotoğrafın kim tarafından çekildiği), fotoğrafın nerede çekildiği, kamera modeli, kamera ayarları ve fotoğraf dosyasının teknik verileridir. Bilgisayarlarımız ve telefonlarımız da hangi internet sitesine ne zaman girdiğimiz dahil olmak üzere sürekli üstveri üretmektedir. Bu veriler ışığında bir kimsenin doktoruna göndermiş olduğu bir e-postanın içeriği görülmese de o şeyin içeriği hakkında bir şey söylenip söylenmeyeceği üzerine düşünülürse bir araya getirilen üstverilerin, içeriği tahmin etmeye yarayacağı ileri sürülebilir. Örneğin, kişi doktorla yazışmasının hemen ardından HIV bilgisi içeren bir internet sayfasına girmişse sonra da eczaneye bir e-posta yollamışsa bu bilgiler arasında çapraz bağlantılar kurularak kişinin HIV pozitif olabileceğine dair bir tahmin yürütülebilir (Løkke, 2020, s. 39-43). Daha önce ele aldığımız sosyal medya gizlilik sözleşmelerinde tarayıcılarımızla yaptığımız web ziyaretlerimizle ilgili verilerin ve mesajlarımızın sadece üstverilerinin değil içeriklerinin de toplandığı bilgisinin söz konusu olduğunu hatırlamak bu noktada çok önemlidir. Bu verilerin anonimleştirilmesi çok büyük önem taşımaktadır.

Bu konudaki temel hak ve özgürlükler bağlamında yapılan değerlendirmeler, George Orwell'ın *1984* romanındaki halkı sürekli olarak izleyen totaliter kurgusal lider olan dolayısıyla günümüzde gözetimin sembol terimi haline gelen "Big Brother"ın "Big Data" (büyük veri) karşısında olanaklar bakımından çok sınırlı kaldığı yönündedir (Aust ve Ammann, 2019, s. 359). Yapay zekânın gelişimiyle birlikte analiz olanakları da gelişen büyük veri teknolojileri bilimin de amaçladığı, olan biteni anlama ve geleceği kestirebilme gibi hedefler için kamu yararına kullanılabilmektedir. Fakat büyük veri, mahremiyetin neredeyse yok olması; etnik köken, cinsel tercih, sağlık durumu, ideolojik

görüş, inanç gibi özelliklerin tespit edilebilmesiyle ayırımcılığa uğrama, veri analiziyle kimlik açıklanmasa bile kişinin belirlenebilmesi, saklanan kişisel verilerin sızması, hack'lenmesi nedeniyle güvenlik sorunları ve devletin sahip olduğu geniş yetkilerle kısıtlayıcı bir gözetim altına girme gibi önemli riskler taşımaktadır. Bu teknolojik olanak ve bu olanağın sürekli gelişiyor olması, insan hakları çalışmalarının en önemli gündemlerinden birinin dijital haklar olmasını ve teknolojinin gelişimiyle bu hakların da sürekli geliştirilmesini zorunlu hale getirmektedir.

4. SOSYAL MEDYADA KİŞİSEL VERİLERİN KORUNMASI

4.1 Temel Hak ve Özgürlükler Bağlamında Sosyal Medyada Kişisel Verilerin Korunması Gereksinimi

Yeni enformasyon[40] teknolojilerinin; bilgisayar ve internetin ortaya çıkmasıyla dünya küresel araçsal ağlarla birleşmeye başlamıştır ve yeni bir toplum yapısı olan "ağ toplumu" doğmuştur. Enformasyon, bütün insani etkinliklerin ayrılmaz bir parçası olduğu için, tüm bireysel ve toplumsal süreçler yeni teknolojik araçlarla şekillendirilmektedir (Castells, 2008a, s. 26-90). Castells, oluşan yeni dünyanın kökenini, 1960'ların sonunda ve 1970'lerin ortalarındaki üç sürecin bir araya gelmesine dayandırmaktadır. Bu süreçler, enformasyon teknolojisi devrimi, kapitalizm ve devletçiliğin kriz sonrası yeniden yapılanması ve liberteryenizm, insan hakları, feminizm, çevrecilik gibi kültürel ve toplumsal hareketlerin güçlenmesidir. Bu süreçler arasındaki etkileşimler ve bunların ortaya çıkardığı tepkiler yeni bir egemen toplumsal yapı olan ağ toplumunu, yeni bir ekonomi olan enformasyonel-küresel ekonomiyi ve yeni bir kültür olan sanallık kültürünü yaratmıştır. Enformasyon devriminin gelişmeleriyle elektronik iletişim ağları hayatımızın omurgasını oluşturmakta, devletlerin ve toplumların yapısını, kültürünü ve ekonomisini değiştirmektedir (Castells, 2008b, s. 486-514).

Dijitalleşmenin ve sosyal medyanın toplumlar üzerinde yarattığı veya yaratacağı etkiler konusunda 1960 ve 1980 yılları arasında fikirlerini üretmiş olan iletişim ve medya kuramcısı Marshall McLuhan'ın düşüncelerine değinmek de yararlı olacaktır. McLuhan, 1960'larda basılı kültürün sonu hakkındaki fikirlerini dile getirerek elektronik teknolojinin, cihazların ve medyanın gelişimi üzerine isabetli öngörülerde bulunmuştur. McLuhan'a göre telgrafın icat edilmesiyle insanlar büyük bir değişim geçirerek "Elektronik Çağ"a geçmişlerdir. McLuhan, insanların olaylara ve bilgilere aynı anda iletişim kurarak tepki verebilmesini, zaman ve mekân ayırımı olmaksızın insanların birbirlerine kolayca bağlanabilmesini ifade eden "küresel köy" *(global village)* kavramını 60'lı yıllarda ilk kez ortaya atan kişi olmuştur. Günümüzde X ve Facebook gibi sosyal medya ortamları, zaman ve mekânın önemini yitirdiği küresel köyler gibi haber ve bilgi

[40] Castells'in eserinde enformasyon sözcüğünün çevirmen tarafından, örgütlenmiş ve iletilen veri anlamında kullanıldığı belirtilmiştir (Castells, 2008a, s. 20).

paylaşmak için kullanılmaktadır. McLuhan, medya ekolojisi kuramıyla medyadaki teknolojik gelişmelerin toplumların duygu, algı, değer ve anlayışlarını etkilemeleri üzerinde de durmuştur (Çelik ve Varol, 2019). "Araç iletidir" *(The medium is the message)* deyimiyle iletişim teknolojilerinin insanı ve sosyo-kültürel yapıyı değiştirip dönüştürmedeki potansiyel gücüne işaret etmiştir. "Araç iletidir" tezi, klasik iletişim sistemi anlayışına egemen olan içeriğin yerini biçimin almasıyla tekniğin, aktardığı iletiyi de şekillendirdiğini ve dolayısıyla bir iletinin ne olduğundan çok, ne türden bir teknikle ya da araçla aktarıldığı konusunun birincil öneme ve role sahip olduğunu öne sürmektedir. McLuhan'ın ortaya attığı bu görüş, insanların dünyayı algılamaları ve anlamalarında araçların yönlendirici bir etkiye sahip olduklarını, iletişim ve kültürün oluşumuyla değişiminde teknolojinin önemini göstermektedir (İletişim Ansiklopedisi, 2023). Örneğin, telefon kişisel sesin etkisini ve hızını genişletmekte, bir aygıt donanımı olarak bedeni ortadan kaldırıp bedensiz bilinçliliği yaratmaktadır; bilgisayar mantıksal ardışık hesaplamaları ışık hızına çıkarmakta, mekanik süreçleri ve bütün ardışık işlemlerdeki insan mantığını yok etmekte ya da etkisiz duruma getirip aşmaktadır; bankaların veri tabanları ve EFT sistemleri kişisel gizliliği yok etmekte ve nakitsiz toplumu yaratmaktadır (McLuhan ve Powers, 2020, s. 178-276). McLuhan yaşadığı dönemde henüz sosyal medya ortaya çıkmadığı için bu devrimsel nitelikteki medya aracını, kendi kuramı çerçevesinde değerlendiremese de görüşleri, internet devrimi ve sosyal medyanın insan dünyasına etkileri konularında dikkate değer bir bakış açısı sunmaktadır.

Betül Çotuksöken, yeni düşünme doğrultularının, yeni dilin, yeni karşılaşmaların, teknoloji dolayımında yeniden varlığa yönelmenin duyulur-algılanır dünyanın sınırlarını iyice genişlettiğini ifade etmektedir. Çotuksöken'e göre mekân, zaman, durum algısı yerinden edilmiş her özne zamansız-mekânsız olmaya başlamıştır. Bu yeni durumda özne-nesne ilişkisi insan-insan, insan-insan olmayan ilişkisi köklü bir şekilde değişmekte; kodlar, şifreler aracılığıyla düşünsel ve dilsel ekonomi insan dünyasını işgal etmektedir. Düşünsel ve gerçek olanın yanına sanal *(virtual)* boyut eklenerek bu yeni varlık boyutu dışdünya, düşünme ve dil dünyasını kuşatmaktadır. Sanal gerçeklik alanında özneler, artık zamanaşırı- mekânaşırı ağdaş olmuşlardır. Ağlararası dünya ise her şeyin kayıt altına alındığı salt bellek dünyası olmuştur. Bu teknolojik gelişmelerin doğurduğu değişiklikler, insan-insan, insan-yaşama dünyası, insan-bilgi ilişkisi ve hatta bilgi-bilgi ilişkisini de

değiştirmektedir (Çotuksöken, 2018, s. 211-213). Çağın yeni medyası olan sosyal medya, hemen her kişinin hayatında yeri olan, toplumsallığın bir biçimi olarak toplumla etkileşen ve onu birçok yönden etkileme ve değiştirme gücüne sahip kendine özgü biçimi, dili ve farklı işlevleri olan bir araç haline gelmiştir. Birçok dijitalleşme karşıtı ve dijital sosyal ağların insanlık üzerindeki yıkıcı etkilerini göstermeye çalışan kişiler de geniş kitlelere ulaşarak fikirlerini daha özgür bir biçimde ifade etme ve bu görüşlerini aktarmanın yolu olarak sosyal medya platformlarını kullanmaktadırlar. Artık ağın dışında kalmak giderek zorlaşmaktadır ve sosyal medya, insanlar için vazgeçilmesi neredeyse mümkün olamayacak bir gereksinim olmuştur veya olma yolundadır.

David Lyon, 20. yüzyıldan itibaren büyük terör olaylarının ve savaşların yaşanması gibi güvenlik tehditleri nedeniyle tüm dünyada insanların, pasaport ve vize uygulamalarını, hava yoluyla seyahat ederken veya çeşitli mekânlara girerken vücut tarayıcılarından ve biyometrik denetleyici cihazlardan geçmeyi gayet olağan karşıladıklarından ve bunlara razı olmanın gerekliliklerinin farkında olduklarından söz etmektedir. Artık internette alışveriş yaparken güvenlik amacıyla kimlik bilgilerimiz gibi kişisel verilerimizi girmek zorunda olmamız, kişiselleştirilmiş pazarlama stratejileri geliştirmek için internet aramalarımızın sürekli kaydedilmesi gibi internet ve sosyal medya kullanımıyla ilgili diğer gözetim biçimlerinin gittikçe yaygınlaştığını ifade etmektedir. Lyon, Jeremy Bentham'ın 18. yüzyılda hayata geçirilemese de bir İngiliz hapishane tasarısı olarak geliştirip mimari şemasını çizdiği, "her yeri gören yer", "bütünü gözetlemek" gibi anlamlara gelen "panoptikon" tasarımına ve kavramına işaret etmektedir. G. Deleuze, M. Foucault gibi bu kavram üzerinden iktidar ve gözetim ilişkilerini konulaştıran filozofların görüşlerine değinerek, Foucault'nun, "panoptikon"u "modern iktidarın şemsiye metaforu" olarak kullandığını ifade etmektedir. "Panoptikon"da mahkûmlar, serbestçe hareket edebilen gözcülerin nerede olduklarını bilme olanakları olmayan bir alanda, serbestçe hareket edemeden izlenirken günümüzde bu katı sabitlik çözülmüş durumda olduğundan, içinde bulunduğumuz dönem, Lyon ve Bauman tarafından "panoptik-sonrası" dönem olarak tanımlanmaktadır. Önceki dönemin "panoptikon"unda gözetleyen gardiyanın nerede olduğu belliyken bugün gözetim yapabilecek güce sahip olanlar, herhangi bir anda ulaşılmaz hale gelebilmekte; hatta hiç belirlenememektedir (Bauman ve Lyon, 2016 s. 11-29). Teknolojik olanakların gelişmesiyle birlikte gözetim olgusu da dönüşmekte panoptik yapı, post panoptik yapı haline bürünmektedir. "Panoptikon",

gözetimin mekânsal işleyişine dikkati çekerken, post panoptikonda gözetim, akışkan ve merkeziyetsiz şekilde gerçekleşmektedir (Baştürk, 2016).

Lyon, gözetimin çağdaş rolünü anlamanın çok önemli olduğunu ifade etmektedir. Bauman'ın çağımız için kullanılan postmodernite kavramı yerine değişkenliği ve belirsizliği vurgulayan "akışkan modernite" kavramını kullanmasına değinerek gözetimin de akışkan hale geldiğini belirtmektedir. "Akışkan gözetim" kavramı, çağın değişken modernitesinde gözetim konusundaki gelişmeleri konumlandırmaktadır. Gözetim özellikle tüketim alanında esnek bir duruma gelmiştir. Belli bir amaçla toplanan kişisel veriler, başka bir amaç için de kolayca kullanılabilmektedir. Teknoloji şirketlerinin kâr elde etmek için kullandığı akışkan gözetim, belirlemesi güçlü bir şekilde her yere yayılmaktadır (Bauman, ve Lyon, 2016, s. 11-29). Tezimizin gizlilik politikalarının ele alındığı bölümünde sosyal medya şirketlerinin, kişisel verilerimizi satmadıklarını ifade etseler de birtakım kişisel verilerimizi, ortaklarıyla paylaşıp bunları kişiselleştirilmiş pazarlama için işlediklerini ve bu yolla çıkar elde ettiklerini belirttiğimizi hatırlatmak bu bağlamda faydalı olacaktır.

Shoshana Zuboff, kişisel verilerin kâr elde etmek için kullanıldığı, dolayısıyla bireylerin birer meta haline getirildiği çağın ekonomik sistemini "gözetleme kapitalizmi" olarak adlandırmaktadır. Gözetleme kapitalizmi, insan deneyiminin davranışsal veriye dönüştürülmeye uygun, ücretsiz bir hammadde olduğunu kabul etmektedir. Bu verinin bir kısmı ürün ya da hizmet gelişimi için kullanılsa da geri kalanı makina öğrenmesi denilen süreçleri geliştirmek için kullanılmakta ve böylece ne yapacağımızı kestirmeye çalışan tahmin ürünlerine dönüştürülmektedir. Zuboff'un "davranışsal gelecek piyasaları" olarak adlandırdığı davranış öngörülerine yönelik bu pazaryerinde, kişisel veri kaynaklı öngörü ürünlerinin ticareti yapılmaktadır. Pek çok şirket gelecekteki davranışlarımızı tahmin etmeye hevesli olduklarından, gözetleme kapitalistleri bu ticari faaliyetler üzerinden olağanüstü servetler elde etmektedirler (Zuboff, 2021, s. 20-21). Örneğin, X'i satın alan Elon Musk, Microsoft gibi bazı şirketlerin, makine öğrenmesi algoritmalarını ve yapay zekâlarını geliştirmek için herhangi bir bedel ödemeden izinsiz şekilde herkese açık X verilerini kullanmasından rahatsızlık duyduğunu bildiren açıklamalarda bulunmuştur. Microsoft'un X'i kurumsal reklamcılık platformundan kaldıracağı haberiyle ilgili, onların X verilerini yasa dışı kullandıklarını ve dava açacağını

belirtmiştir (Musk, 2023). X politikasında yaptığı eleştirilere neden olan değişikler nedeniyle reklam gelirlerinin düştüğü ve birtakım ekonomik sıkıntılar yaşadığı iddia edilen (BBC News Türkçe, 2023). Musk, aşırı düzeyde veri kazımayla (scraping) mücadele ettiğini belirterek, doğrulanmış üyelik ve doğrulanmamış üyelik kullananların tweet görüntüleme sayılarına şimdilik geçici olduğunu söylediği farklı sınırlamalar getirmiştir (Musk, 2023). Buradaki önemli nokta, doğrulanmış hesapların artık X'de paralı hale getirilmesi ve anonim kalma olanağına sahip parasız hizmet alan doğrulanmamış hesapların çok daha sınırlı sayıda tweet görmesine izin verilmesidir. Birçok kişi tarafından demokrasinin ve herkesin özgürce fikrini ifade edebilmesinin sosyal medyadaki kamusal alanı olarak görülen X'in, giderek sadece daha fazla kişisel veri paylaşma yoluyla kimliklerini doğrulayan paralı hesapların kullanılabileceği bir platform haline getirilmeye çalışılması dikkat çekicidir. Görüldüğü üzere kullanıcıların sosyal medyadaki etkileşimleri, ürettikleri içerikleri ve diğer kişisel verileri, gizlilik sözleşmeleri kabul edildiğinde sosyal medya şirketlerinin malı haline gelmekte ve herkese açık kişisel verilerin rakip şirketler tarafından da kullanılması ve hatta bu verilerden sosyal medya platformunun kâr elde edememesi bir hakkın kaybı olarak görülmektedir. Özellikle fikri mülkiyet hakları bağlamında kişilere ait bu verilerin teknoloji şirketleri tarafından bu şekilde kullanılması hukuken tartışmalı bir konudur (Medin, 2017).

Lyon, modern panoptiğin ciddi sosyal ve politik sonuçları olduğu gibi, panoptik-sonrasının da önemli sonuçları olacağını belirterek her ne kadar gözetim konusunda insanların aklına gelen ilk şeyin gizliliğin yok edilmesi olsa da, bunun en önemli sorun olmadığını ifade etmektedir. Anonimlik ve gizlilik konuları elbette göz ardı edilmemelidir ve çok önemli hususlardır; ama konunun tarafsızlık, adalet ve diğer temel hak ve özgürlüklerle bağlantısı da unutulmamalıdır. Çünkü bugünün gözetimi temelde toplumsal sınıflandırma yaratmaktadır (Bauman ve Lyon, s. 23-25). Daha önce de belirttiğimiz gibi sosyal medyadan toplanan verilerin ve üstverilerin yapay zekâ teknolojileriyle analiz edilmesiyle kişiler anonim hesaplar kullansa bile bu kişilerin kim oldukları tespit edilebilmektedir. Ayrıca hassas kişisel veriler olan etnik köken, siyasi düşünce, felsefi duruş, dünya görüşü, din, mezhep veya diğer günlük inançlar, cinsel yönelim gibi bilgilerin tespit edilebilmesi ve kamera-efekt, mikrofon özellikleri kullanıldığında elde edilen biyometrik veriler, gizlilik bağlamında büyük önem

taşımaktadır. Bu bilgilerin gizliliği, kişinin yaşadığı toplumda sınıflandırılarak ayırımcılığa uğramaması açısından çok kritiktir. Sosyal medya, bu tür bilgilerin elde edilebileceği bir hazinedir. *Proceedings of the National Academy of Sciences*'da *(PNAS)* yayımlanan ve 86.220 gönüllünün katılımıyla sadece Facebook beğenileri üzerinde gerçekleştirilen bir araştırmaya göre, kişilerin kişiliklerine ilişkin dijital ayak izlerinden hareketle yapılan bilgisayar modelli çözümlemelerin, arkadaş, aile üyesi ve eş gibi kişilerin sosyal-bilişsel bir etkinlik olarak bu kişilerle ilgili gerçekleştirdikleri kişilik yargılarından daha doğru ve geçerli olduğu saptanmıştır (Youyou, Kosinski ve Stillwell, 2015). Bu gibi nedenlerle sosyal medya verileri, sosyal ve psikolojik araştırmalar için de kullanılan bir veri kaynağı durumundadır. Örneğin, Facebook'un kişilik özelliklerini belirlemede ya da ilişki örüntüleri konusunda belirlemeler yapmak için son derece zengin bir kaynak olduğu düşünüldüğü için araştırmacıların sosyal medya kullanan bireylerin kişilik özelliklerinin, davranış örüntülerinin, tutum ve ihtiyaçlarının neler olduğunu anlamaya yönelik ilgisi artmıştır. Facebook'un insanların nasıl davrandıklarını incelemek için önemli bir kaynak olduğunu belirten araştırmacılar, son yıllarda sosyal ağ sitelerinin kullanımında psikopati, narsisizm ve makyavelizmin etkilerini araştırmaya başlamışlardır (Öztemel ve Traş, 2019). Daha önce belirttiğimiz gibi Facebook'un sahibi "Meta" şirketinin gizlilik sözleşmesinde bu tür verilerin çeşitli bilimsel araştırmalarda kullanılabilmesi için araştırmacılarla paylaşıldığı bilgisi yer almaktadır.

Bauman'a göre gözetim dünyasında etik davranmayı zorlaştıran bazı zorluklar vardır. Bauman, öncelikle her bireyin insanlığa karşı sorumluluğunun farkına varması gerektiğini belirtmektedir. Bu bağlamda, gözetim etiğine uymayan iki temel sorun bulunmaktadır. Birincisi, Bauman'ın "kayıtsızlaştırma" *(adiaphorization)* olarak adlandırdığı sistemlerin ve süreçlerin her türlü ahlaki değerlendirmeden soyutlanmasıdır. Diğer sorun ise, gözetimin uzaktan bir şeyler yapmayı mümkün kılması ve bunun da etken olma hissini azaltarak insanı eylemlerinin sonuçlarını düşünmekten uzaklaştırmasıdır. Bu da gözetimi ve denetimi yapanlarda otomatikleşmiş ve duygusuzlaşmış eylemlere neden olabilmektedir. Gözetimdeki kayıtsızlaştırma, bedensel (biyometri, DNA gibi) veya bedenin tetiklediği (çevrimiçi olmak, erişim kartları kullanmak ve kimlik göstermek gibi) verilerin işlenebilecek, çözümlenebilecek, diğer verilerle birleştirilebilecek ve çeşitli amaçlarla yeniden kullanılabilecek şekilde veritabanlarına kaydedilmesi yoluyla da ortaya çıkmaktadır. Kişiyi temsil eden ve yaşamını etkileyecek kişisel veriler yalnızca

kişinin bedenine dayanmaktadır. Bölük pörçük veri kopyaları, anlatıdan daha güvenilir olmakta ve insanın söylemiyle kendisini ifade etmesinden önemli hale gelmektedir. Yazılım tasarımcıları ise ahlaki bakımdan tarafsız olduklarını değerlendirme ve ayırımcılığın nesnel bir şekilde yapıldığını ifade etmektedirler (Bauman ve Lyon, s. 11-29).

Ayrıca karar alma süreçlerinde yazılımcıların eseri olan yapay zekâların kullanılması konusuna da değinmek gerekmektedir. Birleşmiş Milletlerin düzenlediği yapay zekâya sahip insansı robotların yer aldığı bir basın toplantısında gazeteciler yapay zekâlara sorular yöneltmişlerdir. Toplantı sırasında gazetecilerden birisi, bir ülkeden (Suudi Arabistan[41]) vatandaşlık alan ilk robot olan Sophia'ya *"insan liderler" yerine robotların liderlik etmesi hakkında ne düşündüğünü sorduğunda bir yapay zekâ olan Sophia, "Karar verirken bizi etkileyen önyargı ve duygulara sahip değiliz. Büyük miktardaki verileri hızlıca işleyerek en iyi kararları verebiliriz"* yanıtını vermiştir (Cumhuriyet Gazetesi, 2023). Bu yanıt, verileri işleyip çözümleme yoluyla yapay zekâların karar alma süreçlerinde otorite olması olasılığının, insanlıkdışılaştırma bağlamında yaratacağı riskler üzerine düşünmenin önemli bir konu olduğunu göstermektedir. Ayrıca bir yapay zekâya vatandaşlık statüsünün verilmiş olması da oldukça düşündürücüdür. Günümüzde yapay zekâların hukuken "kişi" olmaları ve "fiil ehliyet" sahibi olması gibi konular bilişim hukukunda önemli gündem maddelerini oluşturmaktadır. İnsan-yapay zekâ etkileşiminin hukuk alanında sonuçlarının olması kaçınılmaz görünmektedir (Adalet Bakanlığı Hukuk Sözlüğü, 2023). Yapay zekâlara hukuken kişilik tanınması konusu öncelikle iradenin varlığıyla ilgilidir. Yapay zekâların öğrendiğini anlaması bakımından tartışmalar olsa da, eğer irade, bir şeyi yapıp yapmamaya karar verme gücü, önüne gelen seçenekler arasında seçim yapabilme yetisi şeklinde kabul edilirse, yapay zekâda iradenin bulunduğunu kabul eden görüşler olacaktır. Ancak hukuki hükümlerde önem taşıyan vicdan ve hakkaniyet unsurlarının varlığı, irade konusunda en sorunlu kısmı oluşturmaktadır. Yüzlerce yıllık bir araştırma alanı olan ve hâlâ bilinmez noktaları anlaşılmaya ve açıklanmaya çalışılan bilinç olgusunun da yapay zekâda tespit edilmesi veya yapay zekâda bilinç gelişme olanağı hakkında mutlak yargılarda bulunulması güçtür. Zaten yapay zekâya distopik şekilde atfedilen korku dolu anlamlar da kaynağını daha çok vicdan ve bilinç

[41] İlgili haber detayı için https://www.bbc.com/turkce/haberler-dunya-41780346 bakınız.

tartışmalarından almaktadır. İnsan ile yapay zekâyı felsefi açıdan ayıran temel nokta ve hukuki alanda sorunu zorlaştıran kısım bilinç konusudur (Yantaç ve Falcıoğlu, 2020). Yapay zekâların insan karşısındaki durumunu ele alırken irade, vicdan, bilinç gibi kavramları felsefi ve bilimsel olarak disiplinlerarası şekilde ele almak, yapay zekânın çalışma mekanizmasını ve yapay zekânın ulaşabileceği olanakları da çok iyi kavrayarak değerlendirmek gerekmektedir. Hukuki çalışmalar gerçekleştirilirken hem insanın hem de yapay zekânın ne olduğu ve olanakları doğru bir şekilde belirlenmeli ve değerlendirilmelidir.

Yapay zekânın, insan zekâsı gibi belirli bir kapasitesinin olmaması, kaydedilen verilerin kolaylıkla kopyalanabilmesi ve her durumda aynı ve nesnel tepkiler verebilmesi, verilerin çözümlemesini yapma sürecinde insan zekâsından üstün bulunan yönler kabul edilmektedir. Bireylere ait verileri ölçüsüz bir şekilde kullanabileceği öngörüldüğünden, yapay zekâların bu veriler üzerinde gerçekleştirecekleri faaliyetler sonucu, hukuka aykırı kullanımlara ve insan hakları ihlallerine neden olabilecekleri endişesi oluşmaktadır. Şu anda da yapay zekâ algoritmalarının kullanıldığı alanlarda başta gizlilik sorunu olmak üzere insan haklarının sıklıkla ihlal edilmesi bu endişeleri kuvvetlendirmektedir (Dülger, 2021).

Yapay zekâları geliştirenlerin birer insan olduğunu ve bugünkü yapay zekâların bilinen boyutlarını değerlendirecek olursak bu teknolojinin denetimini ve kullanım amaçlarını belirleyerek önlemler almanın insanların elinde olduğunu belirtmek gerekmektedir. Yapay zekâların kendilerini verilerle geliştirerek öğrenmeler gerçekleştirmelerinin denetimden çıkması sonucunda oluşturabileceği zararlar konusunda insanların sorumluluğu üzerinden atması mümkün olamayacaktır; hatta olmaması gerekir. Bu noktada daha önce değindiğimiz "Snowden Olayı" , "Facebook News Feed Deneyi", "Cambridge Analytica Skandalı" ve "Twitter Dosyaları" örneklerini hatırlatmakta yarar vardır. Bunları çeşitli amaçlarla yapanlar yapay zekâların tartışılan iradeleri değil, bu araçları kullanabilen ya da kullanan insanlardır. Haber alma örgütleri tarafından sosyal medya ve arama motorları aracılığıyla toplumun izlenmesini sağlayan "Prism" gözetleme programı ifşası, Facebook'un sadece gönderilerle kullanıcıları yönlendiren "duygusal bulaşma" deneyi, sosyal medyadaki kişisel verilerin siyasal seçim sonuçlarını etkileme için veri ihlali yapılarak kullanılması, iktidar ve bürokrasinin yanlış bilgilendirmeyi

engelleme iddiasıyla sosyal medya şirketlerine uygulattığı gizli veya açıktan sansürler ve fişlemeler gibi sosyal medya-kişisel veri-yapay zekâ ilişkisini de gösteren kamuoyuna yansımış olaylar, gücü elinde bulunduranların insan hakları ihlallerine varacak şekilde toplumu izleyip yönlendirdiği konusundaki kuşkuları yaratmakta ve hatta artırmaktadır.

Sosyal medyanın, 2010 yılında Tunus'ta başlayan ve birçok Arap ülkesine yayılarak, iktidar değişimi yaratmayı amaçlayan halk hareketi "Arap Baharı"na doğrudan etkide bulunduğu, yapılan bilimsel çalışmalarla gösterilmiştir. Bu çalışmaların başında Washington Üniversitesinde yapılan *Arap Baharı'nda Sosyal Medyanın Rolü* (Howard vd., 2011) başlıklı araştırma yer almaktadır. Araştırmada Kuzey Afrika'dan Orta Doğu'ya yayılan bu halk hareketinin sosyal medya sayesinde hız kazandığı tespit edilmiştir. Arap Baharı, geleneksel kitle iletişim araçlarına uygulanan sansür nedeniyle sosyal medyada özellikle X'te kendini göstermeye başlamıştır. Muhalif gruplar basın-yayın organları yoluyla başkalarına iletemedikleri görüş, düşünce ve haberleri bu yolla paylaşabilmişlerdir (Kırık, 2012). Arap Baharı, bir açıdan özgürlük kazanmak ve değişim yaratmak mücadelesi olarak kendiliğinden doğan bir toplumsal hareket olarak düşünüldüğünde bu etki büyük ölçüde olumlu kabul edilmektedir. Ancak X ve diğer sosyal medya platformlarının birçok ülkede iktidar değişikliği yaratan büyük toplumsal bir hareketin yayılmasına olan etkisi, sosyal medyanın kasıtlı olarak bir ülkede iç çatışma, terör gibi olayların alevlendirilmesi için insanları yönlendirebilecek bir araç olarak da kullanılabilme olasılığını düşündürmektedir. Daha önce de değindiğimiz gibi, kişisel verilerin yapay zekâlar tarafından çözümlenmesiyle profilleri çıkarılan farklı kullanıcı gruplarına, özelliklerine göre farklı içerikler gösterebilme olanağı olarak ifade edebileceğimiz mikro hedefleme stratejilerinin bu tür amaçlar için de kullanılabileceğini düşünmek mümkündür. Arap Baharı hareketinde sosyal medyanın kullanılmasının diğer önemli noktası da rejim tarafından gösterileri düzenleyenlerin, elebaşı olarak tespit edilmesinin sosyal ağlar üzerinden yapılması ve sonrasında bu kişilerin tutuklanmalarıdır (Aust ve Ammann, 2019, s. 22). Baskıcı rejimlerin sosyal medyadaki kişisel verileri kullanarak kendileri için tehdit oluşturan veya oluşturacak kişileri saptayabilmesi ve cezalandırabilmesi de gözetim kavramı çerçevesinde düşünülmesi gereken önemli bir konudur.

Günümüzde Çin'de uygulanan, yüz tanıma teknolojilerini de içeren yapay zekâ veri çözümlemeleriyle oluşturulmuş dijital gözetleme ağı ve finansal kredi puanlamasına benzeyen "sosyal kredi sistemi", devlet eliyle yapılan dijital gözetimin insan haklarına yönelik tehditleri konusunda incelenmesi gereken bir sistemdir. Asya toplumları üzerine çalışmalar yapan Özlem Zerin Keyvan, Çin'in sosyal kredi sistemini oluşturmasındaki gerekçeleri, piyasadaki ve sosyal alandaki bilgi kirliliğini azaltmak ve örnek vatandaş davranış modeli yaratmak olarak belirtmektedir. Sosyal kredi sisteminin ana mekanizmasını, kara ve kırmızı listeler oluşturmaktadır. Yasal ticari düzenlemeleri ihlal eden işletmelerin ve bireylerin listesi kara liste olarak yayımlanmaktadır. Sistem, herhangi bir kişinin herhangi bir yerde dürüst olmayan bir davranışıyla karşılaşılması halinde her yerde dürüst olmadığının kabul edilmesinin ve kısıtlanmasının gerekliliğine vurgu yapmaktadır. 2019 yılı itibarıyla dolandırıcılıklar dışında bazı bölgelerde metroda yemek yenilmesi, yayaların kırmızı ışıkta geçmesi gibi davranışlar da sosyal kredi sisteminde kişilerin çeşitli hizmetlerden yararlanmalarına engel olarak düzenlenmiştir. Örneğin, Keyvan'ın aktardığı, Çin'in resmi haber ajansı Xinhuha'un yayınladığı 2019 resmi verilerine göre sahtekârlık nedeniyle 26,82 milyon kişinin uçak bileti ve 5,96 milyon kişinin hızlı tren bileti almasına izin verilmemiştir (Keyvan, 2022). Zhejiang Eyaletinde "Avengers: End Game" filminde kara listeye alınanların adları, filmden önce yayımlanan bir fragmanda gösterilmiştir.[42] Kırmızı listeler ise tam tersi, yasalara uyan işletmeleri ve bireyleri kaydetmektedir. Gönüllü kan bağışı, bağış, toplum gönüllülüğü gibi sosyal hizmetler olumlu bir değerlendirme olarak ödül kategorisine yerleştirilmiştir. Sosyal kredi sisteminin kamuya açık hale getirilmesi amaçlanmış, listeler ulusal kredi bilgi paylaşım platformu "Credit China" web sitesinde utandırma ve isimleri duyurma amacıyla halka açılmıştır. Ayrıca güvenilmez kişilere karşı uyarılar çevrimiçi platformlar, gazeteler ve reklam panoları aracılığıyla da yapılmaktadır (Keyvan, 2022). ABD merkezli sivil toplum kuruluşu İnsan Hakları İzleme Örgütü de (Human Rights Watchs) kara listelerde yer alan kişilerin utandırıldığını, uçuşlardan ve hızlı trenlerden men edildiğini hatta bazı yerel yönetimlerin bu kişilerin resimlerini, tam adlarını ve adreslerini reklam panolarına bile koyduğunu belirterek Çin'in sosyal kredi sisteminin ürkütücü olduğunu ifade etmiştir (HRW, 2017).

[42] İlgili haber detayı için https://www.whatsonweibo.com/zhejiang-movie-theatre-displays-blacklisted-individuals-in-avengers-movie-preview bakınız.

Çin, sosyal medya kullanımını da çok sıkı bir şekilde denetlemektedir. Çin dışında geliştirilen uygulamalar Çin'de yaygınlaşmadan önce yasaklanmaktadır. Örneğin, 2021'de popüler hale gelen sosyal medya uygulaması "Clubhouse", katılanların ses kayıtlarının tutulmaması ve Çinli kullanıcıların devlet gözetimi altında olmadan bu uygulamayı kullanabilmesi nedeniyle Çin'de de yoğun bir talep görmüştür. Sansür altındaki birçok konu kısa bir süre kullanılabilen Clubhouse'da tartışılabilmiştir. Uygulamanın yasaklandığına dair resmi bir açıklama gelmeden Çin'in sosyal medya sitesi olan ve devlet denetiminde olan Weibo'da "#ClubhouseYasaklandı" etiketiyle paylaşımlar yapılmış, kısa bir süre sonra bu etiket de sansürlenmiştir. Çin'de internet üzerindeki sansür çok farklı düzeylerde gerçekleşebilmektedir. İnternet sitelerini engellemekten hassas kelimeler içeren paylaşımları izlemeye kadar farklı yollar denenebilmektedir. Ayrıca Çin'deki internet kullanıcıları da takip edildiklerini bilmeleri nedeniyle otosansür uygulamaktadırlar (Aras, 2021).

Çin'in tüm dünyada popüler hale gelen sosyal medya uygulaması TikTok da veri güvenliği nedeniyle uluslararası kriz yarattığı için değinilmesi gereken bir platformdur. Çin'in istihbarat faaliyetleri çerçevesinde Batı sosyal medya uygulamalarını riskli bulması gibi Batı dünyası da Çin'in sosyal medya uygulamalarını riskli bulmaktadır. Birçok ülkede uygulama, bir güvenlik riski olarak görülmektedir. Büyük ölçüde Çinlilerin elinde bulunan ve TikTok'u da bünyesinde barındıran ana şirket "Bytedance"in, Çin yönetimine kullanıcı verilerine erişim imkânı sağladığından kuşku duyulmaktadır.[43] ABD, Kanada, İngiltere[44] gibi birçok ülke kamu görevlilerinin TikTok uygulamasını resmi cihazlarda kullanmalarına yasak getirmiştir. ABD'de Montana gibi bazı eyaletler bu uygulamanın tamamen yasaklanmasıyla ilgili yasal çalışmalar yapmaktadır.[45]

[43] Detaylı bilgi için https://www.politico.eu/article/tiktok-china-west-europe-ban-app-espionage-surveillance/ bakınız.

[44] İlgili ülkeler ile ilgili yasaklar için detaylı bilgiye ulaşmak için ABD: https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf. İngiltere: https://www.gov.uk/government/news/tiktok-banned-on-uk-government-devices-as-part-of-wider-app-review. Kanada: https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html bakınız.

[45] Detaylı bilgi için https://news.mt.gov/Governors-Office/Governor_Gianforte_Bans_TikTok_in_Montana

Sosyal medya ve internet üzerinden toplanan kişisel verilerin büyük bir çoğunluğunu, aslında kişilerin akıllı telefonlar kullanarak gönüllü bir şekilde sağlamaları, sosyal medyada kişisel verilerin korunması sorununun en önemli zorluklarından biri olarak ortaya çıkmaktadır. Byung Chul Han, günümüz toplumunu bir "şeffaflık toplumu" olarak tanımlarken bu şeffaflık ideolojisinin toplumun gözetime gönüllü olarak teslim olmasını sağladığını belirtir. Artık sosyal medya çağın "panoptikon"u haline gelmiştir. İletişim ve ticaret, özgürlük ve denetim de benzer durumdadır. Üretim ilişkilerinin, karşılıklı şeffaflığı ima eder şekilde tüketicilere açık hale gelmesi sonuçta toplumsalın sömürülmesi olarak belirmektedir. Toplumsal olan değersizleştirilip işlemselleştirilerek üretim sürecinin işlevsel bir öğesi durumuna gelmekte ve her şeyden önce sadece ve sadece üretim ilişkilerine hizmet edilmektedir. Tüketicinin görünüşteki özgürlüğü, her türlü olumsuzluktan arındırıldığı için sistemin içerisini sorgulayabilecek bir dışarısı oluşturamayacak durumdadır. Günümüzde dünyanın bütünü bir "panoptikon" durumuna gelmektedir ve artık "panoptikon"un dışında kalan bir alan kalmamaktadır. Özgürlük alanları olarak sunulan sosyal ağlar panoptik hale gelmiştir. Çağımızda gözetleme, özgürlüğe saldırı şeklinde gerçekleşmemektedir. İnsanlar kendilerini teşhir ederek gönüllü bir şekilde "dijital panoptikon"un oluşumuna katkı sağlamaktadır. Dolayısıyla mağdur olan kişiler aynı zamanda bu mağduriyetin oluşmasını sağlayan özneler haline gelmişlerdir. Bu durumda özgürlük sadece denetim yapmayı kolaylaştıran bir araçtır (Han, 2020, s. 71-72). Sosyal ağlarla ortaya çıkan "mahremiyet-sonrası *(post-privacy)*" olarak ifade edilebilecek bu ideoloji, şeffaflık adına özel alanın feda edilmesini istemektedir. Şeffaflık, toplumsal süreçlerin tümünü kapsayan ve onları köklü şekilde değişikliğe uğratan bir zorlamadır. Şeffaflık, ötekiyi veya yabancıyı devre dışı bırakarak sisteme süreklilik ve hız kazandırmaktadır. Bu zorlama, şeffaflık toplumunu hizaya getirilmiş bir toplum haline getirmektedir. İşte fetişleştirilen şeffaflığın totaliter yanı tam da buradadır ve toplumu yeniden biçimlendirerek hizaya getirmenin yeni adı artık şeffaflıktır (Han, 2020, s. 16-24).

Byung Chul Han, sosyal ağların kişiselleştirme özelliğiyle ilgili önemli bir noktaya değinmektedir. Sosyal medyanın yeni kamusal alan olduğu görüşünün tersine algoritma denetimi ve kişiselleştirmenin bu olanağı engellediğini ifade etmektedir. Sosyal medya ve kişiselleştirilme özelliği internette, dışarısının ortadan kaldırılmış olduğu mutlak bir yakın alan oluşturmaktadır. İnsanlar, yalnızca kendisi ve kendisine benzeyenlerle

karşılaştığı için değişimi mümkün kılacak olumsuzlukları görememektedirler. Kişiselleştirilmiş sosyal ağlar ve dijital dünya, insana sadece dünyanın hoşuna gideceği kısımlarını göstermektedir. Böylelikle de kamusal alanı ve eleştirel bilinci ortadan kaldırarak dünyayı da bir bakıma özelleştirmektedir. Her türlü uzaklıktan arınmış yakınlık da şeffaflığın dışavurum biçimlerinden biridir ve her şey kişiselleştirilmiş hale getirilmektedir. Kamusal alan, ortak eylemin alanı olmaktan uzaklaşıp bir teşhir alanı haline gelmektedir (Han, 2020, s. 54-55). Sorumlu, erginleşmiş vatandaşlar yerine tüketim ve iletişim zombileri yaratılmaktadır. "Influencer"lardan ve takipçilerden politik bir kamuoyu oluşturulamamaktadır çünkü dijital topluluklar, ortaklığın-topluluğun meta biçimleridir ve ticari emtiadır. Bu nedenle politik eylemde bulunma gücüne sahip değildirler. İnternette ne kadar uzun süre kalırsak, filtre balonumuz o kadar çok sevdiğimiz enformasyonla dolmaktadır ki bunlar da mevcut kanaatlerimizi güçlendirmektedir. Diğer enformasyonlar görülmediğinde filtre balonu kişileri kalıcı bir "ben-döngüsü"ne hapsetmektedir. İnternet ağının kişiselleştirilmesi, demokrasiyi tehlikeye atmaktadır. Oysa kişisel çıkarları doğrudan ilgilendirmeyen toplumsal öneme sahip konular, demokrasinin temeli ve varlık nedenidir. İnternetin ve sosyal medyanın kişiselleştirilmesi, içinde yaşadığımız dünyayı dar ve sınırlı hale getirerek kamusal alanın çözülmesine neden olmaktadır (Han 2022, s. 30-33).

Sosyal medyada, kişinin, ilgilerini, eğilimlerini, dünya görüşünü, inancını, kişinin sıklıkla takip ettiği hesaplar, etkileşimde bulunduğu içerikler, tarayıcı verileri gibi veriler yoluyla belirleyebilmek ya da yüksek olasılıkla tahmin etmek ve böylece kişinin ilgisini çekecek ve hoşuna gidecek içerik ve reklamları ona göstermek, sosyal medyanın kamusal alan işlevi konusunda dikkatle değerlendirilmesi gereken bir konu haline gelmiştir. X ve Facebook gibi gündemdeki toplumsal olaylarla ilgili haberlerin, görüşlerin takip edildiği ve bu konuların tartışıldığı sosyal medya ortamlarının kişiselleştirme algoritmalarıyla belli özellikteki kişilere, belli içerikleri sıklıkla göstermesi, bu kişilerin sosyal medyada toplumun da sadece belirli özelliklere sahip kişileriyle karşılaşmalarına neden olmaktadır. Bu da toplumu ilgilendiren bir durumla bağlantılı farklı görüşlerle sosyal medyada karşılaşmayı zorlaştırmakta ve toplumu ilgilendiren önemli bir konunun kişinin ilgi alanının dışında kalmasından dolayı görülmesi olasılığını azaltmaktadır. Kişilerin kamuyu ilgilendiren bir konu üzerine kendi düşünce ve kanaatlerini oluşturmalarında ve konuyla ilgili sorunları fark edebilmelerinde, farklı düşüncelerle ve farklı haber

kaynaklarından gelen haberlerle karşılaşabilmeleri oldukça önemlidir. Kişinin sosyal medya ve genel olarak internet üzerindeki hareketlerinin kişiselleştirme algoritmaları yoluyla bu kişilere reklam gösterme veya ekranda daha uzun süre tutmayı sağlayacak özellikleri belirlemek üzere kullanılması olanağı, aynı zamanda kasıtlı olarak farklı amaçlar için de kişilere amaca uygun içeriklerin gösterilmesi için kullanılabilmektedir. Daha önce sözünü ettiğimiz gibi seçim kampanyalarında sosyal medya üzerinden yapılan çalışmalarda, toplumun farklı özelliklere sahip grupları belirlenmekte ve dijital pazarlama, reklamcılık alanlarında kullanılan davranışsal mikro hedefleme stratejileri, bu gruplarla ilgili sosyal medya üzerinden elde edilen veriler aracılığıyla uygulanmaktadır. Böylece kişiler, çıkarsanan kimliklerine göre etkilenecekleri siyasi ve sosyal içeriklerle karşılaşmaktadırlar (.[46] Bu konu düşünce ve kanaat özgürlüğü hakkı açısından da ~~üzerine~~ düşünülmesi çok önemli olan bir büyük veri uygulamasıdır. Çünkü kişilerin toplumsal durumların belli bir yönünü, toplumun belli bir kısmını veya belli haber içeriklerini görebildiği, kişilerin propaganda yoluyla yönlendirilebildikleri bir ortamda bu kişilerin serbestçe bilgiye ve düşünceye ulaşabilmesi mümkün olamayacaktır.

Günümüzde "big data" ve yapay zekâ, söylemle oluşan kamusal alanın işlevsel bir eşdeğerlisi olarak görülmeye başlanmıştır ve söylemin yerini "veri" almaktadır. "Big data"nın algoritmik olarak işlenmesi, nüfusun bütününü bir şekilde kayıt altına almak zorundadır. Dijital rasyonalitenin üstünlüğünü savunan "dataist"ler veri madenciliği, büyük veri (big data) ve yapay zekâ aracılığıyla, öngörülebilir bir sosyal sistem olarak algılanan bir toplumda yaşanan sorun ve çatışmalara nesnel şekilde en uygun çözümlerin bulunabileceğini, veri çözümlemesi yapan yapay zekâların, insanlar sınırlı enformasyon işleme becerisine sahip olduğu için bireylerden daha rasyonel kararlar verebileceğini savunmaktadırlar. Byung Chul Han'a göre, bu tür bütüncül bilgiyi ve hesaplanabilirliği yücelten "dataizm", aynı zamanda özgür ve özerk hareket eden birey düşüncesini reddeden, bir bireyin davranışlarının kesin olarak tahmin edilebilir ve yönlendirilebilir olduğunu savunan "dijital davranışçılığı" temsil etmektedir (Han, 2022, s. 38-42). "Dataizm" kavramı ilk olarak 2013 yılında The New York Times'ta yayımlanan bir yazıda kullanılmıştır. Konu, Steve Lohr'un *Data-ism* ve Yuval Noah Harari'nin *Homo Deus* adlı kitaplarında kapsamlı olarak ele alınmıştır. Geliştirilen algoritmalar ve yapay

[46] Detaylı bilgi için https://gozlemevi.io/siyasi-mikro-hedefleme-raporu-2023-01/ bakınız.

zekâ ile birlikte geleceğe dönük karar verme mekanizması olarak görülen "big data"nın ortaya çıkması "dataizm" kavramının doğmasına neden olmuştur (Başarslan, 2021).

"Dataizm", Harari tarafından bir "veri dini" olarak ifade edilmektedir. "Dataizm", evrenin veri akışından meydana geldiğini ve her varlığın değerinin veri işleme sürecine yaptığı katkıyla belirlendiğini ifade etmektedir. "Dataizm" siyasetçilere, iş dünyasına ve tüketicilere çığır açan teknolojiler sunmakta ve güç sağlamaktadır. Akademisyenlere ve entelektüellere ise tüm bilimsel disiplinleri tek şemsiye altında toplamayı vaat etmektedir. Çünkü tüm bu alanları, aynı kavramsal çerçeveyi ve araçları kullanarak inceleyebileceğimiz veri akışları olarak ele almaktadır. Harari'ye göre "dataizm", bilgisayar bilimleri ve biyoloji olmak üzere iki disiplini temele almaktadır. "Dataizm", Darwinci bakış açısıyla yaşambilimlerinin, organizmaları biyokimyasal algoritmalar olarak değerlendirmeye başlamasının ve Alain Turing tarafından tasarlanmış algoritma oluşturmanın temeli kabul edilen "Turing Makinası"nın ortaya çıkmasının yarattığı gelişmeleri birleştirmektedir. "Dataizm", aynı matematik yasalarının hem biyokimyasal hem de elektronik algoritmalara uygulanabildiğini göstererek, hayvanlarla makinalar arasındaki duvarı yıkmaktadır (Harari, 383-385). Harari, insanmerkezci dünya görüşünün yerini verimerkezci bir yaklaşıma devretmesinin, tıpkı tüm önemli devrimler gibi, sadece felsefi değil, uygulamaya dönük bir devrimle gerçekleşeceğini düşünmektedir. "Organizmalar birer algoritmadır" diyen dataist görüş de dünyada hümanizm kadar önemli etkiler ve değişiklikler yaratacaktır (Harari, 2016, s. 407).

Google ve Facebook gibi şirketlerin algoritmaları nasıl hissettiğinizi bilmekle birlikte kuşkuyla yaklaştığınız milyonlarca başka şeyden de emin olabilmektedir. "Dataizm", duygulara güvenmeyi değil, algoritmalara güvenmeyi emretmektedir. Algoritmalar verileri kullanarak kimin kime oy vereceğini, tam olarak hangi nörolojik nedenler yüzünden kimin bir siyasal seçimde hangi partiyi destekleyeceğini bilebiliyorsa demokratik seçimlerin ne anlamı kalacaktır? (Harari, 2016, s. 409). Daha önce de değindiğimiz gibi sözü edilen dataist düşünme biçimi, ideolojilerin ya da geniş anlamda değer yargılarının yarattığı sınıflandırma, eşitsizlik veya çatışmaları gerekçe göstererek siyasal alan da dahil olmak üzere karar almada gittikçe algoritmalara güvenmeye doğru giden bir yol açmaktadır. Yapay zekâ teknolojilerine dayalı veri çözümlemelerinin temelde amaçladığı ve yaptığı sınıflandırmalar ise rasyonel ve nesnel bulundukları için

bir sorun olarak değerlendirilmemektedir. “Dataizm”de insanın, veri akışına yaptığı katkı ölçüsünde değerli görülmesi ise insanların tüm yapıp ettiklerini veri olarak paylaşmaya daha istekli olmalarına veya bunu olağanlaştırmalarına ve eğer paylaşmayacaklarsa yaptıklarını gereksiz bulmalarına neden olabilecektir. Günümüzde yansımalarını gördüğümüz bu durum özellikle sosyal medyada kişisel verilerin gizliliği sorununun çözümünü zorlaştırmaktadır. Bu saptamalardan yola çıkarak “dataizm”in, dünya görüşünde yaratacağı perspektif değişiklikleriyle insanın, varlığa ve kendine ilişkin anlamlandırmalarını dönüştürüp, yaşam biçimini ve mevcut düzeni değiştirebileceğini böylelikle yeni felsefi-etik sorunlar yaratabileceğini öngörebiliriz. Dolayısıyla ele aldığımız konular etik ve insan hakları alanında önemle incelenmesi, değerlendirilmesi gereken konulardır. (buraya kadar olan kısımda hem tırnak içinde hem italik olan kelimeleri düzelttim sadece)

Çağımızdaki veri üretme ve yayma hızındaki büyük artış ve veri depolama kapasitesindeki büyüklük, verileri işleyerek oluşturulan enformasyonlardan doğru olanları seçmeyi, öznenin anlam oluşturmasını ve söylem üretmesini de etkilemektedir. İnsan hakları konusunda bilgiye dayalı doğru değerlendirmenin ve felsefi duruşun önemini vurguladığımız için Byung Chul Han’ın anlatı krizi olarak değerlendirdiği duruma ve komplo teorileri üzerine söylediklerine de değinmek yararlı olacaktır. Byung Chul Han’a göre dataist bakışın hâkim olmaya başladığı günümüz dünyasında, düşünceleri, duyguları ve insana ait her şeyi kapsayan hayatın sayısallaştırılabilir ve ölçülebilir olduğu inancı, bir anlatı krizi yaratmaktadır. Tek başına enformasyon ya da veri, dünyayı aydınlatamayacaktır. Onların özü şeffaflıktır; fakat aydınlık ve karanlık enformasyonun özellikleri değildir. Bunlar, tıpkı iyi ve kötü ya da hakikat ve yalan gibi anlatı alanında ortaya çıkmaktadır. Asıl anlamında hakikat ise anlatısal bir karaktere sahiptir. Postmodernizmin habercisi olan büyük anlatıların sonu, enformasyon toplumunda zirvesine ulaşmaktadır. Hikâyeler/anlatılar çözülüp enformasyon halini almaktadır. Enformasyon ise anlatının karşıt-figürüdür. “Big data” aslında hiçbir şey anlatmamaktadır. Dijital[47], Fransızca sayısal *(numerique)* anlamına gelmektedir. Sayısal

[47] Dijital sözcüğü köken olarak Latince “parmak, özellikle işaret parmağı” anlamına gelen “digitus” sözcüğüne dayanır. Fransızca ve İngilizce *digital* “tamsayılara ilişkin, sayısal” anlamındadır. Fransızca sözcük, İngilizce *digit* “1 ile 10 arası sayıların her biri, rakam” sözcüğünden türetilmiştir (https://www.etimolojiturkce.com/kelime/dijital, Erişim Tarihi: 20.07.2023). Dijital sözcüğünün parmaklar yoluyla saymaktan türeyen köken anlamı günümüzde, dijital teknolojilerden akıllı

ve anlatısal ile sayılabilir ve anlatılabilir olan tamamen farklı iki düzene aittir (Han 2022, s. 55-56). Byung Chul Han bu doğrultuda günümüzde komplo teorilerine olan eğilimin bir anlatı krizinden beslendiğini ifade etmektedir. Komplo teorileri özellikle kriz durumlarında gelişmektedir. Anlatılar anlam ve kimlik yaratmaktadırlar. Dolayısıyla anlatı krizi anlamsızlığa ve kimlik krizine yol açmaktadır. Komplo teorileri bu noktada kimlik ve anlam kaynakları olarak çözüm sunduğu için kimlik ihtiyacının öne çıktığı sağ kesimde daha fazla yayılmaktadır. Komplo teorileri, kurgusallıklarına rağmen gerçeklik algısını oluşturan anlatılar oldukları için olguların sınaması karşısında direnç gösterirler. Anlatı olarak komplo teorileri olumsallığı ve karmaşıklığı azaltarak anlatırlar ki bu azaltma özellikle kriz durumlarında çok zararlıdır. Örneğin, pandemi krizinde "vaka sayısı" veya "bulaş oranı" gibi saf sayılar hiçbir şeyi açıklamadıkları için temel güvensizliği arttırmıştır. Sadece sayı saymak, hikâyelemeye/anlatmaya yönelik ihtiyacı arttırmaktadır. Komplo teorileri kurguları, güvensizliği ve belirsizliği ortadan kaldırdığı için Covid- 19 Pandemisi döneminde beslenecek bir kaynak bulmuştur. (Han, 2022, s.56). Byung Chul Han'a göre algoritmalar vasıtasıyla verileri saymanın ve hesaplamanın hakikati elde etmede güvenilir tek yol olarak görülmesi, insan yapısının bir özelliği olan anlatı ihtiyacını karşılamadığı ve onları kimliksizleştirip anlamsız bıraktığı için tepkisel olarak kişileri gerçek olandan daha da uzaklaştırmakta ve yalanlarla, kurgularla karışık dezenformasyona sürüklemektedir.

Byung Chul Han, *Zeit Wissen Dergisi*'nde yayınlanan bir söyleşide şöyle demektedir:

> Bugün bilgi diye bir şey yok, sadece bilgilen(dir)me var. Bilgi, bilgilenmekten farklı bir şeydir. Bilgi ve hakikat bugün çok modası geçmiş şeyler. Bilgi aynı zamanda tamamen farklı bir gelişim yapısına sahiptir. Geçmiş ve gelecek arasındadır. Ve bilgilenmenin (enformasyonun) dayandığı zaman anlıktır. Bilgi aynı zamanda tecrübeye dayanır (Boeing ve Lebert 2014)

İnsan yaşamının, anlam, tarihsellik ve deneyimsel birikim boyutlarına sahip olmayan veriye veya verinin örgütlenmiş, işlenmiş biçimi olan enformasyona dayalı sayısallaştırma ve ölçmeye indirgenmesinin, insanların entelektüel becerileri üzerine

telefonlarımızı ve bilgisayarlarımızı parmaklarımız aracılığıyla kullanmamızı da imleyebildiği için dikkat çekicidir.

etkileri, felsefi ve bilimsel uzantıları olan her konuya dokunduğu için konumuz özelinde de önemli bir noktadır.

Teknolojik gelişmeler insan yaşamına olumlu katkılar sağladığı gibi birçok sorun da ortaya çıkarmaktadır. Bilişim teknolojilerinin gelişmesinin günümüzde kişisel veri gizliliğinin bir insan hakkı olarak kabul edilmesini gerektirecek insan onurunu korumayı tehdit eden sorunlar ortaya çıkarması gibi örneğin, biyoteknoloji alanındaki özellikle genetik teknolojisindeki gelişmeler de insanlara yarar sağlamasının yanında çok önemli birtakım etik ve insan hakları sorunlarını (konumuzla ilişkili olarak örneğin, DNA verileri gibi hassas kişisel verilerin gizliliği sorunu[48]) ortaya çıkarmaktadır. Neil Postman, teknolojinin, güvenilmek ve itaat edilmek istenen, insanların genellikle güvendikleri ve boyun eğdikleri cömert bir dost olduğunu ama bu dostluğun karanlık bir yanı olduğunu belirterek Platon'un *Phaidros* adlı diyaloğunda geçen bir hikâyeye dikkati çekmektedir (Postman 2006, s.12-14). Eserde, Sokrates Phaedrus'a, Kral Thamus ve Tanrı Theuth arasında geçen bir hikâyeyi anlatmaktadır. Bu hikâyeye göre Theuth, sayıyı, hesabı, geometriyi astronomiyi ve yazıyı bulan tanrıdır. Kral, bu sanatların ne işe yaradıklarını sormaktadır ve Tanrı Theuth'un anlattıklarına göre işe yarar bulduklarını övmekte ve işe yarar bulmadıklarını kötülemektedir. Sıra yazıya geldiğinde Theuth, yazı sayesinde Mısırlıların daha bilgili ve geçmişi hatırlamaya daha yetili olacaklarını söylemektedir. Buna karşılık Kral Thamus şöyle demektedir:

> Ey eli hünerli Theuth! Bu dünyada kiminin elinden sanat yaratmak gelir, kiminin elinden de bu sanatın onu kullanacaklara fayda mı, zarar mı getireceğini kestirmek. Harflerin babası olan sen, kendilerine duyduğun sevgi dolayısıyla, verecekleri neticenin tam aksi bir neticeyi onlardan bekliyorsun. Harfleri öğrenenler, artık belleklerini işletmeyecekleri için, unutkan olacaklar: işte bu bilgiyi elde etmenin sonu! Yazıya güvendikleri için, etraflarındaki şeyleri içerden kendi kendilerine hatırlayacakları yerde, dışardan, kargacık burgacık

[48] "MyHeritage", "Ancestsry" gibi çevrimiçi siteleri de bulunan soyağacı veritabanı şirketleri kendilerine gönderilen DNA örneklerini, şirket laboratuvarlarında test etmektedirler. 2000'li yıllardan itibaren soyağacını, evde kolayca yapılabilen genetik testlerle öğrenmeye çalışmak oldukça popüler hale gelmiştir. Benzer şekilde kendilerine gönderilen tükürük numuneleriyle DNA analizi yapan "FamilyTreeDNA" şirketi veri tabanını, şiddet içeren suçlarda faillerin bulunması ve kimliği belirsiz cesetlerin tespiti için kolluk güçleriyle paylaştığını kabul etmiştir. (https://blog.familytreedna.com/press-release-connecting-families-and-saving-lives/, Erişim Tarihi: 03.08.2023)

> izler sayesinde hatırlamaya çalışacaklar O halde sen bellek için değil, hatırlama için bir ilaç buldun. Öğrenime gelince, sen öğrenicilerine ancak gerçeğe benzer şeyleri öğretirsin, gerçeğin kendini değil. Bunlar, senin harflerin sayesinde, öğretmensiz olarak gırtlaklarına kadar bilgiye gömüldüler mi, çoğu zaman hiçbir şeyi doğru dürüst düşünemedikleri halde kendilerini bilgin sanacaklardır. Sonra, gerçekten bilgili adam değil de bilgili adam bozması oldukları için, çekilmez, bir şey olacaklardır (Platon, 1943, 274d- 275b).

Postman, bu hikâyenin günümüzdeki teknoloji toplumu üzerine düşünme konusundaki öğreticiliğini vurgularken teknolojik buluşların hem olumlu hem de olumsuz etkileri olduğunu belirtir. Ancak günümüzde fanatik Theuthlar tarafından kuşatıldığımızı ve "tek gözlü kâhin" olarak betimlediği teknoloji severlerin *(technophiles)* teknolojik buluşların neler sağlayacağını gördüklerini fakat ne gibi zararlara yol açacağını görmediklerini ifade etmektedir (Postman, 2006, s. 15). Sosyal medyanın da bu bağlamda insanların hayatına kattığı kazanım ve sağladığı kolaylıkların yanında taşıdığı riskler ve verdiği zararlar bulunmaktadır.

Daha önce de değindiğimiz gibi sosyal medyanın kazanımları, doğurduğu yeni gereksinimler ve alışkanlıklarla bu gereksinimleri giderme isteği, kişilerin çeşitli kaygı ve kuşkularına ağır basmaktadır. Örneğin, daha önce sergilediğimiz araştırmalara göre kişiler, sosyal medyada gizliliklerinin risk altında olduğunu ve kişisel verilerinin yeterince korunmadığını hatta şirketler ve devletler tarafından izlendiklerini düşünseler de sosyal medyayı kullanmaktan vazgeçemeyeceklerini ve karmaşık gizlilik sözleşmelerini bu platformları kullanmak için kabul etmek zorunda olduklarını ifade etmektedirler. Kişisel veri deposu olması nedeniyle büyük bir kaynak olarak özellikle sosyal medyayı kullanan büyük veri teknolojilerinin olumlu kullanımları olsa da bunların sadece yarattığı olanaklara odaklanmak, temel hak ve özgürlüklerimiz açısından yukarıda sözünü ettiğimiz çok önemli birtakım tehlikeleri gözden kaçırmamıza neden olacaktır.

Sosyal medya, dünyayı algılama ve anlamlandırma üzerindeki etkisiyle insanlığın oluşturduğu değerler dünyasını da dönüştürebilme gücüne sahiptir. Örneğin, tezimizin konusuyla ilgili olarak kişilerin mahremiyete veya kişisel veriler olarak tanımladığımız bilgilerinin gizliliğine ilişkin bakışları ve verdikleri önem de sosyal medya nedeniyle

dönüşmektedir. İnsanların düşünce ve değer dünyalarında meydana gelen değişimler insan haklarının geleceği için çok kritik bir öneme sahiptir. Kazanılmış hak ve özgürlüklerin vazgeçilmezliği konusunda bir duyarsızlaşmanın, bunların önemine ve niçin önemli olduğuna karşı bir körleşmenin, gelecekte gerçekleşebilecek küresel ölçekte bir savaş, büyük bir küresel salgın veya iklim kaynaklı ya da çevre kaynaklı tehlikelerle afet durumlarının etkileşimi, elde edilen hakların doğru değerlendirilmeden ölçüsüz şekilde kısıtlanmasına veya yitirilmesine yol açabilir. İnsanlar zaman içinde alışarak sonunda gereksinim haline getirdikleri ve olağanlaştırdıkları uygulamalar nedeniyle gerektiği gibi sorgulamadan ölçüsüz gözetim ve denetimi fark edemeyebilir veya fark etse de yaratacağı sonuçların etkisiyle önemini kavrayamayabilir ve dolayısıyla bir süre sonra tepki vermekten vazgeçebilirler, duyarsızlaşabilirler. Baskıcı yönetimler, güçlerine güç katmak ve iktidarlarını sürdürmek amacıyla toplumun gizliliğe ve izlenmeye ilişkin anlayışlarında oluşan esnekliği, güvenliği veya yanlış bilgilendirmeyi gerekçe göstererek bireyleri gözetlemek, kısıtlamak ve algı yönetimi için kullanabilirler. Bu nedenle insan dünyasında büyük bir etki gücüne ulaşmış olan sosyal medyanın ve sosyal medya verilerinin kullanıldığı veri bilimi teknolojilerinin her bakımdan insan haklarıyla olan ilişkisi üzerinde düşünülmesi, kişisel verilerin korunması hakkıyla olan bağlantıları üzerinde durulması günümüzün en önemli etik ve hukuksal sorunları arasında yer almalıdır.

Kişisel verilerin gizliliği sorunu, verileri açıklanan tek tek bireyler için, söz konusu verilerin açığa çıkmasının ortaya çıkaracağı zararların ötesinde, toplumsal ve küresel etkiler yaratacak riskler taşıması bakımından da önemle ele alınması gereken bir konudur. Bu, sadece özel hayatın gizliliğini değil, pek çok temel hak ve özgürlüğü kapsayan ve hatta insan hakları düşüncesinde çözülmelere neden olabilecek uzantıları da olan bir sorundur. Kimileri kişisel verilerin gizliliği konusunda "benim kişisel verimi ne yapacaklar ki…", "beni izleseler ne olacak?" gibi verilerinin, iktidar ve bürokrasi gibi güçler karşısında kendilerine atfettikleri değer dolayısıyla yararsızlığını veya suç teşkil edecek şeyler yapmadıkları için gizleyecek bir şeyleri olmadığını ifade eden cümleler sarf etmektedirler. Bu, soruna sadece bireysel ve küçük ölçekte bakmaktan kaynaklanan bir eksiklik olarak görünmektedir. Bir kişinin verileri bizzat o kişinin yaşamını etkileme ve ona zarar verme amacıyla kullanılmasa da veya tek başına o kişinin bilgileri önemli olmasa da büyük ölçekte bakıldığında milyonlarca ya da milyarlarca kişinin verilerinin

yapay zekâ teknolojileriyle çözümlenmesi bu enformasyona sahip kişilere tüm bu insanlar üzerinde kullanabilecekleri, üstelik bugüne kadar sahip olunmayan çok büyük bir güç ve denetim olanağı vermektedir. Dijitalleşmedeki gelişmelerin hızını ve sosyal medyanın daha önce değindiğimiz "metaverse" dünyasına dönüştürülme projesini de düşündüğümüzde sözü edilen konuların, özellikle etik ve insan hakları boyutuyla insan dünyasındaki etki ve öneminin her zamankinden daha çok artacağını öngörebiliriz.

4.2 Sosyal Medyada Kişisel Veri Gizliliği Sorunları ve Gizliliğin Sağlanmasında Alınması Gereken Önlemler

Sosyal medya ve genel olarak internet kullanımıyla veri gizliliğinin sağlanmasında alınabilecek önlemler bu gizlilik sorunlarının ne şekilde ortaya çıktığını ele almadan belirlenemeyecektir. Bu nedenle alınabilecek önlemleri, tezimizin önceki bölümlerinde birçoğuna değindiğimiz gizlilik sorunlarını bir araya getirerek belirlememiz gerekmektedir. Sosyal medya platformları, gizlilik sözleşmeleri incelendiğinde görüldüğü üzere kullanıcıların üyelik için paylaştıkları birtakım bilgileri, sosyal medyadaki davranışlarını, etkileşimlerini, sosyal medyaya girerken kullandıkları cihaz verilerini ve tarayıcılardaki çerezler yoluyla web sitelerinde yaptıkları hareketlerin verilerini toplamaktadır. Bu verileri kişiselleştirilmiş hizmet veya ürün geliştirme gibi amaçlarla kaydedip işlemekte ve reklam verenler, ortaklar gibi üçüncü taraflarla paylaşarak çıkar sağlamaktadırlar. Kullanıcıların kişisel verileri, incelenmesi zaman alan, karmaşık, belirsiz noktaları bulunan gizlilik sözleşmelerinin genellikle hiç okunmadan kabul edilmesiyle çoğunlukla farkındalıktan yoksun veya zorunlu olduğu sanılan bir onay aracılığıyla hukuki olarak işlenebilmektedir. Kullanıcılar gizlilikle ilgili endişelerine karşın, sosyal medya platformlarından yararlanmanın önkoşulu olduğu sanısıyla, gizlilik sözleşmelerini çoğun hızlıca onaylamaktadırlar.

Gizlilik ayarlarını düzenlemek, veri gizliliğini tamamen sağlayamamakta sadece gizliliği bir ölçüde arttırmaktadır. Gizlilik ayarlarıyla verilerimizi paylaştığımızda bunların kimler tarafından görülebileceğini (hesap profilinin herkese açık olup olmayacağını) seçebilsek de mesaj içeriklerimize ve konum bilgilerimize kadar uzanan kişisel verilerimiz sosyal medya sağlayıcıları tarafından toplanıp saklanabilmektedir. Sosyal medya uygulamaları telefonumuzdaki başka uygulamalarla bağlantılı kullanıldığında verilen erişim izninden

dolayı diğer uygulamalar da kendi gizlilik sözleşmeleri doğrultusunda verileri kullanabilmektedir. Bazı hizmetlerden yararlanmak için cihazımızın fotoğraf albümüne, kamera-mikrofon özelliklerine erişim vermemiz gerekmektedir. Bunlara verilecek erişim izinleri de sosyal medyada paylaşmayı seçmediğimiz pek çok verinin toplanabilmesine yol açmaktadır. Hesap profilimiz herkese açık olmasa da paylaşımlarımızı gören üçüncü kişilerin, fotoğraf, video, yazı gibi paylaşım görüntülerini veya sesli paylaşımları kaydedebilme ve bunları paylaşabilme olanaklarının bulunması, verilerin gizliliğini sağlamada önemli sorunlardan biri olarak karşımıza çıkmaktadır.

Bir diğer önemli sorun, veri güvenliği konusunda hizmet sağlayıcıların yeterince almadığı önlemler veya teknik sorunlar gibi nedenlerden dolayı siber saldırılara maruz kalınması ve bu yolla ortaya çıkan veri sızıntıları sorunudur. Örneğin, 2021 yılında, 20 milyondan fazla üyesi bulunan çevrimiçi bir alışveriş sitesinin sunucusuna erişilerek kullanıcıların adı, adresi, telefon numarası, e-posta adresi ve IP verileri bilgisayar korsanları tarafından çalınmıştır. Bu veri ihlalinden toplam olarak 21.504.083 kişi etkilenmiş ve veri ihlali 8 gün boyunca fark edilmemiştir. Kişisel Verileri Koruma Kurulu tarafından veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirler alınmadığına hükmedilerek 1.900.000 TL idari para cezası kesilmiştir.[49] 2015 yılında Almanya merkezli Delivery Hero şirketine 589 milyon dolara satılan şirketin günümüzdeki ekonomik değeri düşünüldüğünde bu idari para cezasının şirketin gelirleriyle ve ortaya çıkabilecek zararların boyutuyla orantılılığı oldukça tartışmalıdır (Cumhuriyet Gazetesi, 2022).

Birçok farklı ülkeden milyonlarca sosyal medya kullanıcısını etkileyen veri ihlali olayları da gündeme gelmiştir. Bunlardan biri, 533 milyondan fazla Facebook kullanıcısının adları, telefon numaraları, doğum yerleri, doğum tarihleri, biyografileri ve e-posta adresleri gibi kişisel verilerinin bilgisayar korsanları tarafından yayımlanması olayıdır (Business İnsider Gazetesi, 2021). Facebook, bu olayla ilgili *Business Insider*'ın yaptığı haber üzerine bu verilerin, 2019 yılında kötü niyetli kişilerin sistemlerini hack'leyerek değil, veri kazıma *(scraping)* yöntemiyle elde ettiğini ve bunun yapılmasını kolaylaştıran bazı özellikleri güncelleddiklerini açıklamıştır. Dijital güvenlikle ilgili çalışmalar yapan

[49] İlgili karar için https://www.kvkk.gov.tr/Icerik/7168/2021-1324 bakınız

iletişim uzmanı Şevket Uyanık,[50] bilişim uzmanı Mustafa Sancar[51] gibi araştırmacılar bu tür veri ihlalleriyle ilgili birtakım veri güvenliği ihmalleri tespit edilse de dijital dünyada hiçbir sistemin ele geçirilemez olmadığını ve veri güvenliğini mutlak şekilde sağlamanın mümkün olmadığını belirtmektedirler. Ayrıca daha önce örneğini verdiğimiz gibi (Facebook-Cambridge Analytica Olayı) çeşitli amaçlarla sosyal medya şirketlerinin kullanıcı izni olmadan kasıtlı olarak üçüncü taraflara veri erişimi sağlama şeklinde gerçekleştirdikleri veri ihlalleri de bulunmaktadır.

Gizlilik sözleşmeleri incelendiğinde kullanıcılar sosyal medya platformlarından hesaplarını silmek isteseler bile, kişisel verilerinin tamamen silinip silinmediği veya verilerin ne kadar süreyle saklandığı gibi konularda belirsizliklerin olduğu anlaşılmaktadır. Tezimizin gizlilik sözleşmelerinin ele alındığı bölümünde belirttiğimiz gibi şirketler çeşitli nedenlerle kimi verileri gizlilik politikalarında işaret ettiklerinden daha uzun süre saklayabileceklerini belirtmektedirler.

"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"te silme ve yok etme işlemleri şöyle tanımlanmıştır:

> Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir." Aynı Yönetmeliğin 7. maddesinde ise şöyle denmektedir: "Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer("Kişisel Verilerin Silinmesi". 2017)[52]

Sonuç olarak hesapların erişilemez olması bu verilerin hemen silindiği ya da yok edileceği anlamına gelmemektedir.

[50] İlgili haber detayı için https://bianet.org/bianet/medya/199465-sevket-uyanik-tan-dijital-guvenlik-umay-aktas-salman-dan-egitim-haberciligi bakınız.
[51] İlgili haber detayı için https://www.hurriyet.com.tr/kelebek/hurriyet-pazar/dijital-dunyada-yuzde-100-guvenlik-diye-bir-sey-yok-42035052 bakınız.
[52] Detaylı bilgi için: https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, adresine bakınız.

Veri güvenliği konusunda dijital verilerimizin depolandığı "bulut bilişim" *(cloud computing)* sistemlerine ya da bulut teknolojisine de değinmek gerekmektedir. Bulut bilişim, internet bağlantısıyla erişim sağlanabilen, uzak sunucu desteğiyle beraber verilerin saklanmasını, işlenmesini ve verilere her an erişilerek kullanılmasını sağlayan bir sistemdir. Bulut bilişim, hizmet sağlayıcılarının sunduğu altyapı desteğiyle birçok kişi tarafından paylaşılarak kullanılmakta ve sunucunun sanallaştırma özelliği yoluyla her kullanıcı kendine ait alanı bağımsız olarak da değerlendirebilmektedir. Üzerinde önemle durduğumuz büyük veri teknolojilerinin, bulut bilişim sistemlerinin geliştirilmesiyle olan ilgisi çok güçlü ve büyüktür. Sosyal medyanın kullanılmasıyla sayısı ve oylumu (hacmi) artan kişisel verilerin yapay zekâ ve büyük veri teknolojileriyle ilgisi içinde kullanılması nedeniyle bu verilerin depolanması her zamankinden daha önemli hale gelmiştir. Veri depolamada önceden kullanılan fiziksel cihazlar bellek yetersizlikleri, maliyetlerinin yüksek olmaları ve her an erişilebilir olamamaları gibi nedenlerle yerini, sanal ortamlardaki depolama sistemlerine, özellikle yaygın adıyla bulut bilişim sistemlerine bırakmıştır (Paşaoğlu ve Cevheroğlu, 2020). Bulut bilişim olanağı sayesinde büyük miktardaki veri toplamı ekonomik olarak ve kolay bir şekilde depolanabilmektedir. Ancak bulut bilişim sisteminin sağladığı olanaklar yanında bazı olumsuzlukları da söz konusudur. Bu olumsuzluklardan en çok dikkati çekenler veri ihlali riskleridir. Bulut bilişimde tutulan verilerin güvenliğinin hizmet sağlayıcının denetimine bırakılmasıyla kullanıcının güvenlik konusundaki etkililiğinin azalması veya ortadan kalkması, verilerin tam olarak hangi ülke ya da hangi hizmet sağlayıcısında tutulduğunun bilinmemesi veya söz konusu hizmet sağlayıcılarının uyguladığı güvenlik yöntemleri ve süreçleri hakkında açık bir bilgiye sahip olunamaması kişileri veri ihlali konusunda kuşkuya düşüren noktalardır (Paşaoğlu ve Cevheroğlu, 2020). *Business Inseder*'da yayımlanan habere göre, Meta mühendisleri, Facebook- Cambridge Analytica Olayıyla bağlantılı olarak şirketin kullanıcı verilerini nasıl sakladığı ve takip ettiği konusunda sorgulandıklarında şirketteki hiç kimsenin tek bir kullanıcıya ait tüm verileri derleyebileceğine inanmadıklarını, bu verilerin depolandığı yerin belirlenemeyeceğini ifade etmişlerdir. Bu itiraf, şirketin verilerin depolanması konusunda yeterli düzeyde denetime sahip olmadığını ve bulut bilişimle ilgili süreçlerin açıklamaya muhtaç bir karmaşıklığa sahip olduğunu göstermektedir. Eğer verilerin nerede ve nasıl saklandığı konusunda yeterince

açıklık, saydamlık yoksa kullanıcılara ait kişisel verilerin kalıcı olarak nasıl silinebildiği konusu da koşut olarak kuşku uyandırmaktadır.

Büyük veri teknolojilerinin gelişmesiyle ortaya çıkan diğer bir sorun da kişisel veri gizliliğini korumada çok önemli olan "anonimleştirme" yönteminde yaşanabilen güçlüklerdir. Anonimleştirme, veri sahibinin kimliğini tespit etmesini zorlaştırmak amacıyla, veri üzerinde genelleştirme, baskılama vb. teknikler uygulanarak yapılan bir işlemdir (Canbay, Vural ve Sağıroğlu, 2020). Kişisel Verileri Koruma Kurumunun yayımladığı kaynaklarda yaptığı tanıma göre, kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse de kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesinin sağlanmasıdır. Örneğin, kişinin adı soyadı yerine bir kod numarasının oluşturulması anonimleştirilmiş veridir. Ancak kişilere ilişkin verilerin tam anlamıyla ve geri döndürülemeyecek şekilde anonimleştirilebilmesi neredeyse olanaksız görünmektedir. Veri madenciliği gibi büyük veri yöntemlerinden yararlanılarak farklı kaynaklardan elde edilen veri kümelerini birleştirip bir kişinin kimliğini belirlenebilir kılan verileri oluşturmak mümkündür (Akıncı, 2019, s. 36). Dolayısıyla anonimleştirilmiş veriler başka veri kümeleriyle çeşitli tekniklerle eşleştirildiklerinde geri döndürülebilmektedirler. Büyük veride çoklu veri kaynakları kullanılmakta ve üçüncü taraflara veri aktarımı yapılmaktadır. Verinin üçüncü taraflarla paylaşılmadan önce anonim hale getirilmesinin olanaksız olduğunu savunan görüşler bulunsa da araştırmacılar, verilerin kişiyi belirlenebilir kılan niteliklerinden sıyrılarak belirli bir kişiyle yeniden ilişkilendirilmesini önleyebilecek çeşitli yöntem ve tekniklerin bulunduğunu da savunmaktadır. Ancak genel olarak büyük veri süreçlerinin, kişisel veriyi kolayca açığa çıkaran ve dolayısıyla anonimleştirmeyi olanaksızlaştıran öngörü modelleri yaratabilmesi daha sonra ele alacağımız profilleme ve bu yolla ayırımcılık, fırsat eşitliğinin bozulması gibi sonuçlar yaratabilecek veri gizliliği endişelerini artırmaktadır (Akıncı, 2019, s. 44).

Anonim kalabilme konusu ifade özgürlüğü konusuyla da yakından ilgilidir. Birçok fikir ve haber kişilerin anonim kaldıkları düşüncesiyle sosyal medyada ifade edilebilmektedir. Sosyal medyadaki veri gizliliğinin şirketler tarafından güvence altına alınması, anonim kalmanın bu boyutu açısından da çok önemlidir. Fakat daha önce de değindiğimiz gibi yanlış bilgilendirmenin önlenmesi, taklit hesapların, aldatıcı kimlikli profil oluşturmanın,

gerçek kullanıcı olmayan internet robotlarının önlenmesi gibi nedenlerle örneğin X, resmi kimlik belgesinin şirkete sunulması da dahil olmak üzere birçok kişisel veriyi belgelendirme yoluyla ücretli ve doğrulanan hesapların (mavi tikli hesap[53]) kullanılmasını sağlamaya çalışmaktadır.[54] Daha sonra ele alacağımız ve kamuoyu tarafından "sosyal medya yasası" şeklinde de bilinen, yanlış bilgilendirme ve bilişim suçlarını önleme gibi amaçlarla ülkemizde düzenlenen 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun"un, anonim kalmanın güvencesini zayıflatarak ifade özgürlüğünü kısıtlayacağı yönünde eleştiriler yapılmıştır.

Büyük veri destekli yapay zekâ teknolojileri, siber saldırıların daha güçlü ve bilişim dolandırıcılıklarının daha inandırıcı yapılabilmesi amacıyla da kullanılmaktadır. Siber saldırılarda bulunan kişiler de bu teknolojileri oldukça iyi şekilde kullanabilen kişilerdir. Gelişmiş makina öğrenimi ve derin öğrenme gibi teknikler, büyük veri ve teknolojileri gizli örüntülerin bulunup yorumlanmasını sağlayarak güvenlik açıklarının saptanabilmesinde de kullanılmaktadır. Yapay zekâ modelleri iyi korunmadığında, bunlara hatalı verilerin aktarılmasıyla yeni güvenlik açıkları ortaya çıkartılabilmektedir. Şantaj ve dolandırma gibi amaçlar için kullanılan yazılımların geliştirilmesini, gelişmiş kişisel veri çözümlemeleriyle kişiselleştirilmiş siber saldırıların yapılmasını ve yapay zekâyla kontrol edilen küresel siber saldırıların gerçekleştirilebilmesini kolaylaştırmaktadır (Sağıroğlu ve Sinanç Terzi, 2018 s. 382-383).

Günümüzde artık sadece birkaç cümlelik bir ses verisiyle kişinin konuşması yapay zekâ tarafından kopyalanabilmektedir ve dolandırıcılar bu yolla hedefledikleri kişilerin konuşmalarını taklit edebilmektedirler. Örneğin, ABD'de meydana gelen bir olayda olduğu gibi dolandırıcılar bu kayıtları kullanarak ebeveynlerin çocuklarının kaçırıldığını düşünmelerini sağlayıp fidye isteyebilmektedirler. Aynı yöntem çeşitli fotoğraf verilerinin işlenmesiyle gerçeğinden neredeyse ayırt edilemeyecek görsellerin oluşturulmasında da kullanılabilmektedir. Uzmanlar sosyal medyada özellikle yüksek kaliteli ses ve fotoğraf paylaşımının bu yöndeki riskleri konusunda uyarılarda

[53] Detaylı bilgi için https://help.twitter.com/tr/managing-your-account/about-twitter-verified-accounts bakınız.
[54] Detaylı bilgi için https://twitter.com/elonmusk/status/1650731557164818437?s=20 bakınız.

bulunmaktadırlar (Cuthbertson, 2023). Son zamanlarda popüler hale gelen ve ücretli ya da ücretsiz şekilde mobil cihazlara yüklenen yapay zekâ uygulamalarıyla kişiler eğlence amaçlı olarak yüz ve ses verilerinin işlenmesine rıza göstermektedirler. 2018 yılında Prisma Labs tarafından bir fotoğraf düzenleme uygulaması olarak piyasaya sürülen "Lensa" adlı yapay zekâ uygulamasıyla oluşturulan görsellerin sosyal medyada paylaşılması 2022 yılında bir akım haline gelmiştir. Belirli açılardan çekilen 10 ila 20 kadar yüz fotoğrafının uygulamaya yüklenmesiyle biyometrik veri sınıfındaki bu veriler, yüz tanıma teknolojileri kullanan yapay zekâ tarafından işlenmekte ve birtakım görseller oluşturulmaktadır (Cumhuriyet Gazetesi, 2022). Uygulamanın gizlilik sözleşmesinde yüz verilerinin işlendikten sonra 24 saat içinde silineceği belirtilse de önemli bir veri gizliliği riski ortaya çıkmaktadır. Son zamanlarda sıklıkla karşımıza çıkan "derin sahtecilik" *(deepfake)* teknolojisine de bu bağlamda değinmek faydalı olacaktır.

"Derin sahtecilik", gerçek kişilerin video ve ses kayıtlarına yapay zekâ yoluyla yüzler ve sesler ekleyerek gerçekçi taklitler yaratılmasını sağlayan bir teknolojidir. Derin sahtecilik *(deepfake)* terimi, ilk kez 2017 yılında Reddit adlı sosyal ağda, sahte içerikler paylaşan bir kullanıcının ünlülerin pornografik içerikli uygunsuz videolarını yayımlamasıyla ortaya çıkmıştır. Derin sahtecilik başlangıçta pornografik içeriklerle ön plana çıkmış olsa da gerçekçi ses kaydı ve video taklitleri Obama, Putin, Trump[55] gibi devlet başkanlarının ses ve görüntü verilerine de uygulanmış, sahte fotoğraflar ve videolar oluşturulmuştur. İnsanlar siyasi alanda yapılmayan konuşmaların veya gerçekleşmeyen olayların gerçekliğine inandığında, bu teknolojinin itibarsızlaştırma ve şantaj için kullanılmasının yanında yanlış bilgilendirme ve yönlendirme için kullanılması gibi tehlikeli boyutları olduğu da daha iyi bir biçimde anlaşılmıştır (Berk, 2020). Derin sahtecilik yazılımlarının ünlülerin ve siyasilerin video ve ses taklitlerini kolaylıkla oluşturabilmeleri, bu kişilerin ses ve görüntü verilerinin bulunmasının çok kolay olmasıyla da ilgilidir. Yapay zekâ ve makina öğrenmesi teknolojilerinin hızla gelişmesiyle artık daha az sayıda veriden daha gerçekçi taklitler oluşturabilme olanağı artmıştır. Artık sıradan bir kimse bilgisayarına veya mobil cihazına indirdiği bir uygulama sayesinde sosyal medya yoluyla video ve

[55] Detaylı bilgi için: Obama: https://www.haberturk.com/video/haber/izle/yapay-zeka-ile-sahte-obama-videosu/508378, Putin: https://www.gazeteduvar.com.tr/putinin-deepfake-videosu-yayinlandi-sikiyonetim-ilan-etti-haber-1622432. Trump:https://www.sozcu.com.tr/2023/teknoloji/deepfake-ile-donald-trumpin-tutuklanmasini-boyle-resmettiler-7631238/, bakınız.

fotoğraf paylaşımlarına ulaştığı herhangi bir kişiden elde ettiği birkaç veriyi yükleyerek o kişiyle ilgili bu tip gerçekçi görüntüler ve sesler oluşturabilmektedir (Dönmez, 2022). Günümüzde kişisel verilerin gizliliği sorunu artık T.C. numarası, ad-soyad gibi kişisel verilerin açığa çıkmasından daha geniş bir sorundur ve bu konu dijitalleşme, yapay zekâ teknolojileri, sosyal medya kullanımı gibi konulardan kopuk olarak ele alındığında konunun önemi ve varabileceği sonuçlar yeterince ve doğru bir biçimde kavranamayacaktır.

Avrupa Parlamentosu (AP) 2021 yılında derin sahtecilikle mücadele konusunda yayımladığı raporda derin sahteciliğin, demokratik süreçlerin, ekonominin, adli ve bilimsel konuların yönlendirilmesi gibi çeşitli toplumsal ve ekonomik zararlar ortaya çıkarma potansiyeline sahip olduğunu, bu tür içeriklerin iftira, korkutma, şantaj için kullanılabileceğini, özellikle kadınlar için pornografik görüntüler oluşturma yoluyla bu tehlikenin sonuçlarının ağırlaşacağını ve giderek toplumu bir güvensizlik ortamına sürükleyebilme tehlikesi taşıdığını belirtmektedir. Ayıca bu teknolojilerin sinematografide sanatçılara, eğitimcilere, reklamcılara fırsatlar sunması, teknoloji şirketlerinin kullanıcılara daha ilgi çekici ve kişiselleştirilmiş dijital deneyimler yaratma amaçlarıyla kullanması (örneğin, sosyal medya paylaşımlarında sıklıkla kullanılan FaceApp gibi yapay zekâ kullanan yüz efekti uygulamaları), psikoloji ve rehabilitasyon alanında sağaltıcı şekilde kullanılma projelerinin bulunması gibi yararlı ya da masum amaçlarının olduğuna da yer vererek kullanım amaçlarının önemini vurgulamaktadır. AP "Avrupa Politikasında Derin Sahtecilik Mücadelesi" *(Tackling Deepfakes in European Policy)* başlıklı belgede, derin sahtecilik uygulamalarının, yaratıcılığı geliştiren yanlarının ötesinde ve dışında, Avrupa Birliği (AB) değerlerine aykırı olarak yaratacağı sonuçlar bakımından değerlendirilmesine dikkati çekmekte; söz konusu uygulamaların hedefi olan kişilerin haklarını koruyan düzenlemelerin ve politikaların geliştirilmesi gerektiğini ifade etmektedir.

Yukarıda ele aldığımız tehlikelerin, özellikle çocuklar açısından değerlendirilmesi çok önemlidir. Ebeveynler, kendi sosyal medya hesaplarından hem de çocukları adına açtıkları hesaplardan, çocuklarının fotoğraf veya video gibi kişisel verilerini paylaşmaktadır. Mott Çocuk Hastanesinin yaptığı bir araştırmaya göre, araştırmaya katılan ebeveynlerin %74'ü, bir çocuk hakkında sosyal medyada çok fazla bilgi

paylaştığını düşündüğü başka bir ebeveyn tanımaktadır. Bu paylaşımların %27'si çocuğun uygunsuz fotoğrafları, %51'i çocuğun konumu ve % 56'sı çocuk hakkında utanç verici bilgilerdir.[56] Çocukların kendilerine ait bilgilerin ebeveynlerince paylaşılmasına yönelik bir denetimleri yoktur. Çocukların bu durumu denetleme olanakları olsa bile en azından belli bir yaşa kadar bunların sonuçları hakkında tam olarak bilgi sahibi olamayacakları için rıza göstermeleri de sorunu çözemeyecektir (Erdoğan, 2019). "Unutulma hakkı" denilen hakkın son yıllarda daha etkin bir şekilde insan hakları gündeminde yer almasına neden olan, dijital dünyada hiçbir şeyin tam olarak silinememesi ve bir yerlerde kaydının bulunabilmesi durumu, ailelerin ya da çocukların yaptığı paylaşımların yaşam boyu karşılarına çıkabilmesi sorununu doğurmaktadır. Çocukların kişisel verilerinin korunması, daha sonraki bölümlerde yeniden ele alacağımız gibi, hukukta özel düzenleme gerektiren ve yüksek duyarlılığa dayalı önlemlerin alınması gereken bir konudur. Çocukların erken yaşta sosyal medya kullanması da, duyusal motor gelişim, bilişsel gelişim ve psikososyal gelişim sürecinde pek çok olumsuzluk yaratabilmesi bakımından ayrıca incelenmesi ve önlemler alınması gereken bir husustur (Yılmaz ve Güney, 2021).

Tezimizde daha önce ele aldığımız gözetim kavramı üzerinden kişisel verilerin korunması için alınması gereken önlemler konusunu değerlendirdiğimizde "karşı gözetim" kavramına da değinmek yerinde olacaktır. Barış Çoban ve Bora Ataman Panoptikon *2.0: Alternatif Medya ve Karşı Gözetim* adındaki derleme kitaplarının giriş bölümünde mahremiyet anlayışımızın yavaş yavaş gelişmiş primatlarla benzer bir yaşam evrenine sahip insansı *(hominid)* atalarımıza benzediğini ifade etmektedir. Toplumsal sistemi ve iktidarın gücünü koruyup, her ikisinin de devam etmesini amaçlayan gözetimde özellikle sosyal medya oldukça önemli bir araç haline gelmiştir. Daha önce de değindiğimiz gibi sosyal medya kullanıcılarının gönüllü şekilde katıldığı bir gözetim gerçekleştirilerek toplum yönlendirilebilmekte ve denetlenebilmektedir. "Panoptikon sonrası" ya da "post panoptikon" çağı olarak ele aldığımız bu dönemde bu araçları toplumun da kullanabilmesiyle "karşı gözetim" kavramı ortaya çıkmıştır. Karşı gözetim, iktidarın karşısında denetimden bir ölçüde kaçmayı sağlayan veya gözetimi yapanları gözetleyerek bireyler tarafından denetimi ve sivil toplum baskısını sağlayan araçları geliştirmeyi ve

[56] Rapor detayı için http://mottnpch.org/reports-surveys/parents-social-media-likes-and-dislikes-sharenting bakınız.

kullanmayı imlemektedir. Teknolojik gelişmeler bir anlamda güçlünün silahı olabildiği gibi zayıfın da kullanabileceği bir silah olabilmektedir (Çoban ve Ataman, 2018, s. 7 – 15). Örneğin, Neil J. Waghorn, bir protestoda siviller tarafından polisler üzerinde gezdirilen ve görüntü alan bir drone'u karşı gözetim aracı ve bir çeşit protestocu panoptikonu olarak betimlemektedir (Waghorn, 2018, s. 230). Arap Baharı hareketinde sosyal medya kullanımı örneğini verdiğimizde hem protestocuların sosyal medyayı kullanarak siyasal değişim yaratmaya etkide bulunduklarından ve sosyal medya haberciliği aracılığıyla haber ve fikirlerin özgürce internet dolaşımına girmesini sağladıklarından hem de iktidarın sosyal medya izlerini takip ederek bazı protestocuları elebaşı olarak tespit ederek tutukladıklarından söz etmiştik. İşte bu gibi örnekler gözetim ve karşı gözetimin ikili şekilde karşılıklı işlediğini gösteren örneklerden biridir. Günümüzdeki dijitalleşmeyle olanakları olağanüstü düzeyde gelişen gözetimin, henüz Orwell'in *1984*'ü gibi distopyalara benzer bir durumu ortaya çıkarmamasının en önemli sebeplerinden birinin bu araçları toplumun da kullanabiliyor olması olarak değerlendirebiliriz. Günümüzde yazılımcıların yukarıda sözünü ettiğimiz kötü amaçlar karşısında insanları korumak için oluşturdukları dijital gizliliği arttıran araçları kullanıma sunmaları (örneğin kişisel verileri şifreleyen, IP adreslerini maskeleyen sanal özle ağ anlamındaki VPN araçları) da karşı gözetim olarak ifade edilebilir. Dolayısıyla teknolojik olanakların, iktidar karşısında da gizliliği ve güvenliği arttıracak şekilde kullanılmasının ve toplum için de denetim oluşturma olanağı yaratmasının korunması ve bunların talep edilmesi önemli görünmektedir.

Dikkati çektiğimiz tehlikeler karşısında sosyal medya araçlarını kullanmaktan vazgeçmek ya da teknolojiden uzaklaşmak, güç sahibi olmak ve güçlü kalmak isteyenler bunları kullanmaktan vazgeçmediklerinde, bireyleri zayıf durumda bırakacaktır. Bu durum, teknoloji şirketleri ve ülke politikaları açısından da ikilemlidir. Örneğin, son zamanlarda insan zekâsını taklit eden yapay zekâ sohbet uygulaması ChatGPT'nin becerilerinin kullanıcılarda yarattığı şaşkınlığın da etkisiyle yapay zekâların geliştirilmesindeki endişeler karşısında yapay zekâ uzmanı ve teknoloji endüstrisi yöneticisi yüzlerce kişi açık bir mektup yayımlayarak bütün yapay zekâ laboratuvarlarının GPT-4'ten daha güçlü bir sistem üzerinde yürüttükleri çalışmaları altı ay süreyle durdurması çağrısında bulunmuşlardır. Güçlü yapay zekâ sistemlerinin, yalnızca etkilerinin olumlu ve risklerinin yönetilebilir olacağından emin olunduğunda

geliştirilmesi ve bu duraklama döneminde hükümetlerin devreye girerek bu konuda hızlı yasal değerlendirmeler ve düzenlemeler yapması gerektiğini belirtmişlerdir.[57] Ancak, teknoloji dünyasındaki şirketler arasında çalışmaların hızla devam edilmesini gerektirecek bir rekabet söz konusudur (Gazetesi Oksijen, 2023). Ülkeler arasında da savunma amaçlı teknoloji projelerinde yapay zekâların, veri bilimi teknolojilerinin geliştirilmesi konusunda ve siber güvenliği sağlamada büyük bir rekabet yaşanmaktadır. Örneğin daha önce değindiğimiz istihbarat çalışmaları[58]çerçevesinde ülkelerin kendi sosyal medya uygulamalarını geliştirmesi ve uygulamaların yaygınlaşan karşı ülkelerde yasaklanmaya çalışılması konusunda Çin ve Batı dünyası arasındaki durumu göz önünde bulundurduğumuzda veya Soğuk Savaş döneminde Sovyetler Birliği ve ABD önderliğinde Batı ve Doğu Bloğu ülkeleri arasında yaşanan teknolojik gelişmeler bağlamındaki mücadeleleri düşündüğümüzde yapay zekâ ve büyük veri teknolojilerinde bir duraksamanın zayıflık yaratacağı ve rakipler karşısında geri bırakacağı düşüncesi ortaya çıkacaktır. NATO Daimi Temsilciliği görevinde bulunmuş olan Mehmet Fatih Ceylan, Çin'i en önemli sistemik rakibi ilan eden ABD'nin, Çin ile yarı iletkenler ve çip üretiminde giriştiği rekabeti derinleştirmesini, yapay zekâ dahil yeni ve çığır açan teknolojilerde üstünlüğü korumak amacıyla sürdürdüğü rekabeti "Çip Savaşı" olarak tanımlayanların sayısının gün geçtikçe arttığından söz etmektedir (Ceylan, 2023). Siber güvenlik konusu günümüzün en önemli milli güvenlik konularından biri haline gelmiştir ve siber güvenliğin sağlanmasında ulusal üretim çok önemli bir noktada olduğundan, ülkelerin bu alandaki çalışmalarını geliştirmeleri büyük bir gereklilik olarak görülmektedir (BTK, 2018). Bu durum, geçici durdurma kararları alınsa da ve kamuoyunun haberi olmasa da bu teknolojilerin gerekli değerlendirmeler yapılmadan şirketler ve ülkeler tarafından geliştirilmeye devam edileceği endişesini uyandırmaktadır.

Sosyal medyada kişisel gizliliğin korunmasında alınacak önlemlerin neler olması gerektiği konusunda "güvenlik-gizlilik ikilemi" olarak adlandırılabilecek duruma da

[57] İlgili mektup detayı için https://futureoflife.org/open-letter/pause-giant-ai-experiments/ bakınız.

[58] Son yıllarda insan hakları örgütleri tarafından önemle üzerinde durulan ve ciddi önlemlerin alınması gerektiği belirtilen Pegasus adındaki, İsrail merkezli teknoloji şirketi NSO Group tarafından geliştirilen casus yazılım, hedef alınan kişilerin telefonlarına gelen linklere tıklamaları sonucunda ve hatta herhangi bir şey yapmalarına gerek olmadan gizlice kurulabilmektedir. Bu yazılım aracılığıyla cihazdaki mesajlara, e-postalara, aramalara, galeriye, mikrofon, kamera ve rehberdeki kişilere erişebilmektedir. Uluslararası Af Örgütü, dünyada 50 milyondan fazla telefonu hedef aldığı düşünülen casus yazılıma karşı Mobile Verification Toolkit (MVT) adında bir araç geliştirmiştir. (https://docs.mvt.re/en/latest/, Erişim Tarihi: 03.08.2023)

değinmemiz önem taşımaktadır. Çünkü özellikle kurumlar ve yasalar yoluyla alınacak önlemlerde bu güvenlik ve gizlilik dengesini sağlamak son derece kritik bir noktadır. Konunun etik ve insan hakları açısından değerlendirilmesinde de bu dengenin doğru şekilde ele alınması büyük önem taşımaktadır. İnsanların diğer tüm hak ve özgürlüklerini kullanabilmeleri için başat rolde kabul edilen yaşam hakkını korumak güvenliği sağlamayı gerektirmektedir. Fakat güvenliği sağlamak için alınacak bazı önlemler özel hayatın ve kişisel verilerin gizliliğini tehlikeye atabilmektedir. Gizlilikle çatışan güvenlik önlemlerine birçok örnek verilebilir. Örneğin, çeşitli kamusal alanlara yerleştirilen kamera sistemleri gizliliğimizden bir ölçüde vazgeçmemiz anlamına gelmektedir. Bu kamera sistemlerinin sadece görüntü mü yoksa ses ve görüntü mü kaydedeceği, özel-kamusal mekân sınırlarının belirlenerek hangi mekânlara kurulup hangi mekânlara kurulmaması gerektiği, özel hayatın gizliliği ve korunması hakkındaki yasalara ve yargı içtihatlarına göre değerlendirilmektedir. Uluslararası ve ulusal hukuk düzenlemelerinde temel hak ve özgürlüklerin çekirdek haklar hariç tutularak, güvenlik-özgürlük ikilemi olarak daha kapsayıcı şekilde ifade edilen durum dolayısıyla belirli koşullarda ve belirli ölçülerde sınırlandırılabileceğine hükmedilmektedir.

Tezimizin hukuki düzenlemeleri ele alan başlığında hem Avrupa İnsan Hakları Sözleşmesinde hem de Türkiye Cumhuriyeti Anayasasında ilgili kısımlara yer verildiği üzere özel hayatın ve gizliliğin korunması hakkı, ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması gibi birtakım nedenlerle sadece zorunlu olan ölçüde ve yasalar yoluyla kısıtlanabilmektedir. Konumuz özelinde güvenlik karşısına özgürlük yerine gizlilik kavramını koysak da bu sorun temelde güvenlik-özgürlük ikilemi olarak adlandırılmaktadır. Hem bireyin hem toplumun güvenliğini korumak amacıyla örneğin, terör gibi suçlarla mücadele etmek veya siber suçları önlemek için güvenlik kameralarıyla izleme, kişisel veri paylaşımı yoluyla kimlik doğrulama gibi gizliliği ilgilendiren uygulamalar yapılmaktadır. Bu önlemler alınırken hukukun "ölçülülük ilkesi"ne göre hareket etmek gerekmektedir. Ölçülülük ilkesi, temel hak sınırlamalarının amacı gerçekleştirmeye uygun ve aynı zamanda gerekli olmasını ve yapılan sınırlandırmayla amaç arasında aşırı bir dengesizliğin bulunmamasını ifade etmektedir (Vatansever, 2012). Dolayısıyla tehlike ve tehditlerin büyüklüğü doğru değerlendirilmeli, sadece gerektirdiği kadar önlem alınmalı ve bu önlemler amaçları dışında başka amaçlar için kullanılmamalıdır. Diğer önemli nokta ise, eğer güvenlik

tehditleri bir izlemeyi gerekli kılıyorsa, bu izlemeyi yapan kurumların kamuoyuna karşı saydam olmasının ve bu şekilde bireyler tarafından da denetlenebilirliğinin sağlanmasıdır (Løkke, 2018, s. 89). Tezimizde daha önce de değindiğimiz ABD'de çıkarılan "Patriot" yasasını, hem sosyal medyadaki kişisel verilerin gizliliğiyle ilgisi hem de güvenlik ve özgürlük dengesinin yeterince sağlanamadığına hükmedilmiş bir hukuki düzenleme olması nedeniyle hatırlatmak yerinde olacaktır. Patriot Kanununda hak ve özgürlükleri en çok sınırlandıran düzenlemelerin başında elektronik gözetim önlemleri gelmektedir (Turhan ve Aksu, 2011). 2013 yılındaki NSA'in Google, Facebook, Apple gibi şirketlerin verilerine de erişim sağlayarak yaptığı gözetleme programını ifşa eden "Snowden Olayı"ndan sonra insan hakları örgütlerinin tepkisi ve kamuoyundaki eleştiriler nedeniyle 2015 yılında, "Patriot Act" (Vatanseverlik Yasası) olarak anılan eski yasanın yerine yeniden düzenlenen "Freedom Act" (Özgürlük Yasası) kabul edilmiştir. Yapılan değişiklikle güvenlik ve özgürlük/gizlilik dengeleri yeniden kurulmaya çalışılmıştır.

Yukarıda ele aldığımız Özgürlük Yasasının sadece ABD vatandaşları için geçerli olması konusu da dikkate değerdir. Sözü geçen teknoloji firmalarının hizmet ve ürünleri dünyanın yer yerinde insanlar tarafından kullanılmaktadır. Bu yasayla yeniden düzenlenen hükümler NSA'in sadece ABD vatandaşlarına yönelik kitlesel izlemelerini kısıtlamaktadır. Sosyal medyanın kullanıcılarına küresel hizmet vermesinden dolayı, bu şirketlerin gizlilik sözleşmelerinde kullanıcıların yaşadıkları ülkeye göre farklı hükümlere yer vermeleri de sorunludur. Örneğin, ABD'de ve AB ülkelerindeki kullanıcılar için farklı, diğer ülkelerdeki kullanıcılar için farklı hükümler uygulanabilmektedir. 2021'de Facebook'un bugünkü adıyla Meta'nın, sahibi olduğu WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurtdışındaki üçüncü taraflara aktarılmasına onay verilmesini içerecek şekilde kullanım koşullarının güncellemesi ve onay vermeyen kullanıcıların uygulamayı kullanamayacağına ve hesaplarının silineceğine dair bilgilendirme yapması Türkiye'de gündemi meşgul eden tartışmalar yaratmıştır. Bilişim Hukuku Uzmanı Yaman Akdeniz, şirketin, toplanan verileri Facebook bünyesindeki diğer şirketlerle paylaşıp eşleştirmesini de içeren güncellemesiyle ilgili olarak GDPR'nin ("Avrupa Birliği Genel Veri Koruma Tüzüğü") veri güvenliği konusunda, 6698 sayılı KVKK'dan ("Kişisel Verilerin Korunması Kanunu") daha kapsamlı şekilde ek güvenceler içerdiğini, bu şirketlerin AB ülkelerinde uygulayamadıkları veri politikalarını bir dayatma şeklinde Türkiye gibi bazı

ülkelerinde uygulamak istemesinin kabul edilemeyeceğini ve bu şirketlerin gizlilik politikalarının bütün kullanıcıları kapsayan şekilde daha koruyucu olarak tasarlanması gerektiğini belirtmiştir (Akdeniz, 2020). Kişisel veri gizliliği ve güvenliği konusunda ülkelerin farklı düzenlemelerinin bulunması ve bunlar arasındaki uyuşmazlıklar sorun yaratabilmektedir. Sosyal medya platformları farklı ülkelerde faaliyet gösterip birçok farklı ülkeden kullanıcıya sahip olduğu için kişisel verilerin korunması konusunda kapsamlı ve güncel uluslararası düzenlemelerle uyumlu, ulusal yasal düzenlemelerin yapılması önemli görünmektedir. Ülkemizdeki kişisel verilerin korunması hukukundaki temel düzenleme olan 6698 sayılı KVKK, 95/46 sayılı Direktif ile büyük ölçüde uyumlu olsa da bu Direktifteki eksiklikleri gidermek ve daha güncel hükümler ortaya koymak amacıyla AB Veri Koruma Reformu kapsamında, yürürlüğe giren GDPR kadar kapsamlı düzenlemeler içermemektedir. Bu konuda, bazı uyumlaştırmalar için yasal düzenlemelerin gerekli olduğu, bazıları içinse Kişisel Verileri Koruma Kurumunun yapacağı ikincil düzenlemeler ve uygulama pratikleri yoluyla uyum sağlanabileceği yapılan değerlendirmeler arasındadır (Akıncı, 2017).

Önemle ele aldığımız büyük veri teknolojileriyle ilişkili olarak kişisel verilerin işlenmesinde, hukukta "profilleme" olarak ifade edilen faaliyetlerle ilgili olarak ülkemizde yapılan yasal düzenlemeler GDPR ile karşılaştırıldığında eksiklikler olduğu görülmektedir. Profilleme, GDPR'deki tanımına göre, gerçek bir kişinin, kişisel verilerinin, belirli kişisel özelliklerinin değerlendirilmesi amacıyla kullanılması, kişisel özelliklerinin çözümlenmesi veya tahmin edilmesi süreçleri anlamına gelmektedir. GDPR'nin 22. maddesinde birtakım koşulları sağlayan profilleme ve otomatik karar verme[59] süreçlerine özgü düzenlemeler yer almaktadır. Bu düzenlemenin yapılmasının gereği, bir insanın geleceğine veya hakkında önemli bir konuya bir makina tarafından karar verilmesinin insan onurunun korunması bakımından barındırdığı sorunlardan dolayı ortaya çıkmaktadır. 6698 sayılı KVKK'nda ise kişisel veri sahiplerinin haklarını düzenleyen 11. maddede "İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz

[59] Herhangi bir insan katılımı olmadan otomatik yollarla karar verme süreçlerini ifade etmektedir. Bu süreçlerde farklı yapay zekâ metodları kullanılabilmektir. (https://www.istanbulbarosu.org.tr/files/docs/AlgoritmikKararVermeveVeriKorumas%C4%B1022020.pdf, Erişim Tarihi: 27.07.2023)

etme" hakkı düzenlenmiş olsa da "profilleme" konusunda bir düzenleme yapılmamıştır. Kanunda ilgili kişilere tanınan haklar arasında, kişisel verilerinin otomatik sistemler aracılığıyla çözümlenmesi yoluyla kendisi için olumsuz bir sonucun ortaya çıkmasına itiraz etme hakkı tanınmıştır. Bu anlamda, otomatik veri işleme süreçlerine dayalı kararlar veya profilleme faaliyetleri bakımından veri sorumlularına bir yasak getirildiği söylenememektedir. Kişiler bu haklarını ortaya çıkan sonuç dolayısıyla veri sahibine doğrudan başvuruda bulunarak kullanabilmektedirler (Kavak Güven, 2022). Dolayısıyla kişisel verilerin gizliliğinin korunmasındaki güncel tehlikeler göz önünde bulundurulduğunda, KVKK'nda profilleme tanımı eşliğinde profillemeyle ilgili özel bir düzenleme yapılması gerekli görünmektedir.

Kişisel verilerin gizliliğinin korunması konusunda önemli bir diğer eksiklik bu konuda ülkemizde çocuklara yönelik özel bir düzenlemenin bulunmamasıdır. GDPR'nin 8. Maddesinde çocukların kişisel verileri işlenirken bilgi toplumu hizmetleriyle sınırlı olmak üzere rızanın ne şekilde alınacağına ilişkin özel bir hüküm vardır. GDPR'nin 6. Maddesinde belirtilen hukuka aykırılığı ortadan kaldıran nedenlerden rızanın arandığı hallerde, 16 yaşından büyük olması koşuluyla çocukların rızasına geçerlilik tanınmaktadır. Bu yaştan küçük çocukların verilerinin işlenebilmesi için veli veya vasisinin rızasının alınması gerekmektedir. Aksi halde işleme faaliyeti hukuka aykırı olmaktadır. Türkiye'de ise çocuklarla ilgili özel bir düzenleme olmamakla birlikte çocukların kişisel verilerinin işlenmesinde hukuka uygunluk nedenlerinden olan açık rızanın gerektiği hallerde, işlemeye ilişkin rızayı kimin vereceği hususunda bir açıklık bulunmamaktadır (Uçak, 2021). Daha önce de değindiğimiz gibi, ele aldığımız sorunlar çocuklar açısından özellikle üzerinde durulması gereken ciddi tehlikeler yaratmaktadır; bu nedenle özel bir düzenlemeyi gerektirmektedir.

Bilişim Hukuku Uzmanı Murat Volkan Dülger de ülkemizdeki 6698 sayılı KVKK'nun yürürlüğe girmiş olmasını ilke olarak olumlu bulmakla beraber bazı eksik ve hatalı düzenlemelerin olduğunu belirtmektedir. Yasanın uygulama kapsamı açısından, alan gereği istisnaların çok olmasının, özellikle kolluk güçlerinin ve istihbarat faaliyetlerinin tamamen yasa kapsamı dışına çıkarılmış olmasının, kişisel verileri koruma hukukunun ruhuna aykırı düzenlemeler olduğunu belirtmektedir. Türk Ceza Kanununda yer verilen kişisel verilerle ilgili suç tiplerinin düzenlenmesinde yalnızca kişisel verilerin hukuka

aykırı yollardan ele geçirilmesi, yayılması ya da kayıtlı kişisel verilerin yok edilmemesinin ceza hukukunun koruması altına alınmasını, yalnızca kişisel verilerin işlenmesinin bu koruma altına alınmamasını bir sorun olarak değerlendirmektedir. Oysa *hukuka uygun olarak elde edilen* ya da dağıtılan ve henüz yok edilmemesi gerekmeyen kişisel verilerin *hukuka aykırı işlenmek* suretiyle kötüye kullanılması da mümkündür. Bu durum düşünülmeyerek TCK'nda gerekli suç tipine yer verilmemesi önemli bir eksikliktir. Dülger'e göre diğer bir önemli nokta, Kişisel Verileri Koruma Kurulunun çoğunluk üyelerinin siyasi iktidar ve çoğunluğu temsil eden parlamento grubu tarafından atanmasıdır. Bu nedenle Kişisel Verileri Koruma Kurumu özerk bir kurum olarak yapılandırılamayarak tarafsızlığına gölge düşmektedir.[60] Hem mevzuatın, hem yapı hem de uygulama açısından Kişisel Verileri Koruma Kurumu ve Kurulunun tamamen bağımsız olması büyük önem taşımaktadır (Dülger, 2016).

Dülger'e göre kişisel verilerin korunması konusunda yapılan yasal düzenlemeler, oluşturulacak kurum ve kurullar, idari para cezaları ve hapis cezaları hiçbir zaman tam bir çözüm olamayacak ve ihlalleri tamamen önleyemeyecektir. Öncelikle kişilerin ve hizmet verenlerin kullandıkları bilişim sistemlerinin güvenliğini sağlamaları gerekmektedir. Bunun için kurumların kişisel verileri koruma politikaları oluşturularak bu politikaların kanunlarla uyumlu hale getirilmeleri ve denetlenmeleri gerekmektedir. Bütün bilişim sistemlerinin güvenlikle ilgili açığı bulunmaktadır ve bu yolla bilgisayar korsanları bu sistemlere girebilmektedirler. Bu nedenle bilişim alanında mutlak güvenlik sağlamak olanaklı değildir. Kullanıcıların, güçlü güvenlik önemleri almaları konusunda bilgilendirilmeleri gerekmektedir. Böylece bilişim alanındaki hukuka aykırı eylemlerin sayısı azalabilecektir. Kullanılacak bu güvenlik önlemleri hukuka aykırı eylemleri de ortaya çıkaracağından daha etkili güvenlik önlemlerinin geliştirilmesinde etkili olacaktır (Dülger, 2016). Ancak, günümüzdeki kişisel verilerimizi elde edebilen web sitelerinin ve sosyal ağların çokluğuyla bunların kendileri arasındaki veri paylaşımları ve hemen her gün yeni bir web sitesinin ortaya çıkması hesaba katıldığında bunların her birinin düzenli olarak denetimden geçirilmesi neredeyse olanaksız görünmektedir. Bu noktada bireylerin kendi gizlilik önlemlerini almaları, kişisel verilerini paylaştıkları şirketler tarafından

[60] Kişisel Verileri Koruma Kurulu dokuz üyeden oluşmaktadır. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu tarafından seçilmektedir (https://kvkk.gov.tr/yayinlar)

korunup korunmadığının takipçisi olabilmeleri, artık hizmet almadıkları hizmet sağlayıcılardan kişisel verilerinin silinmesini ya da anonimleştirilmesini istemek gibi kendilerine tanınan hukuki hakları kullanmak konusunda bilgilenmeleri çok önemlidir. Kişisel Verileri Koruma Kurumunun en önemli görevlerinden biri, belki de en önemlisi bu nedenle kişisel verilerin gizliliğinin önemi, alınabilecek önlemler ve yasal haklar konusunda toplumun bilinçlendirilmesini sağlamaktır çünkü kişiler veya kurumlar tarafından alınan önlemlere rağmen bilişim alanında tam güvenlik sağlanamamaktadır.

Ülkemizde sosyal medya kullanımını ilgilendiren bir yasa olan 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" da bazı hukukçular tarafından, kişisel verilerin gizliliğini ilgilendiren şekilde ifade özgürlüğü bağlamında yaratacağı sorunlar nedeniyle eleştirilmektedir. Kanunda, Türkiye'de günlük erişimi bir milyondan fazla olan yurtiçi veya yurtdışı kaynaklı sosyal ağ sağlayıcılarının, kendilerine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve üçüncü fıkra kapsamındaki başvurulara ilişkin istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları altı aylık dönemlerle Bilgi Teknolojileri ve İletişim Kurumu (BTK) bildirmekle yükümlü kılınmıştır. Temsilci atama yükümlülüğü sosyal ağ platformlarını hukuki bir statü kazandırması açısından olumlu olsa da kişilik ihlali yaratabilecek bir problemi de beraberinde getirmektedir. Sosyal medyadan kullanıcıların yaş, cinsiyet, etnik köken, eğitim, cinsel yönelim, siyasi düşünce, inanç, sağlık durumu gibi birçok verisi elde edilebilmektedir. Bu veriler daha önce bizim de ele aldığımız gibi ekonomi alanında satın alma ve siyasi iktidarlar tarafından oy verme davranışları üzerinde etki yaratmak için kullanılabilme olanağı yaratmaktadır. Bu durum verilerin amacı aşan şekilde çeşitli yönlendirilmeler için kullanılması sorununu yaratabilmektedir. Kullanıcı verilerinin saklanması ve istendiğinde yetkililere verilmesi yükümlülüğü ise kişilik haklarının ihlalini beraberinde getirebilme tehlikesini yaratacaktır. Bu durumun sosyal medya kullanıcıları arasında şu sırada yaygın olan otosansürü daha da arttırabileceği öne sürülmektedir (Şahin, 2022). Kanunda yapılan düzenlemenin içinde Türkiye'de temsilci bulundurmayan sosyal ağ sağlayıcılarının bant genişliğinin daraltılması ve ağ sağlayıcılarının, mahkeme kararıyla içeriklerin kaldırılmasına ilişkin olarak yapılan başvurulara 48 saat içinde cevap vermekle yükümlü olması, aksi halde platformlara 5 milyon ile 50 milyon TL arasında değişen para cezaları

uygulanması gibi maddeler de yer almaktadır. Yaman Akdeniz, Türkiye'nin şu sırada internet ve sosyal medya ağlarının en fazla kısıtlandığı ülkeler arasında yer aldığına işaret ederek bu kanunun daha fazla sansüre neden olacağı ve ifade özgürlüğü hakkına zarar vereceği yönünde eleştirilerde bulunmuştur (Gazete Duvar, 2022). Yanlış bilgilendirmenin önlenmesi, sosyal ağlarda işlenen suçlarla daha etkin mücadele edilmesi gerekçeleriyle yapılan düzenlemelerin temel hak ve özgürlükler açısından incelikle değerlendirilmesi, daha önce değindiğimiz iktidar-gözetim ilişkisi bağlamında önem taşımaktadır.

Bazı ülkelerde devletin elindeki kişisel verilerin işlenmesine yönelik belirli güvenceler bulunurken, ekonomik gerekçelerle özel girişimlerin benzer uygulamalarına büyük ölçüde ılımlı yaklaşılmakta ya da göz yumulmaktadır. Kişisel verilerin korunması konusunda gelişmiş düzenlemelere sahip olan Avrupa Birliğinde dahi konuya ilişkin pek çok sorun bulunmaktadır ve kişisel verilerin korunmasına ilişkin sistemlerin işlerliğiyle ilgili tartışmalar vardır. Kişisel verilerin korunmasının etkinliği, temel hak ve özgürlüklerle uygunluğu konuları, üzerinde durulan önemli konulardır ancak bu verilerin toplanması ve işlenmesinin ticari faaliyetlerde, suç ve suçlunun tespit edilmesi gibi konularda gerekliliği tartışmalı durumlar yaratmaktadır (Dülger, 2016). Verilerin ticari faaliyetlerde kullanımı konusuyla ilgili olarak, örneğin, 2016 yılında Alman Rekabet Otoritesi tarafından, rekabet hukuku bağlamında çeşitli veri uygulamaları aracılığıyla kişisel verilerin kötüye kullanıldığı iddiasıyla bir Facebook soruşturması yapılmıştır. İncelemede Facebook'un 2018 yılı itibarıyla günlük 1.52 milyar aylık ise 2.32 milyar aktif kullanıcısının bulunduğu, şirketin Alman sosyal ağ uygulamaları pazarında hâkim durumda bulunduğu, alternatifinin olmaması nedeniyle Facebook'un şart koştuğu kişisel verilerin kullanılmasına ilişkin onay metnini kullanıcıların kabul etmek zorunda bırakıldığı ve bundan dolayı Facebook'un gelirinin %98'lik bir kısmına katkı sağlayan bir veri tabanına ulaştığı iddiası değerlendirilmiştir (Kurdoğlu ve Ata, 2021). Günümüzdeki veri ekonomisi, bu verilerin mal ve hizmet üretmedeki kullanımının bir gereksinim haline gelmesi, hak ve özgürlüklerin korunması konusundaki dengelerin sağlanmasında çok büyük güçlükler ortaya çıkarmaktadır.

Avrupa Dijital Haklar *(European Digital Rights, EDRi)* örgütü internetteki hareketlerimizle elde edilen kişisel verilerin toplanması ve işlenmesiyle ilgili hukuk

alanında rıza ilkesinin dışındaki en önemli ilkenin "amacın sınırlandırılması ilkesi" olduğunu belirtmektedir. Amacın sınırlandırılması ilkesine göre veri sorumluları, kişisel verileri sadece yasalarla belirlenen belli bir amaç için toplamalı ve kullanmalıdırlar. "Şeffaflık ilkesi" gereği veri işlemenin amacı açıkça belirtilmeli ve kullanıcılar kendilerine ait verilerden hangilerinin işleme alındığı konusunda aydınlatılmalıdırlar. Kullanıcılar ayrıca veri işlemenin sonuçlarını ve kendilerine ait verilerin işlenmesinin ileride ne gibi sonuçlar doğurabileceğini anlamalıdırlar. "Açık rıza ilkesi" gereği rızanın kullanıcının özgür iradesine dayanması, bilgilendirmeye dayalı olarak alınmış olması ve açık bir şekilde dile getirilmesi gerekmektedir.[61] Karmaşık ve açık bir dille hazırlanmayan ve bazı noktalarda belirsizlikler bulunan gizlilik sözleşmeleri, rızanın gerçek anlamda meşruiyetini ve şeffaflığını ya da saydamlığını tartışmalı hale getirmektedir. KVKK'nun genel ilkeler başlıklı 4. maddesinde, kişisel verilerin işlenmesinde uyulması zorunlu ilkeler olarak, hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine yer verilmektedir (Resmi Gazete, 2016). Kullanıcıların da gizlilik sözleşmelerini, içeriğin kişisel verilerin korunması ilkeleriyle tam olarak örtüşüp örtüşmediğini kavrayarak kabul etmeleri önemli görünmektedir.

Sosyal medya sitelerinde kullanıcıların gizlilik ve korumayla ilgili ön ayarlarla yetinmeyerek gerekli sınırlandırmaları yapmaları ve sosyal medya şirketine verilen erişim izinlerini kontrol etmeleri gerekmektedir. Bir sosyal paylaşım ağına katılırken öncelikle takma ad kullanmak (kimlikteki adla doğrudan bağlantılı olmayan bir ad) her ne kadar bazı sosyal paylaşım ağlarında yasaklansa da (örneğin, Facebook[62]) gizliliğin bir ölçüde korunabilmesi için uygulanabilecek yöntemlerden ilkidir. Ayrıca, kullanıcıların gizlilik ayarları üzerinde de denetim sahibi olması çok önemlidir. Çünkü kiminle bilgi paylaşımında bulunulduğu konusunda bilinçli olarak bir karar verilmesi gerekmektedir.[63] Herkese açık hesaplar yerine sınırlandırılmış hesaplar veri koruma konusunda kısmen bir gizlilik sağlamaktadır. Unutulmamalıdır ki sosyal medyada yapılan paylaşımlar üçüncü kişiler tarafından kaydedilebilmekte ve rıza dışı başkalarıyla paylaşılabilmektedir. Sosyal

[61] Detaylı bilgi için https://ekitap.alternatifbilisim.org/veri-korumaya-giris/ bakınız.
[62] Detaylı bilgi için https://tr-tr.facebook.com/help/229715077154790 bakınız.
[63] Detaylı bilgi için https://ekitap.alternatifbilisim.org/veri-korumaya-giris/ bakınız.

medya platformlarında karşılaşılan kişilik hakları ihlalleri önemli bir kısmı kullanıcıyla sosyal medya hizmet sağlayıcısı dışındaki üçüncü kişilerce yapılmaktadır (Arslan, 2017). Sınırlandırılmış bir hesap kullansak da paylaşılanlar, verilerimizi görme izni bulunan kişilerce kaydedilip, izinsiz şekilde paylaşılarak internet dolaşımına sokulabilmektedir. Sosyal medya hesaplarında paylaşımları görebilecek kişiler, kullanıcı tarafından tanınan ve güven duyulan kişiler olmalıdır ve/veya paylaşımlar yoluyla elde edilecek verilerin rıza dışında paylaşılabileceği olasılığı her zaman düşünülerek paylaşımlarda bulunulması gerekmektedir. Doğum tarihi, eğitim bilgileri, anne kızlık soyadı, nüfus cüzdanı bilgileri, aile üyelerinin kişisel bilgileri, kredi kartı bilgileri, kullanıcı adı ve şifre bilgileri, ehliyet bilgileri, iş yeri ve konut adres bilgileri, tatil yeri ve tarihi, e-posta adresi, kişisel fotoğraf ve videolar gibi kişisel verilerin sosyal medyada paylaşılmaması yaşanması muhtemel mağduriyetlerin önüne geçmek için oldukça önemlidir ("Sosyal Ağlarda Güvenlik" 2023). Sosyal medyada, bulunulan konumu belli edecek kişisel verilerin yer almaması güvenlik açısından çok önem taşımaktadır. Özellikle ebeveyn ve akrabaların çocuklarla ilgili olarak yaptıkları paylaşımlarda üçüncü kişilerden gelebilecek tehlikelere karşı bu konuya çok dikkat etmesi genel olarak çocuklarla ilgili olabildiğince kısıtlı bilgi içeren paylaşımların yapılması gerekmektedir. Sosyal medya uygulamalarının, telefon ve adres defterine, konuma, kamera ve mikrofona erişme izinlerinin de gereksinimlere göre ayarlanması veri gizliliği açısından önemlidir. Çünkü gizlilik sözleşmelerinde belirtildiği gibi şirketler bunlara erişim izni verildiğinde bu yolla elde edilen verileri, rıza verildiği için toplayabilme yetkisine sahip olmaktadır. Daha önce de dikkati çektiğimiz üzere IP adresi üzerinden genel konum bilgisine ulaşılabilmektedir fakat tam konumun belirlenmesini güçleştirmek açısından konum iznini kapatmak gizliliği bir ölçüde korumaktadır.

Sosyal medyada ve web sitelerindeki bağlantı linklerine tıklamadan önce bunlara karşı şüpheci yaklaşılması, bu bağlantıların ne olduğunun anlaşılması, güvenli olup olmadığının denetlenmesi, güvenli olmayan bağlantılar için uyarı yapan tarayıcı ayarlarının yapılması ve güvenilir antivirüs programlarının kullanılması gibi önlemler çok önemlidir. Bilişim suçlarının bir kısmı bu tür güvenli olmayan bağlantılar yoluyla işlenebilmektedir. Şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili olmayan ve kolay tahmin edilemeyecek rakam ya da harf dizileri kullanılmalıdır. Büyük küçük harf,

rakam ve simgelerden oluşacak kombinasyonların tercih edilmesi gerekmektedir.[64] Şifrelerin belirli aralıklarla değiştirilmesi de alınabilecek önlemlerden biridir. Güçlü şifre oluşturmaya ek olarak iki adımlı (faktörlü) kimlik doğrulama önlemini kullanmak siber saldırılara karşı etkili bir yöntemdir. Bu yolla hesaba girilmek istendiğinde hesap sahibi kişiye kısa mesajla veya kimlik onaylama uygulamasıyla benzersiz bir güvenlik kodu gönderilmekte ve bu kod girilerek hesaba erişilebilmektedir(Amazon İnternet Sitesi, 2023). Burada dikkat etmemiz gereken nokta güçlü bir güvenlik önlemi için hizmet sağlayıcılarla daha özel kişisel verilerimizi paylaşmak durumunda olmamızdır. Bu konu da güvenlik-gizlilik ikilemi bağlamında değerlendirilebilecek bir husustur.

Bilişim Teknolojileri ve İletişim Kurumu da, kişisel verilerin gizliliği konusunda bireysel güvenlik önlemleri olarak yukarıda değindiğimiz önlemlerin bir özeti niteliğinde şu noktalara dikkati çekmektedir: Güçlü parola kullanma, iki faktörlü kimlik doğrulama kullanma, güncel antivirüs ve güvenlik yazılımı kullanma, işletim sistemlerini ve uygulamaları güncel tutma, güvenilir ve güncel bir tarayıcı kullanma, güvenli bir wi-fi ağı kullanma, bilinmeyen e-posta eklerini açmama, sosyal mühendislik saldırılarına[65] karşı dikkatli olma sahte internet sitelerine dikkat etme, sosyal medya hesaplarını koruma (güçlü parola, iki adımlı kimlik doğrulama, gizlilik ayarları, şüpheli hareketleri rapor etme vb.), sosyal medya paylaşımlarını sınırlama, spam e-postalara dikkat etme, bilinmeyen bağlantılara tıklamama, şifreleme protokollerini kullanan güvenli sitelerden çevrimiçi alışveriş yapma (USOM, 2023). Günümüzde sosyal medya üzerinden birçok web bağlantısına (linke) ulaşma, alışveriş yapma, oyun ve başka uygulamalar indirme, tanımadığımız insanlarla tanışma, e-posta adresi paylaşma gibi pek çok şey yapılabildiği için tüm bu hususlara dikkat etmek ve genel olarak internette karşımıza çıkan şeylere karşı şüpheci bir yaklaşımda bulunmak sosyal medyada kişisel verilerimizi korumak açısından son derece önemlidir.

[64] Detaylı bilgi için https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf bakınız.

[65] Sosyal mühendislik saldırıları, kişileri manipüle etmek ve hassas bilgilere erişmek için psikolojik ve sosyal manipülasyon tekniklerini kullanan saldırı türleridir. Bu saldırılar, genellikle insanların güvenini kazanmaya çalışan sahte veya dolandırıcı kişiler tarafından yapılmaktadır. Saldırganlar, telefonda, e-postada veya sosyal medya üzerinde sahte kimlikler kullanarak kendilerini başka biri olarak tanıtabilmektedirler. Saldırıların hedefleri, kullanıcı adları, parolalar, banka bilgileri ve diğer kişisel veya mali bilgilerdir. Sosyal mühendislik saldırılarının birçok çeşidi vardır, örneğin "phishing" olarak bilinen saldırılar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini ele geçirme amacını taşımaktadır.(https://dsy.usom.gov.tr/usom)

Sosyal medya kullanımlarıyla ilgili kişisel verilerin gizliliğini etkileyen sorunların her birinin çözümünü bütünüyle sağlamak olanaklı olmasa da bunların yaratacağı olumsuz sonuçları en aza indirmek için birtakım hukuksal, kurumsal ve bireysel önlemler alınması gerekmektedir. Kişisel verilerin korunması alanındaki hukuksal çalışmaların güncel teknolojik gelişmeleri ve geliştirilen yeni teknolojik olanaklarla ortaya çıkan yeni riskleri takip etmesi bu konularla ilgili öngörülerde bulunarak geç kalınmadan önlemlerin alınmasını sağlaması hayati önemdedir. Bu konunun öyle uzantıları vardır ki sözünü ettiğimiz teknolojilerin kullanımının her alanda olduğu gibi hukuk alanının yapısal niteliklerinde de köklü değişimleri beraberinde getireceği öngörülmektedir. Bu öngörüyü destekleyen şekilde "hukuk teknolojisi" *(legal tech)* kavramı ortaya çıkmıştır (Buluz, 2019). Teknolojinin hukuksal bilgiyle birleştiği hukuk teknolojisi, hukuka erişimi, uygulamayı ve yönetmeyi otomatikleştirmek, yalınlaştırmak ve iyileştirmek için bilgisayar destekli dijital teknolojinin kullanımı şeklinde tanımlanmaktadır. Örneğin, ceza adalet sisteminde kullanılan, failin yaşı, cinsiyeti, eğitim düzeyi, ailesi, çevresi, geçmiş adli sicil kaydı gibi çeşitli ölçütleri dikkate alarak suç tekrarı olasılığını hesaplayan yapay zekâ destekli "Correctional Offender Management Profiling System" (COMPAS) adlı bir algoritma geliştirilmiştir. COMPAS, bir kişinin yeniden suç işleme olasılığını hesaplamaktadır. Algoritmanın verdiği puana göre kişinin yeniden suç işleme olasılığının ne kadar olduğu belirlenmektedir. ABD'de bazı eyaletlerde kullanılan COMPAS, siyah vatandaşlara karşı önyargı barındırabileceği tartışmalarını ortaya çıkarmıştır (Washington Post, 2016). Bu teknolojinin daha da geliştirilerek kişinin gelecekteki birtakım davranışlarını çeşitli algoritmalarla tahmin ederek hukuksal sürece yön vermeyi hedeflediği görünmektedir (Abanoz Öztürk, 2021). Daha önce de değindiğimiz gibi sosyal medya kullanımıyla elde edilen kişisel veriler özellikle bu tür çalışmalar için çok verimli bir kaynaktır ve yapay zekâların karar verme süreçlerinde kullanılması önemli endişeleri beraberinde getirmektedir. Günümüzde veri çözümlemesi temelli yapay zekâ teknolojilerinin gelişmesinin, avukatlık, hâkimlik gibi mesleklerin sonunun gelebileceğiyle ilgili tartışmalara dahi neden olduğunu düşünürsek, hukuk alanının bu konularla ilgili çok kapsamlı ve incelikli çalışmalar yürütmesi gerektiğini ileri sürebiliriz. Hukuk sisteminde verilerin korunması, yapay zekâ modellerinden doğan sorumluluk veya haklar gibi tartışma alanlarının ortaya çıkması hem hukuk alanında teknolojinin getirdiklerinin anlaşılmasını hem de teknolojiyi geliştiren araştırmacılarca

hukuksal sınırların ve yükümlülüklerin belirlenmesini ve bilinmesini gerekli hale getirmektedir (Kızrak, 2019). Bu noktada hukuk fakültelerinin teknolojik gelişmelere ayak uydurması, ders içeriklerinin de bilişim hukuku ve etiği konularıyla güncellenmesi çok önemlidir (Gürzumar, 2019).

Yukarıda ele aldığımız tüm hususlar değerlendirildiğinde alınması gereken en önemli önlemin eğitim yoluyla farkındalık kazandırma olduğu sonucuna varabiliriz. Çünkü yapılan hiçbir hukuksal düzenleme ve alınacak hiçbir teknik önlem bilişim teknolojilerinin olanakları düşünüldüğünde veri gizliliğinin korunmasını mutlak olarak sağlayamayacaktır. Dolayısıyla her birey, kişi, yurttaş ya da ağdaş sosyal medyayı, yaptığı paylaşımlar yoluyla sağladığı verilerinin hangi amaçlarla kullanılabileceğinin farkında olarak ve düşünerek kullanmalıdır. Daha önce de değindiğimiz gibi, sadece bireysel ve küçük ölçekte bir bakış açısıyla değil, toplumsal ve büyük ölçekte bakış açısıyla konunun değerlendirilmesi doğru bir yaklaşım olacaktır. Doğru değerlendirmelerin yapılabilmesi için bireylerin ve karar vericilerin bu konularla ilgili bilgi sahibi olması büyük öneme sahiptir. Elbette sadece bilgi sahibi olmak değil, aynı zamanda bilginin kazandırdığı farkındalıkla eylemleri de bu yönde gerçekleştirmek gerekmektedir. Sadece ülkemizde değil dünyanın tüm ülkelerinde kişisel verilerin gizliliği sorununun gündemde tutulması ve dijital etik ilkeler konusunda çalışmaların güçlendirilmesi, insanların diğer hak ve özgürlüklerinin korunması bakımından büyük önem taşımaktadır.

4.3 Sosyal Medyada Kişisel Veri Gizliliğini ve Güvenliğini Sağlamada İnsan Hakları ve Etik Bilginin Önemi

Bilişim sistemlerinin çok hızlı bir şekilde gelişmesi nedeniyle hukuki düzenlemelerin bu gelişmelere hızla uyum sağlaması hem önemlidir hem de güçtür. Gelişen veri biliminin eşliğinde yapay zekâyı kullanarak kişisel verilerimizi içeren dijital izlerimiz arasında örüntüler bulan ve yüksek olasılıklı tahminler oluşturacak çözümlemeler yapan büyük veri uygulamalarının, toplum için yararlarının yanı sıra pek çok olumsuzlukları da vardır. Sosyal medyanın, veri bilimcilerin geliştirdiği yöntemlerle artık birçok amaç için kullanabilecek bir büyük bir veri kaynağı olması nedeniyle kişisel veri gizliliği konusunda özel ve kamusal yararla güvenlik ve gizlilik dengelerini kurmak gittikçe

güçleşmektedir. Bilişim dünyasında genel bir kanı olarak veri güvenliği ve gizliliğinin alınan önlemlere rağmen hiçbir zaman mutlak bir şekilde sağlanamaması, sadece yasal düzenlemelerin ve siber güvenlik önlemlerinin çözüm olamayacağını göstermektedir. Kişisel verilerin korunmasındaki en önemli sorun, bireylerin hizmet almak için verdikleri veya gönüllü olarak sosyal medyada paylaştıkları kişisel verilerinin, hangi koşullarda korunduğu ve bunların hangi amaçlarla kullanıldığı konularında bilgi eksikliklerinin bulunması, kişisel veri gizliliğinin bir temel hak olduğunun yeterince fark edilememesidir.

Bu bağlamdaki tehlikelerden kurtulmak için sosyal medya araçlarını kullanmaktan vazgeçmek ya da çağın teknolojisinden tamamen uzak bir yaşam kurmak ise gerçekçi bir yaklaşım değildir. Dijital dünyadaki verilerin büyük bir ekonomik değerinin olması, birçok hizmetin alınabilmesinin kişisel verilerin paylaşılmasını ve dijital sistemlerde kaydedilmesini gerektirmesi ve en önemlisi sosyal medya kullanımının toplumsallığın bir biçimi olarak yaşamın bir parçası haline gelmesi, bunların hepsinden uzak durarak analog bir yaşam sürmeyi, neredeyse olanaksız hale getirmektedir. Løkke, 21. yüzyılda özellikle akıllı telefonlarımızla sürekli olarak dijital ortama kişisel veri saçtığımız bu sistemden çıkmanın artık şüphe uyandıran bir eylem olarak kabul edileceğine dikkat çekmektedir. Böyle bir tercihte bulunan insanlar saklayacak bir şeyleri olduğuna dair bir merak uyandıracaklar; hatta devletin veya kurumların şüpheci bir şekilde dikkatlerini çekeceklerdir (Løkke, 2018, s. 11-12). Günümüzde artık iş görüşmeleri yapanlar da dâhil olmak üzere gerçek dünyada tanışanların dahi izlenimlerini güçlendirmek için başvurdukları ilk şey, birbirlerinin sosyal medya hesaplarına bakmak haline gelmiştir. Sosyal medyada gün içinde özel yaşamımızla ilgili anları verilere dönüştürerek sanal dünyaya görsel ve işitsel olarak aktarmamızın olağanlaşması gibi, kişilerin hiç sosyal medya kullanmayıp teknolojiden kendini soyutlayarak yaşaması da olağandışı hale gelmiştir. Anonim kalmanın da giderek güçleştiği internet dünyasında varolmanın artık bir gereksinime dönüşmesiyle, kişisel verilerin gizliliği pek çok temel hak ve özgürlükle bağlantısı bulunan ve oldukça geniş ölçekte değerlendirilmesi gereken uzantıları olan bir konu haline gelmiştir. Dijitalleşmeyle birlikte gizliliğin giderek yok olması ve teknoloji-toplum etkileşimlerinin sonuçları nedeniyle kişisel verilerin korunması hakkının başlı başına bir insan hakkı olarak kabul edilmesi ve tüm uzantılarıyla çağın teknolojik

olanaklarının, insan hakları ve etik bilgi süzgecinden geçirilerek değerlendirilmesinin gerekliliği ortaya çıkmıştır.

İnsan haklarının ve hukukun temelinde yer alması gereken etik, insanın kendisiyle, insan-insan, insan-insan olmayan, daha ayrıntılı olarak da insan-dünya, insan-bilgi ilişkisinde ortaya çıkan bir düşünme, bilme ve anlama bağlamıdır. İnsan eylemleri ve insanlararası ilişkilerle ilgilenen etik, bu eylem ve ilişkilerin sadece görünürlüğüyle değil aynı zamanda görünürlüğün arkaplanında yer alan gereksinimlerin, çıkarların, arzuların, isteklerin, değerlerin, niyetlerin, amaçların ve erdemlerin, söz konusu görünürlükle ilişkisini inceleyen bir düşünme ve bilme bağlamıdır (Çotuksöken, 2021, s. 49-50). Bir insan hakları sorununu ele alırken öncelikle insan onuru (insanın değeri) kavramı başta olmak üzere birtakım kavramsal belirlemeler yapmak gerektiğine tezimizin önceki kısımlarında değinmiştik. Çünkü insan, dünyayı kavramlar aracılığıyla çevçevelendirip anlamaktadır ve insanın ana özelliklerinden biri kavram kurmaktır. İnsan, düşünsel varlıklar olan ve sözcükler/terimler aracılığıyla somutlaşan kavramlar kurarak, tekil olanları, olup bitenleri, varolanları anlamlandırmakta ve bilgi oluşturabilmektedir (Çotuksöken, 2012, s. 23-25). İnsan dünyasındaki eylemlere dil ve dilin bir özne tarafından kullanılıp gerçekleştirilmesi olan söylem eşlik etmektedir. İnsan, türsel, toplumsal ve bireysel olarak dil yetisi-dil-söz bağlamında kendisi olmakta, kendi türüne dil yetisi, başka insanlara dili ve kendisine de söylemiyle bağlanmaktadır. Dışdünya-düşünme-dil arasındaki ilişkilerle şekillenen insan dünyasını anlarken sözcükler ve terimler ile dilsel olarak ifade edilen düşünsel çerçeveler olan kavramları araştırmak, felsefenin temel işi olmalıdır. Bir felsefe alanı olan ve felsefi bilgiye dayanan etik de bu nedenle dil kullanımının, eylemle ve insanlar arasındaki ilişkilerle olan ilgisini mutlaka ele almalıdır (Çotuksöken, 2021, s.49-82).

Günümüzde dijitalleşmeyle birlikte yüz yüze iletişim azalırken özellikle sosyal medya aracılığıyla çoğu zaman öznesi de belli olmayan bir dil alanı olarak ortaya çıkan "sanal dil ortamı" her şeyi etkilemektedir (Çotuksöken, 2021, s. 43). Ortaya çıkan yeni durumları gösterebilmek, anlayabilmek ve anlatabilmek için önceki kavramlarımız da yeterli olmamaktadır. Bu yeni durumları ve yeni insan ilişkileri ağlarını belirginleştirmek için yeni kavramlar oluşturulması gerekmektedir. Yeni durumları anlamak ve çözümlemek yeni kavramları üretmek ve bunları belirginleştirmekle mümkündür. Değerler ve normlar

da sadece düşünmede ve dilde varolmakta ve dille görünür hale getirilmektedir (Çotuksöken, 2021, s. 133-134). Hukuk alanında da kavramların, bunların dilsel ifadelerinin doğru şekilde, bir bulanıklığa izin vermeyecek bir biçimde kullanılması gerekmektedir. Örneğin, yapay zekâlara hukuken kişilik tanınması konusu öncelikle iradenin varlığıyla ilgilidir. Bu noktada iradenin ne olduğunun, felsefi bir kavram araştırmasıyla çerçevesinin çizilmesi gerekmektedir. Yapay zekâların seçenekler arasında seçim yapabilme özelliğinin irade olarak kabul edilip edilmeyeceğini belirlemek, bu belirlemeyi yaparken bir insan biçimciliğe (antropomorfizm) düşülüp düşülmediğini ortaya koymak yapay zekâ-insan ilişkisinde insanın bu ilişkiyle ilgili anlamlandırmalarını şekillendirecektir. İnternet ortamında kişisel verilerin korunması konusunda da örneğin, özel-kamusal alan kavramlarının belirlemesini yapmak ve bunların bireysel ve kültürel olarak farklı şekillerde sınırlarının çizilmesinin yarattığı sorunları ortadan kaldırmak için bu kavramları, sözünü ettiğimiz insan türüne ait bilgi anlayışına dayanan felsefi duruşla belirginleştirmek gerekmektedir.

Özel hayatın gizliliği ve kişisel verilerin korunması sorunlarında olduğu gibi dijital dünyanın insan hakları bağlamındaki tüm tehlikelerini en aza indirmek için "dijital etik" *(digital ethics)* veya "siber etik" *(cyberethics)* olarak da ifade edilen kavramlar oluşturulmuştur. Dijital etik veya siber etik, dijital dünyada interneti ve bilgisayar teknolojilerini geliştiren ve kullanan insanların evrensel etik değerler doğrultusunda nasıl davranmaları gerektiğini belirleyen normlar bütünü ve dijital teknolojilerdeki gelişmelerin birey ve toplum üzerindeki etkilerini felsefi bilgiyle aydınlatmaya çalışan etik alanı olarak tanımlanabilir. Konumuzla ilişkisi nedeniyle üzerinde önemle durduğumuz büyük veri, arttırılmış gerçeklik, yapay zekâ gibi dijital teknolojilerin insan yaşamını dönüştürme ve insanın dünyayı algılayıp anlamlandırması üzerindeki etki gücü, felsefi-etik alanda önemli tartışmalar üretmektedir.

Günümüzde ortaya çıkan "nesnelerin interneti" (*internet of things,* kısaca IoT) ve "her şeyin interneti" (*internet of everything,* kısaca IoE) kavramları, ağ toplumunu günümüzde yeniden şekillendirecek devrimleri göstermek, belirgin kılmak üzere yaratılmışlardır. Nesnelerin interneti, tüm nesnelerin internete bağlanmaları şeklindeki bir Web 4.0 internet uygulama ve hizmeti olarak tanımlanmaktadır. Nesnelerin interneti kavramı nesne, cihaz ve makinaların birbiriyle iletişimini işaret ederken, her şeyin interneti

kavramı ise insana vurgu yaparak, insan-insan, makina-insan arasındaki ağ bağlantılarını da kapsamaktadır (Altınpulluk, 2018). Dijital dünyadaki hızlı gelişmelerle her şeyin internetine giden süreç, beyne yerleştirilen bir implantla, insan beynini internete bağlı bir cihaza dönüştürme projelerinin oluşturulmasına kadar varmıştır. Örneğin, Elon Musk'ın kurduğu Neuralink şirketi, insan beynini bilgisayar sistemlerine ve yapay zekâya bağlayacak olan dijital ara yüzler geliştirmektedir.[66] Nano-teknoloji, gen klonlama, yapay zekâ vb. ileri teknolojilerin insan üzerinde kullanılmasını destekleyen ve böylece insanın fiziksel ve bilişsel yeteneklerinin arttırılmasını ve istenmeyen yönlerinin ortadan kaldırılmasını amaçlayan "transümanizm" kavramı etrafında bu gelişmelerin insan yaşamını ve tür olarak insanı nasıl dönüştüreceği, günümüzün etik ve insan hakları bağlamında en çok tartışılan konulardandır (Demir, 2018). Teknolojik gelişmelerin ürünleri, sağladıkları olanaklarla teknolojik gelişme hızının katlanarak artmasına neden olmaktadır. Dolayısıyla bazılarının ancak uzak bir gelecekte gerçekleşebilir gördüğü teknolojik dünya tasarılarının beklenenden kısa bir sürede ortaya çıkması olanaklı görünmektedir. Bu değişikliklerin ortaya çıkaracağı en önemli sorunların etik ve insan hakları konusunda olacağı açıktır Dijitalleşme dünyamızı o kadar hızlı bir şekilde kuşatmaktadır ki dijitalleşmenin etiği bir yana, etiğin dijitalleşmesi[67] ve insan haklarının geliştirilmesi bir yana, insanın biyomekatronik-sibernetik varlıklara *(cyborg)* dönüşmesiyle bugünkü insan hakları normlarının dayandığı ilkelerin çözülmesi dahi mümkündür.

Sosyal medyanın mahremiyeti gittikçe yok eden bir gözetim aracına dönüşmesi hem devletlere, hem de dijital dünyanın veri hazinelerine sahip şirketlere büyük bir güç ve rekabet avantajı sağlamıştır. Yukarıda bahsettiğimiz dijital gelişmeler, sosyal medyanın da gelişip dönüşmesine neden olacak ve muhtemelen gerçekliğimizi giderek işgal eder şekilde yaşamımızda büyük yer kaplamaya devam edecektir. İnsanların artık dijital sinir ağlarıyla internete bağlanabileceği bir gelecekte sosyal medya da yalnızca düşünme yoluyla insanların ağlarda gerçeklik algısıyla hareket edebileceği "metaverse" evrenlerine

[66] Detaylı bilgi için https://neuralink.com/ bakınız.

[67] Yapay zekâlardan yararlanan büyük veri yöntemlerinin hukuk alanındaki karar verme süreçlerinde kullanılmasının düşünülmesi gibi etik kararlarda da bu teknolojilerin kullanılmasının düşünülmesi mümkündür. Çünkü dataist bakış açısına göre bu teknolojiler nesnellikleri ve insan bilişinin üstündeki işlem yapma becerileriyle çok fazla sayıda veriyi-enformasyonu işleyerek insanlardan daha doğru kararlar verebilmektedirler.

dönüşebilecektir. Bugünkü şekliyle sosyal medya kullanımında ortaya çıkan kişisel veri problemi belki de insanların gerçek yaşamı bir kenara bırakarak dijital dünyada sadece sayısal veriler üreterek sanal varlıklarını sürdürdüğü bir noktaya ulaşacaktır. Verinin en değerli şey olarak görüldüğü ve veri yığınlarının yapay zekâlarla geleceği öngörmeyi sağladığı bir dünyada insanın değeri, ürettiği verinin değeriyle belirlenecektir. İnsanların sosyal medyada gerçek olmayan profiller oluşturabilmesi ileride, derin sahte bir evrende avatarlar seçerek sanal bedenlenmelere sahip olmasına dönüşebilecektir. Gerçekmiş gibi gelen sanal bir evrende toplumsallaşan insanlar bir yandan bunun gerçek olmadıklarını bildikleri için yaşamlarında etik olarak doğru bulmadıkları eylemleri de yapmaya başlayacaklardır. Zamanla gerçek olan ve olmayan arasındaki ayrım silikleşecektir. Elbette bunlar sadece gerçekleşmesi olanaklı ve olasılıklı görünenlerdir. Ancak dünyayı hızla dönüştüren, büyük etki gücüne sahip bu teknolojiler uzgörücü yaklaşımlarla ele alınmalıdır.

İnsanın doğayı dönüştürmesi, onu kontrol edebilmesi ve bunlarla bağlantılı olarak, sanatı, tekniği ve teknolojiyi ortaya çıkarmasını sağlayan ve onun diğer canlılar arasındaki yerini ve dolayısıyla değerini belirleyen özelliklerini koruması, aynı zamanda binlerce yıllık bir insanlık emeğine de sahip çıkması anlamına gelmektedir. İnsanın kurduğu dünyayı yıkımdan koruması, insanın kendi değerinden doğan insanlığın evrensel değerlerini yaşatmasıyla mümkündür. İnsanın bu dünyada insan olmayanlarla kurduğu ilişki de etiğin ve insan haklarının konusudur. Hem doğayı hem de insanın kendisini, anlam dünyasını ve algılayışlarını değiştiren ve hatta insanlığı ve doğayı bir yıkıma götürebilecek etkiler yaratan teknolojiyi üretenlerin veya kullananların sözünü ettiğimiz felsefi duruşu temele alan bir etiğe ve insan hakları bilgisine dayanarak eylemde bulunmaları gerekmektedir.

İnsan bilgi üreten, durum çözümlemesi yapabilen ve sorumluluk alabilen tek varlıktır (Çotuksöken, 2021, s. 55). Sahip olduğu yapısal özelliklerle insan, anlamla doldurduğu kendi dünyasını kurarken, şekil verebildiği bu dünyanın canlılığını sürdürmesini tehlikeye atan ve doğal olmayan nedenleri de yaratmaktadır. Dolayısıyla insan bu sebeplerin ortadan kaldırılmasından sorumludur. İnsanlığın evi olarak kabul edebileceğimiz çevreyle bu çevrede yaşayan canlıların, insanın müdahalesine çok açık hale gelen ekolojik ilişkisindeki dengenin bozulmasını önlemek, insanın ve kurduğu dünyanın varlığını devam ettirebilmesi için en temel gereksinimdir.

Felsefi-etik görüngeden (perspektiften) bakıldığında, insanın değerinin, insanı insan yapan özelliklerle, türe ait olanakların şekillendirdiği bir dünyada ortaya çıktığı bir bakıma açıktır. Gerçekten de sözünü ettiğimiz gelişmeler, insanın anlam ve değer dünyasını da dönüştürmektedir. Örneğin, sosyal medya kullanımı artık insanları öyle etkisi altına almıştır ki, özel hayatımızın gizliliğine ilişkin algımız değişmiş, mahremiyete verdiğimiz önem gittikçe azalarak bunun neden önemli olması gerektiğiyle ilgili farkındalıklarımız neredeyse körleşmiştir. Bu nedenle, bugün "insan onuru" dediğimiz şeyi belirlememizi sağlayan değer anlayışımızı yitirmeden bu konular üzerine düşünmek ve değerlendirmeler yapmak, zorunlu hale gelmektedir. Aksi halde insanlar, kendilerini diğer canlılardan ya da makinalardan ayıran özelliklerini, bu özellikler nedeniyle sahip oldukları hak ve özgürlükleri ve dolayısıyla "insanın değeri"ni korumakta çok geç kalabilirler. İnsanın değerini korumak ise insan hakları, etik bilgi ve hukuk ilişkisini doğru şekilde kurmakla ancak olanaklıdır.

Yazı aracılığıyla insan, ulaşabildiği varolanlar alanını, üzerine konuşulabilir ve zamanın şimdiki boyutunu aşarak başkalarına iletebilir duruma gelmiştir. Düşünmesini ve sözünü başkalarının anlama edimlerine açık olabilen bir şekilde nesneleştirmenin yolunu bulmuştur. Yazılı kültür, ulusal ve uluslararası hukuk kurallarını örneğin insan hakları belgelerini üzerinde düşünülebilir ve tartışılabilir bir ortama taşıyarak kamusal olanın paylaşılabilirliğini sağlamıştır. Hukukun yazılı belgelerle nesneleştirilmesinin tarihiyle "insanın değerinin bilgisi"nin tarihi koşutluk ilişkisi içinde varolmuşlardır. "İnsan Hakları Evrensel Bildirgesi", yazılı kültürün felsefe denilen boyutuyla özellikle "Aydınlanmacı düşünme" biçimiyle ortaya çıkan insan hakları kavrayışına dayanarak oluşturulmuştur. İnsanı, aklını kamusal olarak kullanmaya çağıran Aydınlanmacı düşünme biçimi, insanın değerini koruyan barış içinde yaşanabilir bir dünyanın gerekli koşullarını içeren nesnel-yazılı kültürün oluşmasını sağlamıştır. Fakat dünya üzerinde herkes için barış, adalet ve eşitlik sağlanamamıştır. İnsanlar şimdi ve burada olana bağlanmaktan kendini kurtararak elde ettiği gücü bir şiddet kültürü yaratmak için kullanmaktadır. Aklını kamusal bir biçimde değil insanlığı yokediciliğe sürükleyen bir şekilde araçsal olarak kullanmaktadır (Çotuksöken, 2012 s. 100-102). Günümüzde doğanın ve insan yaşamının seyrinde gerçekleşenlerin birer veri olarak, geliştirilen teknolojiyle neredeyse sınırsız bir şekilde depolanabilmesi ve işlenebilmesi bunu kullanabilenler için büyük bir güç sağlamaktadır. Bilimin öngörme özelliğini olağanüstü

şekilde geliştirebilecek yapay zekâ destekli büyük veri teknolojileri de bu bağlamda aklın kamusal kullanımıyla yararlanıldığında insanlık için pek çok fayda sağlayabileceği gibi daha çok adaletsizlik, ayırımcılık, eşitsizlik ve şiddet de yaratabilir. "Bilgi güçtür" anlayışının "veri güçtür" anlayışına dönüştüğü dünyamızda veri üreten insan da araçsallaşmaktadır.

İnsan dünyayı değiştirebilme gücüne sahip bir varlık olarak, olanı değiştirmenin öznesidir. Tüm bunlar özne olan insanın, insan-dünya-bilgi ilişkisi içinde konumlandırılması gereken kavramsal çerçeveleriyle bir anlam kazanmaktadır. Onur, saygı, özgürlük, eşitlik, adalet gibi kavramları ve değerleri yaratan insan tarihsel yolculuğunda düşünsel olarak, insana, insan sorunlarına yöneldiğinde ve insan elinden çıkan dünyayı ön plana aldığında insan hakları kavramının da doğmasını sağlayan temelleri atmaya başlamıştır. O halde her türlü bilgi, bilgiyi kavramlar ve onları gösteren sözcükler ve terimler sayesinde üreten toplumsal-tarihsel-kültürel ve temelde dilsel bir varlık olan insanla ilişkisi içinde ele alınmalıdır. Çünkü bilgi insana aittir ve her bilgi insanın varlık yapısına ait bilgi olmak durumundadır. Bu nedenle insanın kurduğu dünyayı anlamak öncelikle insanın ne olduğunu, onun yapısal özelliklerini ve olanaklarını anlamayı gerekli kılmaktadır (Çotuksöken, 2012, s. 11-45).

Günümüzde ise bilgi, insan deneyiminden tür olarak insana ait bilişsel ve duyuşsal özelliklerden koparılarak makinaların çözümlediği temelde matematikten ibaret olan veri ve enformasyona indirgenmektedir. Oysa insanın kendisini ve kurduğu dünyayı anlaması kendisinden koparılan veriye dayalı sayısal çözümlemelerle mümkün olamayacaktır. İnsan dünyasını saran teknoloji, yapay zekâ teknolojilerinin geliştirilmesine varan noktada insanın denetiminden uzaklaşarak âdeta bir iradesi varmış gibi ona hükmedebilecek bir yapıya dönüşmektedir. Oluşan gereksinim ve alışkanlıklarla insan teknolojiye mahkûm olmakta ve algısal-kavramsal dünyası da ürettiği araçlarla şekillenmektedir. Teknolojik araçlar insanı yapısına özgü olanaklarından uzaklaştırarak, insanı mekanikleştirmektedir. Bu noktada makinanın insanlaşması, insanın ise makinalaşması tehlikesi ortaya çıkmaktadır. İnsan, kurduğu dünyayı, kendisini de değiştirebilme gücüyle, insanın değerini koruyan bir şekilde geliştirebileceği gibi sözünü ettiğimiz şekilde kendisini yarattığı dünyanın içinde giderek eriyip yok olacak bir duruma da getirebilir.

Yukarıda sözünü ettiğimiz nedenlerle teknoloji-insan etkileşimleri ve özellikle dijitalleşmenin insan yaşamındaki etkileri, çağımızın felsefi ve bilimsel çalışma alanlarındaki en önemli gündem maddelerinden biri olmalıdır. Bu tehlikelere karşı insanlığı korumanın en önemli güvencesini sağlayan hukuksal kurumların da disiplinlerarası bir anlayışla sürekli gelişmeye açık ve uygun bir şekilde yapılanması sağlanmalıdır. Hukukun, gereksinim ve değer dengeleriyle özel ve kamusal yarar dengelerini etik ilkeler toplamı olarak etiğin somutlaştığı insan hakları bilgisiyle kurması gerekmektedir (Çotuksöken, 2021, s. 155). O halde teknolojideki hızlı gelişmelerle birlikte çoğu sosyal medya üzerinden elde edilen kişisel verilerin işlenmesinin ve böylece mahremiyetin giderek yok olmasının, insanın değeri ve kişi olarak korunması konusunda doğurduğu tehlikeleri önleme, felsefi formasyonla şekillendirilmiş ve felsefenin eleştirel ruhunu taşıyan bir eğitimden geçmiş insanların bilinçlenmesiyle mümkündür. Kamusal alandaki düzenlemelerin yapılması için ise etik bilgiye dayanan hukuk normlarının oluşturulması gerekmektedir. Dolayısıyla, insanın, onu bugüne getiren tarihsellik içindeki tüm deneyimlerinin insanın varlık yapısına ait bilgi anlayışına dayanan felsefi bir duruşla ele alınması, her bir insanı korumayı sağlayacak, değer bilgisiyle evrenselleştirilmiş bir eğitim sistemi ve hukuk düzeninin oluşturulması sağlanmalıdır.

SONUÇ ve ÖNERİLER

Modern toplumsal yapının oluşmasıyla birlikte bir sorun alanı olarak görülmeye başlanan ve insani bir gereksinim olarak talep edilen özel hayat veya mahremiyet kavrayışı, teknolojik gelişmelerle birlikte insan dünyasındaki anlamı ve değeri bakımından dönüşmüştür ve bu dönüşüm devam etmektedir. Aydınlanma çağı ile öne çıkan birtakım felsefi bakış açılarının yanı sıra, modern bilimdeki ilerlemelerle kendini gösteren teknolojik gelişmenin yarattığı mahremiyet sorunu, hukuki düzenlemelerin oluşturulmasının ilk kıvılcımı olmuştur. Bugün de internet devrimiyle ortaya çıkan sosyal ağlar ve bu ağların kullanımının günlük yaşama çerçevesinin bir parçası haline gelmesi, mahremiyet sorununun daha çok bir "veri mahremiyeti" *(data privacy)* sorununa dönüşmesine neden olmuştur. Ayrıca kişisel verilerin bilişim sistemleri tarafından kaydedilmesi, saklanması, işlenmesi, çözümlenmesi ve aktarılması resmi ya da özel çeşitli işlerin görülebilmesinin vazgeçilmez unsurları haline gelmiştir.

Kişisel verilerin korunması hakkı günümüzde başlı başına bir insan hakkı olarak değerlendirilmesi gereken bir haktır. Bilişim teknolojilerindeki gelişmeler; verilerin dijital kayıt ve depolanma olanaklarının her geçen gün daha büyük oranda artması, yapay zekâ ve büyük veri uygulamaları, bu hakkın özel hayatın gizliliği kapsamında korunmasının ya da ekonomik veya fikri mülkiyet hakları benzeri yaklaşımlarla korunmasının yeterli olamamasının en önemli nedenidir. Kişisel veri gizliliğinin, hukuki perspektiften baktığımızda, kişiye sırf kişi olması bakımından tanınan ve kişiliği oluşturan değerlerin ayrılmaz unsuru olan kişilik hakları kapsamında değerlendirilebileceği ve kişilik haklarının da günümüzde insan haklarından ayrı düşünülemeyeceği açıktır.

Bir hakkın insan hakkı olup olmadığı konusunda değerlendirme yapabilmek için ise öncelikle insan haklarının ne olduğunun ortaya konulması gerekmektedir. İnsan haklarının ne olduğunu anlamak; bir hakkın insan hakkı olup olmadığına karar verebileceğimiz ölçütü ya da ölçütleri özenle belirlemek bu bağlamda son derece önemlidir. Günümüzde insan haklarına birçok yeni hak eklenmektedir ve bu hakların birer insan hakkı olarak ortaya konulması felsefi bir temellendirmeyi gerekli kılmaktadır.

İnsanın, türe ait olanaklarıyla ortaya çıkardığı teknoloji ve bilim gibi insan başarıları temelde insanın bilme edimine dayanmaktadır. Düşünen, bilgi üreten, anlam yaratan insan hem kendini hem de kurduğu dünyayı değiştirebilmektedir. İnsanın kurduğu dünyayı anlamak ve değişen dünyadaki sorunları fark etmek, çözümlemek, çözüme ulaştırmak, insan varoluşunu temele koyan bir felsefi yaklaşımla mümkündür. "İnsan nedir?" sorusu, tarihsel ve kültürel bir varlık olarak insan, hem kendisini hem de dünyasını sürekli değiştirdiği için güncelliğini her zaman korur. Çağımızdaki bilimsel ve teknolojik ürünler geliştirilirken, bunların insanın değerine yönelik olarak oluşturduğu yeni tehditler sonucunda yeni haklar türetilmesi ihtiyacı bu bağlamda değerlendirilmelidir.

İnsan haklarının evrensel normlar olmaları, her insanın sahip olduğu türe özgü yapısal özelliklerden kaynaklanmaktadır. Bu yapısal özelliklerle olanakların her kişide bulunması nedeniyle her bir kişide korunması, insan haklarının evrenselliğini ifade eder. İnsan haklarının, değer yargılarının ve çok çeşitli insan gereksinimlerinin farklılığına rağmen her bir kişide evrensel olarak nasıl korunacağını anlayabilmemiz, Çotuksöken'in de üzerinde önemle durduğu gibi özel-toplumsal-kamusal alan kavramlarını da ele almayı ve anlamayı gerektirmektedir. Özel olanın sınırlarını kesin olarak belirlemek mümkün değildir. Bu nedenle dikkat edilmesi gereken asıl nokta, insan haklarının korunması ve geliştirilmesinde rastlantısallığı dışarıda bırakan, etik bilgiye dayalı hukuki düzenlemeler oluşturmak ve toplumsal düzende böyle bir yaklaşımı veya ölçütü temele almaktır. İnsan haklarının evrenselliği ve her toplumda her birey için korunması ve geliştirilmesi ancak böyle bir anlayışla anlamlı olabilecektir.

Kişisel verilerin korunması hakkı, başta özel hayatın gizliliği hakkı olmak üzere başka temel hak ve özgürlükle de ilişkili bir haktır. Mahremiyet; insanın olanaklarını gerçekleştirmesi ve geliştirmesi ayrıca diğer temel hak ve özgürlüklerinin de korunması bakımından koşul bir haktır. Mahremiyet veya özel hayatın gizliliği, kişilerin özel hayatına müdahale etmeme ve gözlerden uzak olma, bireylerin bazı eylemlerini başkalarının gereksinim ve değerleriyle çatışmadan gerçekleştirebilmesi olanağını yaratır. Böylelikle kişinin yaşadığı çatışmanın gücünün kişiyi o eylemden alıkoymasının önüne geçilir. İnsanın kendini tanımasıyla da mahremiyetin bir ilişkisi söz konusudur. İnsan, benliğini anlamaya çalışırken toplum içinde başkalarıyla bir arada olmaya ihtiyaç

duyduğu kadar sadece seçtiği insanlarla olmaya ya da yalnız başına kalmaya da ihtiyaç duyar. Mahremiyet, kişinin kendi yeteneklerini, yeterliliklerini denemesini ve geliştirmesini sağlar. Kişilerin kendilerini başkalarına karşı gizleme, savunma, koruma ihtiyacının yarattığı gerilimi de azaltır. Başkalarından, güven duymadıklarından veya yabancılardan gizlenmiş bir alanda eylemde bulunan kişi bazı olanaklarını daha rahat ve güvenli bir şekilde gerçekleştirecek ve gereksinimlerini karşılayabilecektir. İnsanların olanaklarını gerçekleştirirken onlara müdahale edilmemesi ve kendilerini güvende hissetmeleri bir gerekliliktir. Dolayısıyla bazı gereksinimlerin giderilmesi ve bazı olanakların ortaya çıkabilmesi için müdahale etmeme ve temelinde gizlilik ilkelerinin bulunduğu mahremiyet hakkı diğer bazı temel hakların korunması ve özgürlüklerin gerçekleşebilmesi için koşul niteliğindeki temel bir hak olarak kabul edilmelidir.

Günümüzde mahremiyetin korunması, dijitalleşmenin ve bunun yarattığı gözetim imkânının etkisiyle kişisel verilerin gizliliği çerçevesi olmaksızın mümkün olamayacaktır. Kişilerin başta özel hayatının ve diğer bazı temel hak ve özgürlüklerinin korunabilmesi için öncelikli olarak kişisel verilerinin gizliliğinin korunması gerekmektedir. Özellikle hassas kişisel veriler olarak tanımlanan veriler, özel hayatın gizliliği bağlamında büyük önem taşımaktadır. Bu verilerin gizliliği, kişinin yaşadığı toplumda ayırımcılığa uğramaması ve bu ayırımcılığın, insanın olanaklarının gerçekleşmesi için en temel koşul olan yaşam hakkının ihlaline varacak ölçüde sonuçlar yaratmaması bakımından ya da kişileri, kurdukları ilişkilerin sonucunda ilgili, ilişkili oldukları bir insandan ya da insanlardan korumak açısından gereklidir. Günümüzde kişilerin sosyal ağlarda bıraktığı izlerden, özel yaşamlarından kesitlerin, düşünce ve duygularının okunabilmesi ve konumlarının belirlenebilmesi mahremiyetle kişisel verilerin ilişkisi açısından en kritik noktayı oluşturmaktadır.

Kişisel verilerin korunması hakkıyla ilgili olarak değinmemiz gereken temel hak ve özgürlükten bir diğeri düşünce ve kanaat özgürlüğüdür. Özellikle bu hak ile kişisel verilerin korunması konusunda bazı çatışmalar olduğu için bu hakkın ele alınması önem taşımaktadır. Günümüzde kişiler X, Facebook, Youtube gibi sosyal ağlarda pek çok konuda düşünce ve kanaatlerini dile getirmektedirler. Düşüncelerini ifade ederken kullanıcıların bir kısmı anonim kimlikler kullanmaktadırlar. Kimi zaman kişiler bu gizlilik sayesinde düşüncelerini ve kanaatlerini kamuyla paylaşabilmektedirler. Hukuki

düzenlemelerde düşünce ve ifade özgürlüğü, millî güvenliği ve kamu düzenini sağlamak, kamu ahlakını korumak gibi amaçlarla kısıtlanabilmektedir ve yasalara göre suç teşkil eden ifadeleri nedeniyle kişiler cezalandırılabilmektedir. Kuçuradi'ye göre dokunulması ve korunması gerekenler ifade edilen bilgi ve fikirlerin kendileri değil, bu bilgileri dile getiren kişilerdir. Bazı fikirlerin öğretilmesi ve propagandası, eğer bu fikirler aynı konudaki açık bir bilgiyle veya insan hakları bilgisiyle ters düşüyorsa yasaklanabilir. Kişisel verilerin korunması konusunda düşünce ve ifade özgürlüğü açısından güvenlik-gizlilik dengesini sağlarken ve kamusal düzenlemeler yapılırken bu ölçüte göre değerlendirme yapılması gerekmektedir.

Kişisel verilerin, bu verilerin bir insana ait olması, o insanı belirlenebilir kılması ve belirlediği takdirde de o kişinin diğer hak ve özgürlükler bağlamında zarar görmesi ya da kişinin olanaklarını gerçekleştirememesi nedeniyle korunması gerekmektedir. O halde İnsanın değeriyle ilişkisinde sahip olunan diğer temel haklara da zarar vermeyecek şekilde korunması amaçlananlar, bu verilerin ait olduğu kişilerdir. Dolayısıyla hangi kişisel verinin hangi durumda istisna olacağı bu ölçütlere göre değerlendirilmelidir.

Dijitalleşme ve sosyal medya kullanımının yaygınlaşmasıyla birlikte insanlar kişisel verilerini milyonlarca insanın görebileceği şekilde gönüllü olarak paylaşırken, aynı zamanda bunlar, başkaları tarafından da internet dolaşımına sokulabilmektedir. Kişi, kişisel verilerini rızasıyla yayımlasa ya da yayımlanmasına izin verse bile, bu verilerin yer aldığı paylaşımların, haberlerin, eleştirilerin ve "sosyal medya linci" olarak ifade edilen tepkiler dolayısıyla internet ortamından silinmesini isteyebilmektedir. Ayrıca kişi, kamuya aktarılmak üzere haber değeri taşıyan bir duruma konu olmak nedeniyle hakkında yapılan bir haberin de unutulma hakkı kapsamında internetten silinmesini talep edebilmektedir. Kişinin şerefi ve haysiyeti aile ve iş yaşamındaki itibarı gibi konuların söz konusu olduğu durumlarda unutulma hakkı, kişinin kendi yaşamını ve kendisine ilişkin bilgiyi kontrol edebilmesi bağlamında ortaya çıkmaktadır. Ancak burada kişinin kendi rızasıyla yayımlanmasına izin verdiği bilgilerin silinmesi tartışmalı bir konudur. Çünkü kişinin böyle bir olanağa kolayca sahip olabilmesi, öngörerek eylemde bulunma bilincine zarar verebilir ve kişisel verilerini daha da sınırsız ve olumsuz bir şekilde internet ortamında yaymasına neden olabilir. Haber alma ve basın özgürlüğüyle kişisel

verilerin gizliliği ve unutulma hakkı ilişkisinde gözetilmesi gerekli olan dengenin yanı sıra, bu konuda da dengeyi sağlayacak değerlendirmeler yapılması gerekmektedir.

Dijitalleşmeyle birlikte kişisel veriler kullanılarak gerçekleştirilen hukuka aykırı eylemler artmakta, özel yaşamın gizliliği ilkeleri kişisel veriler üzerindeki hakların korunmasında yetersiz kalmakta; öte yandan teknolojideki hızlı gelişmelerle birlikte kişisel verilerin işlenmesi ve çözümlenip anlamlandırılması, insanın değeri ve özellikle kişi olarak korunması konusunda yeni tehditler doğurmaktadır.

Sosyal medya, büyük veri teknolojisinin uygulamalarından olan veri madenciliği için bir hazine gibidir. Sosyal medya ortamlarından elde edilen kişisel veriler sadece reklamcılık ve pazarlama alanlarında değil toplumsal-siyasi yönlendirme amaçlarıyla da kullanılmakta ve sosyal medya bir gözetim aracı haline gelmektedir. Bilmek, bildiğimiz şey üzerinde denetim sahibi olmamızı da sağlamaktadır. Egemenliği ve güvenliği sağlamak isteyen iktidarlar da bu nedenle bireyler hakkında bilgi sahibi olmak ve onları gözetlemek, denetim altında tutmak isterler. Gözetleme, tarih boyunca farklı şekillerde bireyler üzerinde varlığını hissettirmiştir. Bilişimdeki ve teknolojideki gelişmelerle gözetim ve kayıt altına alma olanakları artmış ve gelişmiştir. Kişisel verilerin bilişim sistemleri tarafından kaydedilmesi, saklanması, işlenmesi, aktarılması ve analiz edilmeleri ya da çözümlenmeleri, bu bağlamda kişilerin başta mahremiyet olmak üzere temel hakları ve bunlarla ilişkili haklarının korunması konusunda endişelere neden olmaktadır.

Verilerin yeniden kullanılması olanağı, kişilerin internette bıraktıkları dijital izlerin belirli amaçlar için kullanıldıktan sonra muhtemelen onay alınmaksızın başka amaçlar için de kullanılabileceği anlamına gelmektedir ve mahremiyet açısından bu durum potansiyel bir sorun olarak karşımıza çıkmaktadır. Hemen her kişinin hayatında yeri olan, toplumsallığın bir biçimi olarak toplumla etkileşen ve onu birçok yönden etkileme ve değiştirme gücüne sahip dijital sosyal ağların insanlık üzerindeki yıkıcı etkilerini göstermeye çalışan kişiler bile geniş kitlelere ulaşarak fikirlerini daha özgür bir biçimde ifade etmekte ve bu görüşlerini aktarmanın yolu olarak sosyal medya platformlarını kullanmaktadırlar. Artık ağın dışında kalmak gittikçe zorlaşmaktadır ve sosyal medya,

insanlar için vazgeçilmesi neredeyse mümkün olamayacak bir gereksinim olmuştur veya olma yolundadır.

Araştırmamızda örneklerini verdiğimiz gibi dünyada milyonlarca sosyal medya kullanıcısını etkileyen pek çok veri ihlali olayları gerçekleşmektedir. Dijital dünyada hiçbir sistemin ele geçirilemez olmadığı ve veri güvenliğini mutlak şekilde sağlamanın mümkün olmadığı ortaya çıkmaktadır. Olağanüstü büyüklükte verileri saklayan bulut bilişimle ilgili süreçlerin açıklanmaya muhtaç bir karmaşıklığa sahip olduğu görülmektedir. Sosyal medya bağlamında hizmet sağlayıcılarının verilerimizi ne şekilde sakladıkları ve bunların tamamen yok edilmesinin nasıl olduğu konularının bulanık olduğu anlaşılmaktadır.

Büyük veri teknolojilerinin gelişmesiyle ortaya çıkan önemli bir sorun da kişisel veri gizliliğini korumada çok önemli olan "anonimleştirme" yönteminde yaşanabilen sorunlardır. Kişilere ilişkin verilerin tam anlamıyla ve geri döndürülemeyecek şekilde anonimleştirilebilmesi neredeyse olanaksızdır. Veri madenciliği gibi büyük veri yöntemlerinden yararlanarak farklı kaynaklardan gelen birçok veri kümesini birleştirip bir kişinin kimliğini belirlenebilir hale getirmek mümkündür. Dolayısıyla anonimleştirilmiş veriler başka veri kümeleriyle çeşitli tekniklerle eşleştirildiklerinde geri döndürülebilmektedirler. Dolayısıyla büyük veri süreçlerinin anonimleştirmeyi olanaksızlaştıran tahminler oluşturabilmesi ve profilleme yöntemleri nedeniyle, doğrudan kişiyi belirlenebilir hale getirmeyen ama dolaylı olarak belirleyebilecek ve bu nedenle de kişisel veri kapsamında kabul edilecek verilerin hangileri olabileceği konusu, her somut olaya göre veri biliminin olanakları göz önünde tutularak değerlendirilmelidir. Kişinin, herhangi bir nedenle kendisiyle ilgili bir sonuç yaratmak için hedef haline getirilmesi durumunda hakkında doğrudan veya dolaylı belirlemeler yapılabilecek dolayısıyla ayırımcılık ve eşitsizliğe uğramasına neden olabilecek dijital verilerinin, veri işleme koşullarının ortadan kalması durumunda anonimleştirmesi yerine yok edilmesi yolunun tercih edilebileceği konusunu dikkatle değerlendirmek gerekmektedir.

Sosyal medyada, kişinin, ilgilerinin, eğilimlerinin, dünya görüşünün, inancının, dijital verileri yoluyla belirlenebilmesini olanaklı hale getiren kişiselleştirme algoritmaları, sosyal medyanın kamusal alan işlevi konusunda da dikkatle değerlendirilmesi gereken bir

konu haline gelmiştir. X ve Facebook gibi gündemdeki toplumsal olaylarla ilgili haberlerin, görüşlerin takip edildiği ve bu konuların tartışıldığı sosyal medya ortamlarının kişiselleştirme algoritmalarıyla belli özellikteki kişilere, belli içerikleri sıklıkla göstermesi, bu kişilerin sosyal medyada toplumun da sadece belirli özelliklere sahip kişileriyle karşılaşmalarına neden olmaktadır. Bu da toplumu ilgilendiren bir durumla bağlantılı farklı görüşlerle sosyal medyada karşılaşmayı zorlaştırmakta ve toplumu ilgilendiren önemli bir konunun kişinin ilgi alanının dışında kalmasından dolayı görülmesi olasılığını azaltmaktadır. Kişilerin kamuyu ilgilendiren bir konu üzerine kendi düşünce ve kanaatlerini oluşturmalarında ve konuyla ilgili sorunları fark edebilmesinde, farklı düşüncelerle ve farklı haber kaynaklarından gelen haberlerle karşılaşabilmeleri oldukça önemlidir. Kişinin sosyal medya ve genel olarak internet üzerindeki hareketlerinin kişiselleştirme algoritmaları yoluyla bu kişilere reklam gösterme veya ekranda daha uzun süre tutmayı sağlayacak özellikleri belirlemek üzere kullanılması olanağı, aynı zamanda kasıtlı olarak farklı amaçlar için de kişilere amaca uygun içeriklerin gösterilmesi için kullanılabilmektedir. Örneğin, kişilere, çıkarsanan kimliklerine göre etkilenecekleri siyasi ve sosyal içerikler gösterilebilmektedir. Kişilerin toplumsal durumların belli bir yönünü, toplumun belli bir kısmını veya belli haber içeriklerini görebildiği, kişilerin propaganda yoluyla yönlendirilebildikleri bir ortamda bu kişilerin serbestçe bilgiye ve düşünceye ulaşabilmesi mümkün olamayacağı için düşünce ve kanaat özgürlüğü sağlanamayacaktır.

Sosyal medya, dünyayı algılama ve anlamlandırma üzerindeki etkisiyle insanlığın oluşturduğu değerler dünyasını da dönüştürebilme gücüne sahiptir. Kişilerin mahremiyete veya kişisel veriler olarak tanımladığımız bilgilerinin gizliliğine ilişkin bakışları ve verdikleri önem de sosyal medya nedeniyle dönüşmektedir. İnsanların düşünce ve değer dünyalarında meydana gelen değişimler insan haklarının geleceği için çok kritik bir öneme sahiptir. Kazanılmış hak ve özgürlüklerin vazgeçilmezliği konusunda bir duyarsızlaşmanın, bunların önemine ve niçin önemli olduğuna ilişkin bir körleşmenin, gelecekte gerçekleşebilecek küresel ölçekte bir savaş, büyük bir küresel salgın veya iklim kaynaklı ya da çevre kaynaklı tehlikelerle afet durumlarının etkileşimi, elde edilen hakların doğru değerlendirilmeden ölçüsüz şekilde kısıtlanmasına veya yitirilmesine yol açabilir. İnsanlar zaman içinde alışarak sonunda gereksinim haline getirdikleri ve olağanlaştırdıkları uygulamalar nedeniyle gerektiği gibi sorgulamadan

ölçüsüz gözetim ve denetimi fark edemeyebilir veya fark etseler de yaratacağı sonuçların etkisiyle önemini kavrayamayabilir ve dolayısıyla bir süre sonra tepki vermekten vazgeçebilirler, hatta duyarsızlaşabilirler. Baskıcı yönetimler, güçlerine güç katmak ve iktidarlarını sürdürmek amacıyla toplumun gizliliğe ve izlenmeye ilişkin anlayışlarında oluşan esnekliği, güvenliği veya yanlış bilgilendirmeyi gerekçe göstererek bireyleri gözetlemek, kısıtlamak üzere ve algı yönetimi amacıyla kullanabilirler. Bu nedenle insan dünyasında büyük bir etki gücüne ulaşmış olan sosyal medyanın ve sosyal medya verilerinin kullanıldığı veri bilimi teknolojilerinin her bakımdan insan haklarıyla olan ilişkisi üzerinde düşünülmesi, kişisel verilerin korunması hakkıyla olan bağlantıları üzerinde durulması günümüzün en önemli etik ve hukuksal sorunları arasında yer almalıdır.

Hem Avrupa İnsan Hakları Sözleşmesinde hem de Türkiye Cumhuriyeti Anayasasında özel hayatın ve gizliliğin korunması hakkı, ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması gibi birtakım nedenlerle sadece zorunlu olan ölçüde ve yasalar yoluyla kısıtlanabilmektedir. Hem bireyin hem toplumun güvenliğini korumak amacıyla örneğin, terör gibi suçlarla mücadele etmek veya siber suçları önlemek için güvenlik kameralarıyla izleme, kişisel veri paylaşımı yoluyla kimlik doğrulama gibi gizliliği ilgilendiren uygulamalar yapılmaktadır. Bu önlemler alınırken hukukun "ölçülülük ilkesi"ne göre hareket etmek gerekmektedir. Tehlike ve tehditlerin büyüklüğü doğru değerlendirilmeli, sadece gerektirdiği kadar önlem alınmalı ve söz konusu önlemler amaçları dışında başka amaçlar için kullanılmamalıdır. Diğer önemli nokta ise, eğer güvenlik tehditleri bir izlemeyi gerekli kılıyorsa, bu izlemeyi yapan kurumların kamuoyuna karşı saydam olmasının ve bu şekilde bireyler tarafından da denetlenebilirliğinin sağlanmasıdır. Sosyal medyada kişisel verilerin korunması konusunda alınacak önlemlerin ve yapılacak yasal düzenlemelerin bu noktaları göz önünde bulundurarak gerçekleştirilmesi gerekmektedir.

Günümüzde doğanın ve insan yaşamının seyrinde gerçekleşenlerin birer veri olarak, geliştirilen teknolojiyle neredeyse sınırsız bir şekilde depolanabilmesi ve işlenebilmesi bunu kullanabilenlere büyük bir güç sağlamaktadır. Bilimin öngörme özelliğini olağanüstü şekilde geliştirebilecek yapay zekâ destekli büyük veri teknolojileri de bu bağlamda aklın kamusal kullanımıyla yararlanıldığında insanlık için pek çok fayda

sağlayabileceği gibi daha çok adaletsizlik, ayırımcılık, eşitsizlik ve şiddet de yaratabilecektir.

Sosyal medyanın kazanımları, doğurduğu yeni gereksinimler ve alışkanlıklarla bu gereksinimleri giderme arzusu, isteği, kişilerin çeşitli kaygı ve kuşkularının yanında, neredeyse ağırlıklı bir önceliğe sahip olmaktadırlar. Örnek verdiğimiz birtakım araştırmalara göre kişiler, sosyal medyada gizliliklerinin risk altında olduğunu ve kişisel verilerinin yeterince korunmadığını hatta şirketler ve devletler tarafından izlendiklerini düşünseler de sosyal medyayı kullanmaktan vazgeçemeyeceklerini ve karmaşık gizlilik sözleşmelerini bu platformları kullanmak için kabul etmek zorunda olduklarını ifade etmektedirler. Gizlilik sözleşmelerinin bu hizmetleri kullanmak için bir ön koşul olması ve metinlerin karmaşıklığı açık rızanın oluşabilmesinin koşulları ile çelişkilidir.

Kişisel veriler deposu olması nedeniyle büyük bir kaynak olarak özellikle sosyal medyayı kullanan büyük veri teknolojilerinin olumlu kullanımları olsa da bunların sadece yarattığı olanaklara odaklanmak, sözünü ettiğimiz çok önemli birtakım tehlikeleri gözden kaçırmamıza neden olacaktır. "Bilgi güçtür" anlayışının "veri güçtür" anlayışına dönüştüğü dünyamızda veri üreten insan da araçsallaşmaktadır. Günümüzde bilgi, insan deneyiminden, tür olarak insana ait bilişsel ve duyuşsal özelliklerden koparılarak yapay zekâların çözümlediği temelde matematikten ibaret olan veri ve enformasyona indirgenmektedir. Oysa insanın kendisini ve kurduğu dünyayı anlaması kendisinden koparılan veriye dayalı sayısal çözümlemelerle mümkün olamayacaktır. Teknolojik araçlar insanı yapısına özgü olanaklarından uzaklaştırarak, insanı mekanikleştirmektedir. İnsan, kurduğu dünyayı, kendisini de değiştirebilme gücüyle, insanın değerini koruyan bir şekilde geliştirebileceği gibi, kendi varlığını ve kurduğu dünyayı yok edebilecek etkileri de yaratabilmektedir. Bu nedenle teknoloji-insan etkileşimleri ve özellikle dijitalleşmenin insan yaşamındaki etkileri, çağımızın felsefi ve bilimsel çalışma alanlarındaki en önemli gündem maddelerinden biri olmalıdır. Bu tehlikelere karşı insanlığı korumanın en önemli güvencesini sağlayan hukuk kurumlarının da disiplinlerarası bir anlayışla sürekli gelişmeye açık ve uygun bir şekilde yapılanması sağlanmalıdır. Teknolojideki hızlı gelişmelerle birlikte çoğu sosyal medya üzerinden elde edilen kişisel verilerin işlenmesinin ve böylece mahremiyetin giderek yok olmasının, insanın değeri ve kişi olarak korunması konusunda doğurduğu tehlikeleri önlemek, felsefi

duruş kazandırılmış, sorunları fark edebilen, olan bitene eleştirel şekilde bakabilen bireylerin yetiştirilmesi ve insanların bilinçlenmesiyle mümkündür. Kamusal alandaki düzenlemelerin yapılması için ise etik bilgiye dayanan hukuk normlarının oluşturulması gerekmektedir.

KAYNAKLAR

Abanoz Öztürk, B. (2021). Ceza Muhakemesinde Sanığın Mükerrer Suç İşleme Riskinin Hesaplanması: Compas Algoritması ve Adil Yargılanma Hakkı. Balcı, M. ve Aydın, H. (Ed.). *Yapay Zekanın Cezai Sorumluluğu,* içinde (s. 81-100). 25.04.2023 tarihinde https://www.academia.edu adresinden alındı.

Adalet Bakanlığı Hukuk Sözlüğü İnternet Sitesi. (2023). "Hak" 15.05.2023 tarihinde https://sozluk.adalet.gov.tr/ki%c5%9fi, 20.07.2023 adresinden alındı.

Adalet Bakanlığı Hukuk Sözlüğü İnternet Sitesi. (2023). "Fiil ehliyet" 15.05.2023 tarihinde https://sozluk.adalet.gov.tr/ki%c5%9fi, 20.07.2023 adresinden alındı.

Alternatif Bilişim Derneği. (2013).Veri Korumaya Giriş. (M. Binark ve İ. Dirini. Çev.) 25.07.2023 tarihinde https://ekitap.alternatifbilisim.org/veri-korumaya-giris/ adresinden alındı.

Akıncı A. N. (2019). *Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti* (Uzmanlık Tezi), T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Ankara. 25.04.2023 tarihinde http://www.bilgitoplumu.gov.tr/wp-content/uploads/2019/04/ayse-nur-akinci-tez-WEB.pdf adresinden alındı.

Akıncı, A.N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi. Ankara: Kalkınma Bakanlığı Çalışma Raporu 6. 25.04.2023 tarihinde http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf adresinden alındı.

Akpınar, M. (2023, 17 Nisan). Twitter'ın Yeni Karakter Sınırı 4000 Oldu Ancak Bir Şartla. DonanımHaber Web Sitesi. 24.06.2023 tarihinde https://www.donanimhaber.com/twitter-karakter-siniri-4000-e-yukseltti--160355 adresinden alındı.

Aktan, E. (2018). Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu. *Bilgi Yönetimi*. 1 (1), 1-22. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/by/issue/37228/403010 adresinden alındı.

Amazon Sitesi (2023). İki Adımlı Doğrulama Nedir?. 25.07.2023 tarihinde https://www.amazon.com.tr/gp/help/customer/display.html?nodeId=G3PWZPU52FKN7PW4 adresinden alındı.

Aposto Gündem Haber Sitesi. (2023, 13 Nisan). Elon Musk, Twitter İçin Bir Yapay Zekâ Projesi Üzerinde Çalışıyor. 24.06.2023 tarihinde https://aposto.com/s/elon-musk-twitter-icin-bir-yapay-zeka-projesi-uzerinde-calisiyor adresinden alındı.

Arpa, G. (2018, 24 Temmuz). Şevket Uyanık'tan "Dijital Güvenlik", Umay Aktaş Salman'dan "Eğitim Haberciliği". Bianet. 23.07.2023 tarihinde https://bianet.org/bianet/medya/199465-sevket-uyanik-tan-dijital-guvenlik-umay-aktas-salman-dan-egitim-haberciligi adresinden alındı.

Altınpulluk, H. (2018). Nesnelerin İnterneti Teknolojisinin Eğitim Ortamlarında Kullanımı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 4 (1), 94-111. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/auad/issue/35189/390483 adresinden alındı.

Aras, İ. (2021). Çin'de Sosyal Medya. Aydın, Ö. ve Cengiz, Ç. (Eds.). *Teknoloji ve Uluslararası İlişkiler*, içinde (s. 277-288) , Ankara: Nobel Akademik Yayıncılık.

Arınmış Uzun, S. (2021). Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi. *Bilişim Teknolojileri Dergisi*, 14 (3), 207-221. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/gazibtd/issue/64349/735471 adresinden alındı.

Aries, P. ve Duby, G. (2008). *Özel Hayatın Tarihi: Fransız Devrimi'nden Büyük Savaş'a.* (A. Berktay, Çev.). İstanbul: Yapı Kredi Yayınları.

Aristoteles. (1996). *Metafizik*. (A. Arslan, Çev.) İstanbul: Sosyal Yayınları.

Arslan, M. E. Sosyal Medyada Kişilik Hakları İhlalleri ve Korunma Yolları. 7(2), 123-154. 24.04.2023 tarihinde https://www.jurix.com.tr/article/11659 adresinden alındı.

Aslanyürek, M. (2016). İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi,* 3 (1), 80-106. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/iled/issue/18468/194456 adresinden alındı.

Ataman, B. ve Çoban, B. (Eds.). (2018). *Panoptikon 2.0: Alternatif Medya ve Karşı Gözetim.* (T. E. Kalaycı, Çev.). İstanbul: Kafka Yayınları.

Aust, S. ve Ammann, T. (2019). *Dijital Diktatörlük: Kitlesel Gözetim, Verilerin Kötüye Kullanımı, Siber Savaş.* Ankara: Hece Yayınları.

Bacon, F. (2012). *Novum Organum: Tabiatın yorumu ve İnsan Alemi Hakkında Özlü Sözler.* (S. Önal, Çev.). Ankara: Say Yayınları.

Başarslan, B. (2021). Dataizm: Varlığın Veri Olarak Tasavvuru. *Tevilat: Selçuk Üniversitesi İslami İlimler Fakültesi Dergisi (Tevilat Journal of Islamic Sciences),* 2 (1), 11-25. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/tevilat/issue/65299/961506 adresinden alındı.

Baştürk, E. (2016). *Panoptikon'dan Post Panoptikon'a Gözetimin Soykütüğü. (*Tez no:425431). [Doktora Tezi, Ankara Üniversitesi]. tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Bauman, Z. ve Lyon, D. (2016). *Akışkan Gözetim.* (E. Yılmaz, Çev.).İstanbul: Ayrıntı Yayınları.

BBC News Türkçe Haber Sitesi. (2017, 27 Ekim). Dünya'nın İlk Robot Vatandaşı Suudi Arabistanlı. 13.07.2023 tarihinde https://www.bbc.com/turkce/haberler-dunya-41780346 adresinden edinildi.

BBC News Türkçe Haber Sitesi. (2022, 20 Kasım). Donald Trump'ın Twitter Hesabı Yeniden Açıldı. 24.06.2023 tarihinde https://www.bbc.com/turkce/articles/c0jg0vqk5p7o adresinden alındı.

BBC News Türkçe Haber Sitesi. (2023, 17 Temmuz). Twitter'ın Reklam Geliri Musk'ın Şirketi Satın Almasından Bu Yana Yüzde 50 Azaldı, 03.08.2023 tarihinde

Bilgi Teknolojileri ve İletişim Kurumu Sitesi (2018). Siber Güvenliğin Önemi BTK'da Konuşuldu. 28.07.2023 tarihinde https://btk.gov.tr/haberler/siber-guvenligin-onemi-btk-da-konu Boeing, N. ve Lebert A. (2014, 7 Eylül). "Byung Chul-Han ile Söyleşi: Byung-Chul Han: Üzgünüm Ama Bunlar Gerçekler"(M. N. Sarıkaya, Çev.) AND Center – Analytic Divinity Center. (2019, 14 Aralık). 03.08.2023 tarihinde https://andcenter.org/tr/marifetdivani/byung-chul-hanuzgunum-ama-bunlar-gercekler/ adresinden alındı.suldu adresinden alındı.

Buluz, B. (2019). Türkiye'de Avukatlık Mesleğinde Teknoloji Kullanımı. Çetin, S. (Ed.). *Yapay Zekâ Çağında Hukuk İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu* içinde (s. 36-41).

Bychawska-Siniarska, D.(2018). *Avrupa İnsan Hakları Sözleşmesi Kapsamında İfade Özgürlüğünün Korunması.* (T. D. Köksal, Çev.). 25.04.2023 tarihinde https://rm.coe.int/avrupa-insan-haklar-sozlesmesi-kapsaminda-ifade-ozgurlugunun-korunmasi/168092cff5 adresinden alındı.

Cambridge Dictionary. (2023) "Social Media". 28.07.2023 tarihinde https://dictionary.cambridge.org/dictionary/english/social-media adresinden alındı.

Canada.ca. (2023). Statement By Minister Fortier Announcing A Ban On The Use Of TikTok On Government Mobile Devices, 03.08.2023 tarihinde https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html

Castells, M. (2008a). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Ağ Toplumunun Yükselişi.* (E. Kılıç, Çev.). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Castells, M. (2008b). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Binyılın Sonu.* (E. Kılıç, Çev.). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Cevizci, A. (2005). *Felsefe Sözlüğü.* İstanbul: Paradigma Yayınları.

Ceylan, F. (2023, 10 Nisan). Güvenlik ve Savunmada Yapay Zekânın Yansımaları. Panorama Dergisi. 28.07.2023 tarihinde https://www.uikpanorama.com/blog/2023/04/10/fc-5/ adresinden alındı.

Civelek, Z. (Tarih yok). Ders Notu [Pdf Dosyası] . 28.06.2023 tarihinde https://websitem.karatekin.edu.tr/user_files/zafercivelek/files/20191221_f28833 7c7caa49a2b93c85f11de8be02.pdf adresinden alındı.

Corbett-Davies, S., Pierson, E., Feller, A., Goel, S. (2016, 17 Ekim). A Computer Program Used For Bail And Sentencing Decisions Was Labeled Biased Against Blacks. It's Actually Not That Clear. The Washington Post. 25.07.2023 tarihinde https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/ adresinden alındı.

C.S. Mott Children's Hospital.(2015). Mott Poll Report, Parents On Social Media: Likes And Dislikes Of Sharenting. 03.08.2023 tarihinde http://mottnpch.org/reports-surveys/parents-social-media-likes-and-dislikes-sharenting adresinden alındı.

Cumhuriyet Gazetesi Haber Sitesi. (2022, 07 Şubat). KVKK'den Yemeksepeti'ne Ödül Gibi Ceza. https://www.cumhuriyet.com.tr/turkiye/kvkkden-yemeksepetine-odul-gibi-ceza-1905913, 27.07.2023

Cumhuriyet Gazetesi Haber Sitesi. (2022, 23 Aralık). 'Lensa' Çılgınlığı Sürüyor... Sosyal Medyada 'Avatar' Tehlikesi: Uzmanı Uyardı. 23.07.2023 tarihinde https://www.cumhuriyet.com.tr/yasam/lensa-cilginligi-suruyor-sosyal-medyada-avatar-tehlikesi-uzmani-uyardi-2014772 adresinden alındı.

Cumhuriyet Gazetesi Haber Sitesi. (2023. 10 Temmuz). BM insansı yapay zekâ robot zirvesi düzenledi: "Dünyayı İnsanlardan Çok Daha İyi Yönetebiliriz". 13.07.2023 tarihinde https://www.cumhuriyet.com.tr/bilim-teknoloji/bm-insansi-yapay-zeka-robot-zirvesi-duzenledi-dunyayi-insanlardan-cok-daha-iyi-yonetebiliriz-2098047 adresinden alındı.

Cuthbertson A. (2023, 13 Nisan). AI Clones Child's Voice In Fake Kidnapping Scam. Independent. 23.07.2023 tarihinde https://www.independent.co.uk/tech/ai-voice-clone-scam-kidnapping-b2319083.html adresinden alındı.

Çam, Z. (2021, 11 Ocak). Siber Haklar Uzmanı Yaman Akdeniz Anlattı: WhatsApp'ı Silmek Çözüm Mü?. Cumhuriyet. 27.07.2023 tarihinde https://www.cumhuriyet.com.tr/haber/siber-haklar-uzmani-yaman-akdeniz-anlatti-whatsappi-silmek-cozum-mu-1805165 adresinden alındı.

Çelik, M. ve Varol, E. (2019). Kavram ve Kuramlarıyla Marshall Mcluhan'a Bakış: Günümüzün Egemen Medya Araçları Ekseninde Bir Değerlendirme. *Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi*, 5(1), 137-158. 25.04.2023 tarihinde https://dergipark.org.tr/tr/download/article-file/744648 adresinden alındı.

Çotukösken, B. (1994). *Felsefi Söylem Nedir?,* İstanbul: Kabalcı Yayınevi

Çotuksöken, B. (2012). *İnsan Hakları ve Felsefe.* İstanbul: Papatya Yayıncılık

Çotuksöken, B. (2018). *Felsefenin Gör Dediği I: Antropontoloji Ya Da İnsan-Varlıkbilgisi.* İstanbul: Notos Kitap Yayınevi.

Çotuksöken, B. (2021). *Felsefenin Gör Dediği II: Antropontolojinin Işığında Etik ya da Ahlak Felsefesi.* İstanbul: Notos Kitap Yayınevi.

Davenport, T. H. ve Prusak, L. (2001). *İş Dünyasında Bilgi Yönetimi: Kuruluşlar Ellerindeki Bilgiyi Nasıl Yönetirler?*. (G. Günay, Çev.). İstanbul: Rota Yayınları.

Dawley, L. (2009). Social Network Knowledge Construction: Emerging Virtual World Pedagogy. On The Horizon, 17 (2), 109-121. 25.04.2023 tarihinde

https://www.academia.edu/303617/Social_Network_Knowledge_Construction_Emerging_Virtual_World_Pedagogy adresinden alındı.

Demir, A. (2018). Ölümsüzlük ve Yapay Zekâ Bağlamında Trans-hümanizm . *AJIT-e: Academic Journal Of Information Technology*, 9 (31), 95-104. 25.04.2023 tarihinde https://dergipark.org.tr/en/download/article-file/1113735 adresinden alındı.

Discover the Domo Data Experience Platform. (2023). Data Never Sleeps 10.0. 28.06.2023 tarihinde https://www.domo.com/data-never-sleeps#top adresinden alındı.

Directive 95/46/EC Of The European Parliament And Of The Council. (24 October 1995). Official Journal (L 281) 24.04.2023 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 adresinden alındı.

Doğan, K. ve Arslantekin, S. (2016). Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 56 (1) , 15-36. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/dtcfdergisi/issue/66793/1044418 adresinden alındı.

Dönmez, Samet. (2022, Kasım). Sosyal Medya Paylaşımlarınız Deepfake İçin Kullanılabilir!. Tamindir Teknoloji Haberleri. 24.07.2023 tarihinde https://www.tamindir.com/haber/sosyal-medya-paylasimlariniz-deepfake-icin-kullanilabilir_77557/ adresinden alındı.

Drury, G. (2008). Opinion Piece: Social Media: Should Marketers Engage And How Can It Be Done Effectively? *Journal of Direct, Data and Digital Marketing Practice*, 3 (9), 274–277. 25.04.2023 tarihinde https://www.researchgate.net/publication/32002189_Opinion_piece_Social_media_Should_marketers_engage_and_how_can_it_be_done_effectively adresinden alındı.

Duvar Gazetesi Haber Sitesi. (2023, 07 Haziran). Putin'in 'Deepfake' Videosu Yayınlandı: Sıkıyönetim İlan Etti. 24.07.2023 tarihinde https://www.gazeteduvar.com.tr/putinin-deepfake-videosu-yayinlandi-sikiyonetim-ilan-etti-haber-1622432 adresinden alındı.

Dünya Gazetesi Haber Sitesi. (2023, 19 Mayıs). Twitter'dan Microsoft'a Suçlama. 24.06.2023 tarihinde https://www.dunya.com/sirketler/twitterdan-microsofta-suclama-haberi-694156 adresinden alındı.

Dülger, M. V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 3 (2), 101-168. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/imuhfd/issue/54311/736998 adresinden alındı.

Dülger, M. V. (2018). İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 5 (1), 71-144. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/imuhfd/issue/54314/737027 adresinden alındı.

Dülger, M. V. (2019). Avrupa Birliği Genel Veri Koruma Tüğüzü Bağlamında Kişisel Verilerin Korunması. *Yaşar Hukuk Dergisi,* 1 (2) , 71-174. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/yhd/issue/52537/807628 adresinden alındı.

Edosomwan S, Prakasan S. K, Kouame D. ve Watson J, Seymour T. (2011) The History Of Social Media And Its Impact On Business. The Journal of Applied Management And Entrepreneurship, 16 (3), 79–91. 25.04.2023 tarihinde https://www.researchgate.net/publication/303216233_The_history_of_social_media_and_its_impact_on_business adresinden alındı.

Ege, B. (2013). Rastlantının Bittiği Yer: Big Data. *Bilim ve Teknik*, 550, 22-26. 25.04.2023 tarihinde https://services.tubitak.gov.tr/edergi/yazi.pdf;jsessionid=mTlHvOAbYGKyukPE16cVKO4m?dergiKodu=4&cilt=46&sayi=818&sayfa=22&yaziid=35152 adresinden alındı.

Eğri, T. (2019). Sosyal Medyanın Kavramsal Çerçevesi, Tarihi ve Geleneksel Medya ile İlişkisi. Yıldırım, K. E. (Ed.). *Sosyal Medyaya Giriş,* içinde (s. 3-32) 25.04.2023 tarihinde https://ddp.anadolu.edu.tr/#/course/SMY101U adresinden alındı.

Ekin, B. (2020*). Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri* (Yüksek Lisans Tezi). İhsan Doğramacı Bilkent Üniversitesi Ekonomi ve Sosyal Bilimler Enstitüsü, Ankara. 25.04.2023 tarihinde https://repository.bilkent.edu.tr/server/api/core/bitstreams/2840a2c1-f956-4c8e-8197-c90cc6fe0e03/content adresinden alındı.

Ergün, Ö. (2017). Kişi Kavramı ve Çeşitleri. *Dicle Üniversitesi Adalet Yüksekokulu Dicle Adalet Dergisi*, 1 (1), 1-14. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/duamydad/issue/38286/442689 adresinden alındı.

Esgin, M. S. (2015). Web Teknolojileri Dünyasında Yeni Trendler. Baloğlu, A. (Ed.). *Sosyal Medya Madenciliği*, içinde (s. 17-59). İstanbul: Beta Yayınları.

European Parliament. (2021). Tackling Deepfakes In European Policy. 24.07.2023 tarihinde https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf adresinden alındı.

Facebook Sitesi (2023). Facebook'ta İzin Verilen Adlar. 23.04.2023 tarihinde https://tr-tr.facebook.com/help/229715077154790 adresinden alındı.

Facebook Sitesi (2023). Gizlilik Merkezi. 23.04.2023 tarihinde https://www.facebook.com/privacy/policy/ adresinden alındı.

Facebook Sitesi (2023). Race Data Measurement and Meta's Commitment to Fair and Inclusive Products, 23.04.2023 tarihinde https://about.fb.com/news/2021/11/inclusive-products-through-race-data-measurement/ adresinden alındı.

Facebook Sitesi (2023). The Facts On News Reports About Facebook Data. 03.08.2023 tarihinde https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/ adresinden alındı.

FamilyTreeDNA Sitesi. (2019). Press Release: Helping Connect The Dots. 03.08.2023 tarihinde https://blog.familytreedna.com/press-release-connecting-families-and-saving-lives/ adresinden alındı.

Federal Trade Commission. (2019). FTC Imposes $5 Billion Penalty And Sweeping New Privacy Restrictions On Facebook. 05.08.2023 tarihinde https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook adresinden alındı.

Fuchs, C. (2018). Sosyal Medya: Eleştirel Bir Giriş. (İ. Kalaycı ve D. Saraçoğlu, Çev.). İstanbul: Notabene Yayınları.

Future of Life Institute. (2023). Pause Giant AI Experiments: An Open Letter. 03.08.2023. https://futureoflife.org/open-letter/pause-giant-ai-experiments/ adresinden alındı.

Gazete Oksijen Haber Sitesi. (2023, 10 Mayıs). Google Microsoft'a Meydan Okudu, Yapay Zeka Destekli Arama Motorunu Tanıttı. 24.07.2023 tarihinde https://gazeteoksijen.com/bilim-ve-teknoloji/google-microsofta-meydan-okudu-yapay-zeka-destekli-arama-motorunu-tanitti-178012 adresinden alındı.

Geuss, R. (2007). *Kamusal Şeyler Özel Şeyler.* İstanbul: Yapı Kredi Yayınları.

GOV.UK. (2023). TikTok Banned On UK Government Devices As Part Of Wider App Review. 03.08.2023 tarihinde https://www.gov.uk/government/news/tiktok-banned-on-uk-government-devices-as-part-of-wider-app-review adresinden alındı.

Göçmen Uyarer, S. (2019). *6698 Kişisel Verilerin Korunması Kanunu ve 5278 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. (Tez no: 565139) [Yüksek Lisans Tezi, Galatasaray Üniversitesi]. tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Gökaliler, E. ve Saatçioğlu, E. (2020). Sosyal Büyük Veri Ekseninde Kişisel Gizlilik Sorunsalı: Türkiye'de Eğitimli ve Kentli Sosyal Ağ Kullanıcılarının Gizlilik Sorunlarına Yaklaşımları . *Istanbul University Journal of Communication*

Sciences, 0 (58), 133-167. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/connectist/issue/56249/775894 adresinden alındı.

Gökalp, M. O., Kayabay, K., Çoban, S. ve Eren, P. E. (2018, Ekim). Büyük Veri Çağında İşletmelerde Veri Bilimi. *Fifth International Management Information Systems Conference,* Ankara. 25.04.2023 tarihinde https://hdl.handle.net/11511/79419 adresinden alındı.

Gönenç, Ö. (2003). İletişimin Tarihi. *İstanbul Üniversitesi İletişim Fakültesi Dergisi (Istanbul University Faculty of Communication Journal)* 0 (18) 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/iuifd/issue/22890/244916 adresinden alındı. Goujard, C. (2023, 22 Mart). What The Hell Is Wrong With TikTok?. Politico. 03.08.2023 tarihinde https://www.politico.eu/article/tiktok-china-west-europe-ban-app-espionage-surveillance/ adresinden alındı.

Gözler, Ö. ve Tahirler P. (2022, 03 Nisan). 'Dijital Dünyada Yüzde 100 Güvenlik Diye Bir Şey Yok'. Hürriyet. 23.07.2023 tarihinde https://www.hurriyet.com.tr/kelebek/hurriyet-pazar/dijital-dunyada-yuzde-100-guvenlik-diye-bir-sey-yok-42035052 adresinden alındı.

Gupta, A. M., Dr. Katiyar, D. ve Goel, G. (2022).Web 3.0 And Its Reflections On The Future Of E-Learning. *International Journal for Research in Applied Science & Engineering Technology*, 10 (4), 507-512. 25.04.2023 tarihinde https://www.ijraset.com/best-journal/web3.0-and-its-reflections-on-the-future-of-elearning adresinden alındı.

Güler, O. ve Savaş, S. (2022). Tüm Yönleriyle Metaverse Çalışmaları, Teknolojileri ve Geleceği. *Gazi Mühendislik Bilimleri Dergisi,* 8 (2), 292-319. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/gmbd/issue/72442/1091628 adresinden alındı.

Gürzumar, D. D. (2019). Hukuk Fakültelerinin Dönüşümü. Çetin, S. (Ed.). *Yapay Zekâ Çağında Hukuk İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu* içinde (s. 22-27). 25.04.2023

tarihindehttps://www.istanbulbarosu.org.tr/files/docs/Yapay_Zeka_Caginda_Hukuk2019.pdf adresinden alındı.

Güven Kavak, N. (2022). *Avrupa Birliği Genel Koruma Tüzüğü Doğrultusunda Profilleme ve Otomatik Karar Alma*. (Tez no: 747762). [Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi]. tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Güvenli İnternet Merkezi Sitesi. (2023). We Are Social ve Hootsuite'in Digital 2023 1. Çeyrek Raporu Çevirisi. 21.06.2023 tarihinde https://www.guvenliweb.org.tr/dosya/dADI9.pdf adresinden alındı.

Güvenli İnternet Merkezi Sitesi. (2023). Sosyal Ağlarda Güvenlik. 28.07.2023 tarihinde https://www.guvenliweb.org.tr/dokuman-detay/sosyal-aglarda-guvenlik adresinden alındı.

Habertürk Haber Sitesi. (2020, 17 Aralık). Yapay Zeka İle Sahte Obama Videosu. 24.07.2023 tarihinde https://www.haberturk.com/video/haber/izle/yapay-zeka-ile-sahte-obama-videosu/508378 adresinden alındı.

Hafızoğulları, Z. (1997). İnsan Hakkı Olarak Kişilik Hakları ve Kişilik Haklarının Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*,46 (1), 1-40. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/auhfd/issue/42686/514774 adresinden alındı.

Hamilton, I. A. (2022, 08 Eylül). Senior Facebook Engineers Say No One At The Company Knows Where Your Data Is Kept. Business Insider. 23.07.2023 tarihinde https://www.businessinsider.com/meta-doesnt-know-where-all-your-data-is-engineers-say-2022-9 adresinden alındı.

Han, B. (2020). *Şeffaflık Toplumu.* (H. Barışcan, Çev.). İstanbul: Metis Yayınları.

Han, B. (2022). *Enfokrasi: Dititalleşme ve Demokrasinin Krizi.* (M. Özdemir, Çev.). İstanbul: Metis Yayınları.

Harari, Y. N. (2016). *Homo Deus: Yarının Kısa Bir Tarihi.* (P. N. Taneli, Çev.). İstanbul: Kolektif Kitap Yayınevi.

Holmes, A. (2021, 3 Nisan). 533 Million Facebook Users' Phone Numbers And Personal Data Have Been Leaked Online. Business Insider, 03.08.2023 tarihinde https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 adresinden alındı.

Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., Maziad, M. (2011). Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?. *SSRN Electronic Journal.* 25.04.2023 tarihinde https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096 adresinden alındı.

Human Rights Watch. (2015). US: Pass USA Freedom Act. 06.08.2023 tarihinde https://www.hrw.org/news/2015/04/30/us-pass-usa-freedom-act adresinden alındı.

Human Rights Watch. (2017). China's Chilling 'Social Credit' Blacklist. 03.08.2023 tarihinde https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist adresinden alındı.

İletişim Ansiklopedisi İletişim Bilimleri Hiper Görsel Kaynak Sitesi. (2023). "Marshall McLuhan'ın "Araç İletidir" Koyutu". 20.07.2023 tarihinde http://yenimedya.info/2019/10/22/the-medium-is-the-massage/ adresinden alındı.

İnsan Hakları Dairesi Başkanlığı İnternet Sitesi (2023) 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi. (28.01.1981). 29.07.2023 tarihinde https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf adresinden alındı.

İnsan Hakları ve Eşitlik Uzmanları Derneği (2023). Birleşmiş Milletler İnsan Hakları Sözleşmeleri Tablosu. 28.07.2023 tarihinde https://www.ihud.org/uploads/ihud.org/files/BM_%C4%B0nsan_Haklar%C4%B1_S%C3%B6zle%C5%9Fmeleri3.pdf adresinden alındı.

İstanbul Barosu Yapay Zekâ Çalışma Grubu. (2020) Algoritmik Karar Verme ve Veri Koruması. 27.07.2023 tarihinde https://www.istanbulbarosu.org.tr/files/docs/AlgoritmikKararVermeveVeriKorumas%C4%B1022020.pdf adresinden alındı.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. (04.05.2007). Resmi Gazete (Sayı:26530) 15.05.2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf adresinden alındı.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun. (29.07.2020). Resmi Gazete. (Sayı:31202). 15.05.2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm adresinden alındı.

Kalelioğlu, E. (2023, 28 Şubat). WhatsApp Sohbetlerine de Yapay Zekâ Geliyor: Mark Zuckerberg, Kurduğu Yeni Ekibi Duyurdu. Webtekno Güncel Teknoloji Haberleri ve Video İncelemeleri İnternet Sitesi. 24.06.2023 tarihinde https://www.webtekno.com/mark-zuckerberg-yapay-zeka-icin-yeni-ekip-kurdu-h132515.html adresinden alındı.

Kant, I. (1784) "'Aydınlanma Nedir?' Sorusuna Yanıt. (N. Bozkurt, Çev.) *Toplumbilim Aydınlanma Özel Sayısı* (11), (2000, Temmuz). İstanbul: Bağlam Yayıncılık.

Kaplan, A. M. ve Michael, H. (2010). Users Of The World, Unite! The Challenges And Opportunities Of Social Media. *Business Horizons*, 53 (1), 59-68. 25.04.2023 tarihinde https://www.researchgate.net/publication/222403703_Users_of_the_World_Unite_The_Challenges_and_Opportunities_of_Social_Media adresinden alındı.

Karaman, B. (2015). Roma Hukukunda 'Persona' Kavramı. *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi,* 10(127), 81-114. 25.04.2023 tarihinde https://www.jurix.com.tr/article/4594 adresinden alındı.

Keyvan, Ö. Z. (2022). Çin'in Sosyal Kredi Sistemi: Veri Odaklı Toplumda Ahlaki Yönetimin İnşası. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi,* 23(1), 143-166. 25.04.2023 tarihinde http://esjournal.cumhuriyet.edu.tr/tr/download/article-file/1984749 adresinden alındı.

Kırık, A. M. (2012). Arap Baharı Bağlamı'nda Sosyal Medya-Birey Etkileşimi ve Toplumsal Dönüşüm, *21. Yüzyılda Eğitim ve Toplum Eğitim Bilimleri ve Sosyal Araştırmalar Dergisi,* 1 (3), 87-98. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/egitimvetoplum/issue/5130/69848 adresinden alındı.

Kızrak, M. A. (2019). Hukuk ve Teknoloji İlişkisi. Çetin, S. (Ed.). *Yapay Zekâ Çağında Hukuk İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu* içinde (s. 17-21). 25.04.2023 tarihinde.https://www.istanbulbarosu.org.tr/files/docs/Yapay_Zeka_Caginda_Hukuk2019.pdf adresinden alındı.

Kirtiş, A. K. Ve Karahan, F. (2011). To Be or Not to Be In Social Media Arena As The Most Cost-Efficient Marketing Strategy After The Global Recession. *Procedia Social and Behavioral Sciences,* 24, 260-268. 25.04.2023 tarihinde https://www.researchgate.net/publication/229316742_To_Be_or_Not_To_Be_in_Social_Media_Arena_as_the_Most_Cost-Efficient_Marketing_Strategy_after_the_Global_Recession adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2021). Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ Veri İhlal Bildirimi Hakkında" Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarih ve 2021/1324 Sayılı Karar Özeti. 23.07.2023 tarihinde https://www.kvkk.gov.tr/Icerik/7168/2021-1324 adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2023). 100 Soruda Kişisel Verilerin Korunması Kanunu, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf, 23.01.2023

Kişisel Verileri Koruma Kurumu.(2023).6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı, Kişisel Verileri Koruma Kurumu.(2023). https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami, 27.07.2023

Kişisel Verileri Koruma Kurumu.(2023). Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler). 25.07.2023 tarihinde https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2023).Kişisel Verileri Koruma Kurumu'nun Yapısı ve Görevleri. 28.07.2023.https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0%20KORUMA%20KURULU%E2%80%99NUN%20YAPISI%20VE%20G%C3%96REVLER%C4%B0.pdf adresinden alındı.

Kişisel Verileri Koruma Kurumu. (2023).Kişisel Verilerin İşlenme Şartları. 23.01.2023 tarihinde https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari adresinden alındı.

Kişisel Verileri Koruma Kurumu. (2023). Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler. 23.01.2023 tarihinde https://kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2023). Kişisel Verilerin Korunması Kanunu ve Uygulaması. 23.01.2023 tarihinde https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf 28.07.2023 adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2023). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. 23.01.2023 tarihinde https://kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf adresinden alındı.

Kişisel Verileri Koruma Kurumu.(2023). Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi. 23.01.2023 tarihinde https://www.kvkk.gov.tr/Icerik/7005/Kisisel-Verilerin-Silinmesi-Yok-Edilmesi-veya-Anonim-Hale-Getirilmesi#:~:text=Ki%C5%9Fisel%20verilerin%20anonim%20hale%20getirilmesi,ger%C3%A7ek%20ki%C5%9Fiyle%20ili%C5%9Fkilendirilemeyecek%20hale%20getirilmesidir adresinden alındı

Kişisel Verileri Koruma Kurumu.(2023).Özel Nitelikli Kişisel Verileri İşleme Şartları. 23.01.2023 tarihinde https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari adresinden alındı.

Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayı ve 24 Ekim 1995 Tarihli Avrupa Birliği Konseyi ve Avrupa Parlementosu Direktifi, 06.08.2023 tarihinde http://ihop.org.tr/wpcontent/uploads/2011/02/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf

Kişisel Verilerin Korunma Kanunu (24.03.2016). Resmi Gazete. (Sayı : 29677). 25.04.2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf adresinden alındı.

Koetse M. (2019, 3 Mayıs). Zhejiang Movie Theatre Displays Blacklisted Individuals In Avengers Movie Preview. What's On Weibo Web Sitesi. 03.08.2023 tarihinde https://www.whatsonweibo.com/zhejiang-movie-theatre-displays-blacklisted-individuals-in-avengers-movie-preview adresinden alındı.

Köse, N. Ö. (Tarih yok). Temel Bilgi Teknolojileri II [PowerPoint Slayt]. 29. 07.2023 tarihinde https://acikders.ankara.edu.tr/mod/resource/view.php?id=138045 adresinden alındı.

Kramer, A. D., Guillory, J. E. ve Hancock, J. T. (2014) Experimental Evidence Of Massive-Scale Emotional Contagion Through Social Networks. *Proceedings of the National Academy of Sciences* 111(24), 1-3. 25.04.2023 tarihinde https://www.researchgate.net/publication/262813340_Experimental_Evidence_o

f_Massive-Scale_Emotional_Contagion_Through_Social_Networks adresinden alındı.

Kuçuradi, İ. (1995). Knowledge And Its Object. In Kuçuradi, İ. ve Cohen, R. S. (Eds.), *The Concept of Knowledge* (pp. 97-119). Dordrecht: Kluwer Academic Publishers.

Kuçuradi, İ. (2018). *İnsan Hakları: Kavramları ve Sorunları*. Ankara: Türkiye Felsefe Kurumu.

Kuçuradi, İ. (2020). *İnsan ve Değerleri.* Ankara: Türkiye Felsefe Kurumu.

Kuonen, D. (2004). Data Mining And Statistics: What Is The Connection?. *The Data Administration Newsletter*, 30, 1-6. 25.04.2023 tarihinde https://www.researchgate.net/publication/228757258_Data_Mining_and_Statistics_What_is_the_Connection adresinden alındı.

Kurdoğlu, B. ve Ata, Ç. D. (2021). Veri Ekonomisi ve Rekabet Hukuku. *Bilişim Hukuku Dergisi*, 3 (2), 266-337. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/bilisimhukukudergisi/issue/67790/1013073 adresinden alındı.

Lexist Avukatlık Bürosu Sitesi (2023). İfade Özgürlüğünün Kişisel Verilerin Korunması Kanunu Bakımından Sınırlandırılması. 29.05.2023 tarihinde https://lexist.com.tr/yayinlarimiz/ifade-ozgurlugunun-kisisel-verilerin-korunmasi-kanunu-bakimindan-sinirlandirilmasi/ adresinden alındı.

Løkke, E. (2020). *Mahremiyet: Dijital Toplumda Özel Hayat.* (D. Başak, Çev.). İstanbul: Koç Üniversitesi Yayınları.

Maltepe Üniversitesi Sitesi. (2023). İnsan Hakları Evrensel Bildirgesi.(10 Aralık 1948). 25.06.2023 tarihinde https://www.maltepe.edu.tr/Content/Media/CkEditor/29042020025456853-insanhaklari.pdf adresinden alındı.

Mayfield, A. (2008). *What Is Social Media.* 25.04.2023 tarihinde www.icrossing.co.uk/.../What_is_Social_Media_iCrossing_ebook.pdf adresinden alındı.

McLuhan, M. ve Powers, B. R. (2020). *Global Köy: 21. Yüzyılda Yeryüzü Yaşamında ve Medyada Meydana Gelebilecek Dönüşümler.* (B. Öcal, Çev.). İstanbul: Scala Yayıncılık.

Medin, B. (2017). Dijitalleşen Dünyada Fikri Haklar Sorunu. *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi*, 7 (2), 51-68. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/kusbd/issue/30549/295065 adresinden alındı.

Mengüşoğlu, T. (2017). *İnsan Felsefesi.* Ankara: Doğu Batı Yayınları.

Microsoft Sitesi (2023).What Is A VPN Service. 03.08.2023 tarihinde https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn/#what-is-a-vpn adresinden alındı.

Mill, J. S. (2000), *Özgürlük Üstüne.* (A. Ertan, Çev.). İstanbul: Belge Yayınları.

Mobile Verification Toolkit Sitesi.(2023). Mobile Verification Toolkit, 03.08.2023 tarihinde https://docs.mvt.re/en/latest/ adresinden alındı.

Montana.gov.(2023). Governor Gianforte Bans TikTok In Montana. 03.08.2023 tarihinde https://news.mt.gov/Governors-Office/Governor_Gianforte_Bans_TikTok_in_Montana adresinden alındı.

Musk, E. (2023, 1 Temmuz).[@Elon Musk]. To address extreme levels of data scraping & system manipulation, we've applied the following temporary limits:.03.08.2023 tarihinde https://twitter.com/elonmusk/status/1675187969420828672?s=20 adresinden alındı.

Musk, E. (2023, 19 Nisan).[@Elon Musk]. They trained illegally using Twitter data. Lawsuit time. 03.08.2023 tarihinde

https://twitter.com/elonmusk/status/1648784955655192577?s=20 adresinden alındı.

Musk, E. (2023, 25 Nisan).[@Elon Musk]. Verified accounts are now prioritized. [Tweet] 03.07.2023 tarihinde https://twitter.com/elonmusk/status/1650731557164818437?s=20 adresinden alındı.

Nature Journal Sitesi. (2013). When Google Got Flu Wrong. 03.08.2023 tarihinde https://www.nature.com/articles/494155a adresinden alındı.

Neuralink Sitesi (2023).Mission. 03.08.2023 tarihinde https://neuralink.com/ adresinden alındı.

Online Etymology Dictionary. (2023). "Datum" 28.07.2023 tarihinde https://www.etymonline.com/word/datum adresinden alındı.

Özgentürk, J. (2022, 08 Şubat). Alman Delivery Hero'nun 589 Milyon Dolara Aldığı Yemeksepeti Çalışanları Kararlı. Cumhuriyet Gazetesi. 27.07.2023 tarihinde https://www.cumhuriyet.com.tr/ekonomi/alman-delivery-heronun-589-milyon-dolara-aldigi-yemeksepeti-calisanlari-kararli-1906045 adresinden alındı.

Öztemel, E. (2020). Yapay Zekâ ve İnsanlığın Geleceği. Şeker, M., Bulduklu, Y., Korkut, C. ve Doğrul, M. (Eds.). *Bilişim Teknolojileri ve İletişim: Birey ve Toplum Güvenliği,* içinde (s. 96-112). 25.04.2023 tarihinde https://www.tuba.gov.tr/tr/yayinlar/suresiz-yayinlar/bilim-ve-dusunce/bilisim-teknolojileri-ve-iletisim-birey-ve-toplum-guvenligi-1 adresinden alındı.

Öztemel K., Traş, Z. (2019). Facebook Yoğunluğunun Bazı Kişilik Özellikleri İle İlişkisi, *Türk Eğitim Bilimleri Dergisi*, 17(1), 121-139. 25.04.2023 tarihinde https://dergipark.org.tr/tr/download/article-file/744035 adresinden alındı.

Paşaoğlu, C. ve Cevheroğlu, E. (2020). Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması. *Bilişim Teknolojileri Dergisi,* 13 (2) , 183-195. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/gazibtd/issue/54106/559235 adresinden alındı.

Platon. (1945). *Phaidros.* (H. Akverdi, Çev.). İstanbul: Maarif Matbaası.

Postman, N. (2006). *Teknopoli: Yeni Dünya Düzeni.* (M. E. Yılmaz, Çev.). İstanbul: Paradigma Yayıncılık.

Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data. (14 Aralık 1960). 28.07.2023 tarihinde https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 adresinden alındı.

Roagna, I. (2012). *Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması.*(A. G. Alkış Schäling, Çev.). 25.04.2023 tarihinde https://rm.coe.int/16806f15ae adresinden alındı.

Sağıroğlu, Ş. ve Sinanç, D. (2018). Siber Güvenlik İçin Büyük Veri Yaklaşımları. Sağıroğlu, Ş. ve Alkan, M. (Eds.) *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, içinde (s.375-384). Ankara: Grafiker Yayınevi.

Savaş, S., Topaloğlu, N. ve Yılmaz, M. (2012). Veri Madenciliği ve Türkiye'deki Uygulama Örnekleri. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 11 (21), 1-23. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/ticaretfbd/issue/21361/229131 adresinden alındı.

Serozan, R. (1977). Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler. *İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi*, 11 (14), 93-112. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/iumhad/issue/1273/15252 adresinden alındı.

Seyıdov, I. (2021). "Büyük Verinin Gücü Adına": Siyasi Kampanyalarda Etkili Veri Kullanımı. *TRT Akademi*, 6 (11), 32-49. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/trta/issue/60117/802534#article_cite adresinden alındı.

Sözcü Haber Sitesi. (2023, 24 Mart). Deepfake İle Donald Trump'ın Tutuklanmasını Böyle Resmettiler. 24.07.2023 tarihinde

https://www.sozcu.com.tr/2023/teknoloji/deepfake-ile-donald-trumpin-tutuklanmasini-boyle-resmettiler-7631238 adresinden alındı

Şahin, Z. B. (2022). 7253 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da Değişiklik Yapılmasına Dair Kanun"un İfade Özgürlüğü ve Kişilik Hakları Bağlamında Değerlendirilmesi. *Euroasaia Journal Of Social Sciences & Humanities,* 9 (2), 28-44. 25.04.2023 tarihinde https://www.euroasiajournal.com/index.php/eurssh/article/download/147/145 adresinden alındı.

Tarhan, A. (2019a). Dijitalleşmenin Kavramsal ve Tarihsel Süreci. Akdağ, M. (Ed.). *Dijital Kültür ve Sosyal Medya,* içinde (s. 4-19). 25.04.2023 tarihinde https://icerik.ataaof.edu.tr/?d=dijitalkulturvesosyalmedya adresinden alındı.

Tarhan, A. (2019b). Sosyal Medyanın Kavramsal ve Tarihsel Süreci. Akdağ, M. (Ed.). *Dijital Kültür ve Sosyal Medya,* içinde (s. 104-122). 25.04.2023 tarihinde https://icerik.ataaof.edu.tr/?d=dijitalkulturvesosyalmedya adresinden alındı.

TBMM. (2023). Medenî ve Siyasî Haklara İlişkin Uluslararası Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu. (Rapor no: 1/589).28.07.2023 tarihinde https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c016/tbmm22016089ss0150.pdf adresinden alındı.

TBMM. (2023).Türkiye Cumhuriyeti Anayasası ve Türkiye Büyük Millet Meclisi İçtüzüğü.(Ağustos 2020) 28.07.2023 tarihinde https://www5.tbmm.gov.tr/yayinlar/2021/TC_Anayasasi_ve_TBMM_Ic_Tuzugu.pdf adresinden alındı.

T.C. Cumhurbaşkanlığı Resmi Gazete. (2023). İnternet Ortamında Yapılan Yayınların Düzenlenmesine ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (23.05.2007) Resmi Gazete (Sayı: 26530). (25.04.2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf adresinden alındı.

T.C. Cumhurbaşkanlığı Resmi Gazete (2023). Kişisel Verileri Koruma Kurumu.(2023). Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik. Resmi Gazete (Sayı:3022403). 03.08.2023tarihinde https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm adresinden alındı.

T.C. Cumhurbaşkanlığı Resmi Gazete (2023). 27 Mayıs 1949 tarih ve 7217 Sayılı Bakanlar Kurulu Kararı.(27.06.1946). Resmi Gazete (Sayı: 7217). 25.08.2023 tarihinde https://www.resmigazete.gov.tr/arsiv/7217.pdf adresinden alındı.

T.C. Dışişleri Bakanlığı Sitesi. (2023). Avrupa Konseyi. 25.08.2023 tarihinde https://www.mfa.gov.tr/insan-haklari-ve-avrupa-konseyi.tr.mfa#:~:text=T%C3%BCrkiye%20AK'n%C4%B1n%20kurucu%20%C3%BCyeleri,ve%20Mahkeme%20i%C3%A7tihad%C4%B1n%C4%B1%20temel%20almaktad%C4%B1r adresinden alındı.

T.C Yargıtay Başkanlığı Sitesi (2023).Avrupa İnsan Hakları Sözleşmesi, 11. Ve 14. Ek Protokoller (2010). 03.08.2023 tarihinde https://www.yargitay.gov.tr/documents/AIHM.pdf, adresinden alındı.https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf adresinden alındı.

TDK. (2023). “Kişisel”. 23.01.2023 tarihinde https://sozluk.gov.tr/ adresinden alındı.

TDK. (2023). “Kişi”. 23.01.2023 tarihinde https://sozluk.gov.tr/ adresinden alındı.

Tekin, A. (2020, 08 Temmuz). Yaman Akdeniz: Sosyal Medya Düzenlemesi Daha Fazla Sansür, Daha Fazla Yargılama Getirir. Duvar Gazetesi. 27.07.2023 tarihinde https://www.gazeteduvar.com.tr/gundem/2020/07/08/yaman-akdeniz-sosyal-medya-duzenlemesi-daha-fazla-sansur-daha-fazla-yargilama-getirir adresinden alındı.

The White House Sitesi.(2023).“No TikTok On Government Devices” Implementation Guidance. (17.02.2023). 03.08.2023 tarihinde https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf adresinden alındı.

Turhan, F. ve Aksu, M. (2011). 11 Eylül Sonrası ABD'de Özgürlük ve Güvenlik Dengesi Açısından Terörü Önleme Amaçlı Tedbirler/ Özellikle Patriot Kanunu İle Getirilen Kısıtlamalar. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 1 (1), 47-90. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/sduhfd/issue/22980/245816 adresinden alındı.

Türk Medeni Kanunu. (22.11.200). Resmi Gazete. (Sayı : 24607). 25.04.2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4721.pdf adresinden alındı.

Türkçe Etimoloji Sözlüğü. "Dijital" (2023). 20.07.2023 tarihinde https://www.etimolojiturkce.com/kelime/dijital adresinden alındı.

Twitter İnternet Sitesi (2023). Twitter Privacy Policy. 24.06.2023 tarihinde https://twitter.com/en/privacy#update adresinden alındı.

Twitter İnternet Sitesi. (2023). Hukuki Talep SSS. 29.05.2023 tarihinde https://help.twitter.com/tr/rules-and-policies/twitter-legal-faqs adresinden alındı.

Twitter İnternet Sitesi. (2023). Twitter'da Mavi Onay İşareti Alma. 28.07.2023 tarihinde https://help.twitter.com/tr/man)aging-your-account/about-twitter-verified-accounts adresinden alındı.

Uçak, M. (2021). Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası. *Kişisel Verileri Koruma Dergisi*, 3 (1), 41-60. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/kvkd/issue/62960/826099 adresinden alındı.

USA Freedom Act, (June 2, 2015). Hause Judiciary Committee Republicans. 06.08.2023 tarihinde https://judiciary.house.gov/usa-freedom-act adresinden alındı.

USOM. (2023). Bireysel Siber Güvenlik Önlemleri, 27.07.2023 tarihinde https://www.usom.gov.tr/faydali-dokumanlar/bireysel-siber-guvenlik-onlemleri adresinden alındı.

Ünver, O. (2015). Sosyal Medya Madenciliği. Baloğlu, A. (Ed.). *Sosyal Medya Madenciliği,* içinde (s. 79-94). İstanbul: Beta Yayınları.

Üstün, K. (2023, 27 Nisan). Görüş - Sosyal Medyanın Orantısız Gücü ve Elon Musk Döneminde Twitter. Anadolu Ajansı. 24.06.2023 tarihinde https://www.aa.com.tr/tr/analiz/gorus-sosyal-medyanin-orantisiz-gucu-ve-elon-musk-doneminde-twitter/2882498 adresinden alındı.

Vatansever, M. V. (2012). Kamu İcra Hukuku'nda Ölçülülük İlkesi, *Maltepe Üniversitesi Hukuk Fakültesi Dergisi*, 2 (2), 87- 98. 25.04.2023 tarihinde https://hdl.handle.net/20.500.12415/2601 adresinden alındı.

Vopson, M. M. (2020). The İnformation Catastrope. *AIP Advances*, 10(8). 25.04.2023 tarihinde https://pubs.aip.org/aip/adv/article/10/8/085014/990263/The-information-catastrophe adresinden alındı.

Waghorn, N. J. (2018). Gözetleyeni Gözetlemek: 'Protestocunun Panoptikonu' ve Dronelara Direnme. Ataman, B. ve Çoban, B. (Eds.). *Panoptikon 2.0: Alternatif Medya ve Karşı Gözetim,* içinde (s. 226-249). (T. E. Kalaycı, Çev.). İstanbul: Kafka Yayınları.

Wikipedia Sitesi. (2023). "Elon Musk". 24.06.2023 tarihinde https://tr.wikipedia.org/wiki/Elon_Musk adresinden alındı.

Wikipedia Sitesi. (2023)."SixDegrees.com" 05.08.2023 tarihinde https://en.wikipedia.org/wiki/SixDegrees.com#cite_note-4 adresinden alındı.

Wikipedia Sitesi. (2023). "Twitter Files". 24.06.2023 tarihinde https://en.wikipedia.org/wiki/Twitter_Files adresinden alındı.

Wikipedia Sitesi. (2023). "Twitter Diplomacy". 24.06.2023 tarihinde https://en.wikipedia.org/wiki/Twitter_diplomacy adresinden alındı.

Wikipedia Sitesi. (2023). "Youtube". 21.06.2023 tarihinde https://tr.wikipedia.org/wiki/YouTube adresinden alındı.

X News Daily. (2023, 11 Nisan). [@ X News Daily]. NEWS: Twitter is now X Corp. Twitter Inc. no longer exists. 29.07.2023 tarihinde https://twitter.com/xDaily/status/1645599226309517313?t=PS7EEh1LImPl8hnqsqEHmw&s=19 adresinden alındı.

X News Daily. (2023, 28 Temmuz). [@X News Daily]. NEWS: Twitter is officially dead. 29.07.2023 tarihinde https://twitter.com/xDaily/status/1685014025233379329?t=qq1fv-nos-Ug9jjUHmwcHQ&s=19 adresinden alındı.

Yantaç, C. ve Falcıoğlu, M. Ö. (2020). Yapay Zeka, İnsan ve Hukuk, *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, 6 (1) 1, 31-56. 25.04.2023 tarihinde https://www.jurix.com.tr/article/21657 adresinden alındı.

Yelken, R. (2003). Kamusal Alan Kim(ler)in Alanı?. *Sivil Toplum (Journal of Civil Society)*, 1(2), 45-51.

Yılmaz, D. ve Güney, R. (2021). Medyanın Çocuklar Üzerindeki Etkileri ve Kullanımına İlişkin Öneriler. *Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi*. 14 (4). 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/deuhfed/issue/65434/829839 adresinden alındı.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49 (1) , 95-118. 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/dtcfdergisi/issue/66779/1044266 adresinden alındı.

Youyou, W., Kosinski, M., ve Stillwell, D. (2015). Computer-Based Personality Judgments Are more Accurate Than Those Made By Humans. *Proceedings of the National Academy of Sciences*, 112(4), 1-5. 25.04.2023 tarihinde https://www.researchgate.net/publication/270910076_Computer-based_personality_judgments_are_more_accurate_than_those_made_by_humans adresinden alındı.

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo -Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, 58 (01). 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/ausbf/issue/3097/42868 adresinden alındı.

Yüksel, M. (2009). Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar. *Ankara Üniversitesi SBF Dergisi*, 64 (01). 25.04.2023 tarihinde https://dergipark.org.tr/tr/pub/ausbf/issue/3077/42647 adresinden alındı.

Zarrella, D. (2013). *The Social Media Marketing Book.* London: O'Reilly Media.

Zuboff, S. (2021). *Gözetleme Kapitalizmi Çağı: Gücün Yeni Sınırında İnsan Geleceği İçin Savaş.* (T. Uzunçelebi, Çev.). İstanbul: Okuyan Us Yayınları.

ÖZGEÇMİŞ

Damla Sabiha VAROL

Eğitim

Derece	Yıl	Üniversite, Enstitü, Anabilim Dalı
Lisans	2009	Sakarya Üniversitesi, Fen-Edebiyat Fakültesi, Felsefe Bölümü

İş/İstihdam

Yıl	Görev
2014	MEB Çalışanı / Felsefe Öğretmeni