YAPAY ZEKÂ ÇAĞINDA KİŞİSEL VERİ MAHREMİYETİ[1]

Personal Data Privacy in the Age of Artificial Intelligence

Hüseyin Ensari ERYILMAZ[2]

Öz

Yapay Zekâ (YZ), genel olarak, "Dar Yapay Zekâ", "Genel Yapay Zekâ" ve "Süper Zekâ" sınıflaması ile ele alınmaktadır. YZ, son yıllarda mantıktan etiğe, hukuktan ekonomiye, tıptan sanata ve estetiğe kadar aklımıza gelebilecek her alanda disiplinlerarası araştırmaların konusu olmaktadır. Kendi başına karar alabilen, veri toplayabilen YZ sistemleri günümüzde başta veri güvenliği olmak üzere pek çok etik ve hukuki problemin tartışma konusudur. YZ teknolojilerinin gelişimi büyük ölçüde toplanan kişisel verilere bağlıdır. Bu verilerin toplanma, depolanma ve işlenme yöntemleri her geçen gün daha önemli hale gelmektedir. Kişisel verilerin işlenmesi ile ilgili problemlerin azaltılabilmesi için ulusal ve uluslararası birçok yasal düzenleme gerçekleştirilmiştir. YZ sistemlerini geliştirme süreçlerinin bir denetimden yoksun oluşu, yapılan yasal düzenlemelerin her geçen gün yeni yetenekler kazanan sistemler karşısında yetersiz kalmasına neden olmaktadır. Makalemizde, YZ'nın mahremiyet kavramı ile olan ilişkisi, kişisel mahremiyet alanlarımıza dair oluşan ve oluşabilecek riskleri ve bu riskleri azaltmaya yönelik gerçekleştirilebilecek çözüm önerileri dile getirilmiştir. Araştırmamızda nitel araştırma yöntemi kullanılmıştır. Literatür taraması yapılmış, kavramlar betimsel analiz yöntemi ile ele alınmıştır. Çalışmamızın amacı, bu alanda çalışan bilim insanlarının son dönemde daha yüksek sesle ifade etmeye başladıkları YZ geliştirme süreçlerindeki riskleri belirtmek; kişisel mahremiyet içeren verilerin, bulut teknolojisinde bizden habersiz veya farkında olmadan verdiğimiz izinlerle toplanması ve depolanması; bu verilerin YZ'nın eğitiminde kullanılması durumunda ortaya çıkacak problemleri ve bu sorunları azaltmak için gerçekleştirilebilecek çözüm önerilerini tartışmaktır. Bu kapsamdaki son gelişmelere sosyal bilimcilerin dikkatini çekmek, bu alanla ilgili gelişmelerden haberdar etmek büyük önem arz etmektedir.

Anahtar kelimeler: Yapay Zekâ, Kişisel Veri, Panoptikon, Mahremiyet, Süper Zekâ

Abstract

Artificial Intelligence (AI) is generally classified into "Narrow AI", "General AI", and "Superintelligence". AI has become the subject of interdisciplinary research in various fields in recent years, ranging from logic to ethics, law to economics, medicine to art and aesthetics. AI systems capable of making independent decisions and collecting data are currently a topic of debate, particularly concerning issues such as data security as well as numerous ethical and legal concerns. The development of AI technologies is heavily reliant on the collection of personal data. The methods of collecting, storing and processing this data are becoming increasingly important day by day. To address issues related to the processing of personal data, numerous national and international legal regulations have been enacted. The lack of oversight in the development of AI systems leads to existing legal regulations becoming inadequate in the face of systems that continually gain new capabilities. In our article, we discuss the relationship between AI and the concept of privacy, highlighting both existing and potential risks to our personal privacy spaces and proposing potential solutions to mitigate these risks. We employed qualitative research methods in our study, conducted a literature review and analyzed concepts using descriptive analysis. The aim of our study is to draw attention to the risks that researchers in the field of AI are increasingly voicing regarding AI development processes, the collection and storage of personal data containing privacy elements without our knowledge or consent in cloud technologies, the potential problems arising from the use of this data in

[1] Bu makale, 3. Türkiye Sosyal Bilimler Sempozyumu Sempozyumu'nda sözlü olarak sunulan ancak tam metni yayımlanmayan "Yapay Zekâ Çağında Kişisel Veri Mahremiyeti" adlı tebliğin içeriği geliştirilerek ve kısmen değiştirilerek üretilmiş hâlidir.

[2] T.C. Milli Eğitim Bakanlığı İl Milli Eğitim Müdürlüğü, h-ensari@outlook.com, ORCID: 0009-0007-0744-7496.

AI training and the possible solutions to reduce these issues. Bringing the latest developments in this field to the attention of social scientists working in this area and keeping them informed about developments in this field is of paramount importance.

Key words: Artificial Intelligence, Personal Data, Panopticon, Privacy, Superintelligence

Giriş

Teknolojinin hızlanarak ilerlediği ve yaşantımıza farklı veçheleri ile müdahil olduğu günümüzde yapay zekâ (YZ) hayatımızın vaz geçilmez bir parçası haline gelmiş ve çağımız "yapay zekâ çağı" olarak tanımlanır olmuştur. YZ barındırdığı yüksek potansiyeli ile tarih boyunca görmediğimiz ve şu ana kadar tahayyül etmekte bile zorlandığımız birçok alanda köklü değişimleri gerçekleştirmektedir. Baş döndürücü bir hızla geliştirilen ve aynı hızla hayatımıza dahil olan YZ tabanlı teknolojiler bireylerin ve toplumların hayatında etkisini her geçen gün arttırmaktadır. Daha önce tecrübe etmediğimiz bu hızlı değişim süreçleri birçok fırsatı beraberinde getirdiği gibi pek çok problemi de hayatımızın merkezine taşımaktadır (Mazurek and Malagocka, 2019: 345). Günlük hayatımıza dâhil olan kişisel asistanlar, her anımızı kayıt altına alan sosyal medya uygulamaları, tercüme programları, navigasyon programları, verilerimizi bize sormadan kaydeden bulut teknolojileri ve yakın gelecekte hayatımıza dâhil olmayı bekleyen sürücüsüz araçlar, YZ hakimler, insan düzeyinde bir zekâya ulaşması beklenen YZ robotlar hayatımıza kattıkları yeni kavramlarla eski kavramlarımızı etkilemekte ve kavramlarımızı yeniden şekillendirmektedir. İletişim, sağlık, güvenlik, eğitim, sosyal yaşam ve ekonomi gibi pek çok alanda kullandığımız kavramlar ve bu kavramlara yüklenen anlamlar bu hızlı değişim süreçlerinden nasibini almakta ve bizleri kavramlarımızı tekrar ele almak ve üzerlerinde düşünmek zorunda bırakmaktadır.

YZ çağının getirdiği yeniliklerin insan hayatı üzerindeki etkileri yadsınamaz bir gerçekliktir. Tüketim toplumunun getirmiş olduğu hız ve haz çağı her şeyi çok hızlı bir şekilde tüketmektedir. Günümüzde özellikle insani hasletleri ihtiva eden kavramlarımız da bu tüketim çılgınlığından nasibini almaktadır. Soyut kavramların herkes tarafından aynı şekilde algılanmasını beklemek de gerçekçi değildir. Bu süreçte savrulmakta olan insanın makinalardan farkını koruyabilmek için insani hasletleri tekrar tekrar hatırlatmak gerekmektedir.

YZ'nın etkilediği teknolojiler daha rahat, güvenli, konforlu bir hayatı bizlere vadediyor olsalar da hali hazırdaki baş döndürücü hız gerek etik değerlerdeki aşınma gerekse hukuksal düzenlemelerdeki boşluklardan kaynaklı olarak karşılaşmak zorunda kalacağımız birçok etik ve hukuki problemlerle ilgili tartışmaları da beraberinde getirmektedir.

YZ'nın hayatımızda etkilediği ve aşındırdığı en önemli kavramlarımızdan biri de mahremiyet kavramıdır. Günümüzde mahremiyetle ilgili konuları internet, küresel teknoloji şirketleri, algoritmalar, YZ ve genel olarak veriyle ilgili olan tüm kavramlardan bağımsız düşünmek mümkün gözükmemektedir. Son yıllarda kişisel verileri kaydetme üzerine gelişen ekonomik faaliyetler, mahremiyet kavramı ile ilgili problemleri hem bireylerin hem de işletmelerin günlük yaşamlarında giderek daha önemli hale getirmiştir. Hızlı gelişen teknolojik ilerlemelerin bir sonucu olarak, özel bilgiler benzersiz bir ölçekte toplanmakta, depolanmakta ve işlenmektedir. Bu durum gizlilik ve şeffaflık konularında muhtemel problem alanları oluşturmaktadır (Dawoud, 2017: 2).

Gelişmiş veri keşfetme imkanlarının ortaya çıkmasıyla gizlilik, önemli bir sosyal konu haline gelmiştir. İnsanların rızası veya bilgisi olmadan kimliklerini tespit etme, profil oluşturma ve doğrudan etkileme her geçen gün kolaylaşmaktadır. Daha sofistike YZ sistemlerinin ortaya çıkmasıyla bu süreçler hızlanmakta ve bu durum gizlilik endişelerini de arttırmaktadır. Bu bağlamda, YZ, farklı kaynaklardan büyük miktarda veriyi toplama, analiz etme ve birleştirme yeteneğini artıran ilerlemiş makine öğrenme algoritmalarını kullanabilmektedir (Mazurek and Malagocka, 2019: 346). YZ'nın günümüzde yaygın kullanım alanlarından biri olan derin öğrenme algoritmaları yüz fotoğraflarına dayanarak bir bireyin cinsel yönelimini %91 doğrulukla sınıflandırabileceğini göstermiştir. Bu tür teknolojiler, gizlilikle doğrudan ilgili olarak, yönelimlerinin açıklanmasını istemeyen bir bireyin cinsel yönelimini ortaya çıkaran bir mekanizma sağlamaktadır (Curzon, 2021: 96). Ayrıca, yapay zekâ modellerinin eğitiminde kullanılan veriler ve bu verilerin toplanma şekilleri de günümüzdeki önemli tartışma konularıdır.

Yapay zekânın alt öğrenme alanlarından olan makine öğrenmesindeki son gelişmeler, artan miktarda veriye

erişimi olan derin öğrenme modellerinin kullanılması, insan benzeri makine zekâsına yaklaşıyor oluşumuz ve bunun sonucunda onun kontrolden çıkma ihtimali herkesi endişelendirmektedir. Kişisel verilere bağımlı YZ tabanlı sistemlerin, kişisel verilerimizin gizliliğini ihlal etme durumlarını ele almak; bu kapsamdaki son gelişmelere sosyal bilimcilerin dikkatini çekmek ve bu alanla ilgili gelişmelerden onları haberdar etmek büyük önem arz etmektedir. Yaptığımız incelemeler ve analizler sonucunda yeni yeterlilikler kazanan YZ'nın, etkilediği alanlarla ilgili çalışmaların interdisipliner bir bakış açısıyla ele alınması gerektiği, bu alandaki çalışmaların sadece mühendislere bırakılmasının yakın gelecekte pek çok problemi beraberinde getireceği düşünülmektedir. Bu nedenle, bu makalede, mahremiyet ve yapay zekâ konusunda bir değerlendirme sunulacak, YZ ile ilişkili bilinen gizlilik riskleri ifade edilecek, bu sistemlerin kontrolsüz kullanımında karşılaşılacak riskler tartışılacak ve ulaşabildiğimiz çözüm önerileri dile getirilecektir.

1. Yapay Zekâ

İnsanlar tarih boyunca oluşturmuş olduğu edebi ürünlerde ve sözlü anlatımlarında kendilerine benzer varlıklar hayal etmiş bunları edebi ürünlerde kayıt altına almışlardır. Ancak tarihin hiçbir döneminde değişim hızı günümüzdeki değişim hızıyla kıyaslanabilecek durumda değildir. YZ teknolojilerinin her geçen gün gelişmesi hayatımıza YZ şemsiye kavramının altında birçok yeni kavramı da katmakta ve daha önceki kavramlarımızda bazı değişimlere neden olmaktadır. YZ kavramı ilk olarak 1956 yazında Hanover, New Hampshire'daki Dartmouth College'da düzenlenen ve sonradan "Yapay Zekâ Üzerine Yaz Araştırma Projesi" olarak isimlendirilen programda John McCarthy tarafından kullanılmıştır. Düzenlenen bu program YZ çalışmalarının günümüze ulaşmasındaki en temel taşlardan biri olmuştur. Her biri kendi alanında uzman on bilim insanının katıldığı bu çalışma programının amacı, "Öğrenmeyi ve zekâyı net bir şekilde tanımlayarak bu sayede makinelere bunu aktarma; dil kullanabilen, soyutlama yapabilen, kavram oluşturabilen, insanlar gibi problem çözebilen ve kendilerini geliştirebilen makinelerin nasıl geliştirilebileceğine dair bir girişim." olarak tanımlanmıştır. Bir araya gelen on bilim adamı iki aylık süreçte bu alanlarda ilerleme kaydetmeyi düşünmüştür (McCarthy vd., 2006: 13).

YZ, özellikle akıllı bilgisayar programları yapma bilimi ve mühendisliğidir. İnsan zekâsını anlamak için bilgisayarları kullanan YZ, biyolojik olarak gözlemlenebilir yöntemlerle sınırlı kalmak zorunda değildir (URL-1). YZ üretebilmek için insanların yapabildiği en üstün zihinsel etkinlikler olduğu düşünülen dama, satranç ve go gibi oyunlar oynayabilen YZ'lar tasarlanmaya çalışılmıştır. Yapılan çalışmalarda insan gibi düşünen, insan düşüncesini taklit eden ve insan zekâsına benzer kararlar alan YZ'ları oluşturmak amaçlanmıştır. Oluşturulan yapılarda mantıklı düşünme ve bu düşünmeyi sağlayarak doğru sonuçlara ulaşmak hedeflenmiştir (Nilsson, 2009: 75).

YZ insan davranışlarının eşdeğerlerini yapay sinir ağları ile gerçekleştirmeye çalışan bir teknolojinin adıdır. YZ mantık, akıl yürütme, problem çözme ve yaratıcılık gibi tüm yeteneklerin bir program tarafından gerçekleştirilmesiyle oluşur. Mantık, olasılık ve istatistik gibi matematiksel unsurlar, yukarıda bahsedilen yeteneklere ulaşmak için kullanılırken, algılama, yorumlama ve öğrenme gibi bilişsel disiplinlerden de faydalanılır. YZ'da temel hedef insanın düşünme sistematiğinin taklit edilerek sentetik ve kusurlardan arındırılmış güçlü bir yapay zekâ oluşturmaktır (Coşkun ve Kuşçu, 2021: 116-129). Oluşturulacak YZ'nın insan zekâsına özgü olan algılama, öğrenme, kavram oluşturabilme, kavramlar arası bağ kurabilme, sorgulayarak çıkarsama yapabilme ve sonunda doğru kararlar verebilme gibi özellikleri yerine getirmesi beklenmekte, bu noktaya ulaşmak için özellikle son on yılda hummalı bir çalışma gerçekleştirilmektedir (Büyükuslu, 2021: 57-60). Günümüzde YZ öncelikle yazılım ve bilgisayar mühendislerinin ilgilendiği bir alan olarak görülse de artık mühendislerin, matematikçilerin, felsefecilerin, doktorların, sosyolog ve psikologların en önemlisi politikacıların sürece katılmak durumunda oldukları çok disiplinli bir araştırma alanı haline gelmiştir (Kutlusoy, 2019: 26).

YZ'yı ve günümüze etkisini daha iyi anlamak için kısaca tarihsel gelişiminden ve kavramlarından bahsetmenin gerekli olduğunu düşünüyoruz. YZ kavramı bir çatı kavram olarak kullanılsa da son elli yılda meydana gelen gelişmelerle sürekli olarak yeni alt kavramlar üretilmiş ve hâlâ da üretilmeye devam

etmektedir. Yapay sinir ağları, uzman sistemler, evrimsel algoritmalar, makine öğrenmesi, derin öğrenme, dar yapay zekâ, genel yapay zekâ, süper zekâ bu alanda kullanılan en yaygın kavramlardan bazılarıdır. Yapay zekâ ve etkileri ile ilgili yapılan tartışmalarda bu kavramların içeriklerinin, dolayısıyla etki potansiyellerinin tam olarak kavranamaması tartışmaların sağlıksız olmasına neden olmaktadır.

1.1. Yapay Zekâ Tarihine Genel Bir Bakış

YZ tarihi farklı dönemlerden başlatılabilmektedir. Kimi bilim insanları bunu tarihsel metinlerde kurulan düşlere kadar dayandırmaktadır. Makineye zekâ kazandırma çalışmalarının en önemlisi İngiliz matematikçi Alan Turing (1912-1954) tarafından gerçekleştirilmiştir. Bu alanda ilk dikkat çeken makalesi *"On computable numbers, with an application to the Entscheidungsproblem"* 1936 yılında yayımlanmıştır. Bu makalede otomatik makine olarak geçen ve daha sonraları Turing Makinesi olarak da ünlenecek olan basit bir varsayımsal cihaz tanımlanmıştır. Turing makinesi, problemin bir algoritma olarak ortaya konulabildiği durumlarda akla gelebilecek herhangi bir matematiksel hesaplamayı yapabilen evrensel bir bilgi işlem makinesidir (1936: 135). Ancak onun esas tanınmasını sağlayan çalışması, 1950 yılında Mind isimli felsefe dergisinde yayımlanan *"Computing Machinery and Intelligence"* isimli makalesi olur. Turing bu metinde "Evrensel Makine" olarak işlev gören bilgisayarlara temel teşkil edecek bir makineden bahsetmiştir. Bu makaleye "Makineler düşünebilir mi?" sorusuyla başlayan Turing, makalede, "Imitation Game" olarak bilinen bir taklit oyununu ortaya koyar. Onun ortaya koyduğu bu düşünsel deney günümüze kadar etkisini devam ettirmiştir (Topal, 2017: 1345-1348).

Turing'in makalede ifade ettiği "Imitation Game" taklit oyunu daha çok "Turing Testi" olarak makinelerin zekiliğinin bir ölçütü olarak kullanılmaktadır. Turing bu oyunda bir kadın, bir erkek bir de sorgucu olduğunu düşünmemizi ister. Soru soran kişi karşıdaki kişilerin cinsiyetlerini bilmemekte ve sorduğu sorulara aldığı cevaplardan hareketle karşısındakilerin cinsiyetlerini doğru bir şekilde tahmin etmeye çalışmaktadır. Ancak oyunu ilginç kılan nokta oyundaki kadın ve erkeğin sorulara cinsiyetlerinin doğru tahmin edilmemesi için sorgucuyu yanıltıcı cevaplar vermeleridir. Turing kurguladığı bu oyunda kadın ve erkek yerine makine ile bir insanın varlığını düşünmemizi ister. Bu oyunda makinenin bir zekâya sahip olup olamayacağını çeşitli başlıklarda tartışır. Ona göre makine kendisinin bir insan olduğuna sorgulayıcıyı ikna edebilirse insan düzeyinde bir zekâya ulaşmış olacaktır (Turing, 1950).

Turing'in kavramsal çerçevesini çizdiği bu evrensel makine tasarımını gerçekleştirmek için çeşitli modeller denenir. Etkili olacağı düşünülen modellemelerden biri de yapay sinir ağlarıdır. Waren S. McCulloch ve Walter H. Pitts bu alanda 1943 yılında *"A Logical Calculus of Ideas Immanent in Nervous Activity"* isimli bir makale yayımlamış ve bu makalede oluşturulacak bir yapay sinir ağının matematiksel modellemelerini tanımlamışlardır. Onların bu çalışmaları üzerine Mervin Minsky bir sinir ağı makinesi geliştirmiş, üç bin adet vakum tüple kırk nöronlu bir sinir hücresini simüle etmeyi başarmıştır (Sönmez, 2020: 5). 1958 yılına gelindiğinde McCharty üst seviye bir programlama dili olan LISP'i programlamıştır. Böylece kendi kendini değiştirebilen yazılımlar süreci başlamıştır. 1963 yılına gelindiğinde ise Standford Ünivesitesi'nde yine McCharty tarafından ilk yapay zekâ laboratuvarı oluşturulmuştur. 1976 yılında bulaşıcı hastalıkların teşhisi için ilk uzman sistem olan MYCIN kullanılmaya başlanmıştır. Dönem dönem YZ'dan beklentiler artmış ancak beklentilerin gerçekleşmediği dönemlerde derin hayal kırıklıkları oluşmuş ve çalışmalar neredeyse durma noktasına gelmiştir. Bu dönemlere "yapay zekâ kışı" denilmiştir. Ancak her seferinde yeni bir atılım imkânı bulunarak tekrar çalışmalar canlanmıştır. Belki de tarihin dönüm noktalarından biri olarak 1997 yılında Japonya'da düzenlenen uluslararası RoboCup yarışmasında IBM'in satranç bilgisayarı Deep Blue'nun dünya satranç şampiyonu Kasparov'u yenmesi görülebilir. YZ tabanlı bir programın bir insanı yenmiş olması tekrar dikkatlerin YZ'ya çevrilmesine neden olmuştur. O zamana kadar insanların en üstün zihinsel beceri olarak gördükleri satrançta bir program insanı yenmiştir. Satranç oynayabilen bir makinenin her şeyi yapabileceği düşüncesinin gerçekleşmemiş olması derin bir hayal kırıklığı oluşturmuştur. Elimizde artık çok iyi satranç oynayabilen ancak başka hiçbir şey yapamayan bir program bulunmaktadır (Bostrom, 2020: 27-29). 2009 yılına gelindiğinde Google sürücüsüz araçlarını test etmeye başlamıştır. 2011 yılında IBM'in üretmiş olduğu Watson isimli bir program bilgi yarışmasında insanlara karşı kazanmıştır. 2016

yılında yapılamaz olduğu düşünülen çok fazla olasılık içeren Go oyununda Google'ın üretmiş olduğu Alpha Go dünya şampiyonu Lee Sedol'u ezici bir şekilde yenmiştir. Yine aynı yıl Microsoft Twitter'da "Tay" isminde bir sanal chatbotu kullanıma açmış ancak insanlar tarafından manipüle edilerek yanlış şeyler öğrendiği için kısa zamanda kaldırılmak zorunda kalmıştır (URL-2). YZ tabanlı programların en son halkası 2018 yılında Microsoft'un bir alt şirketi Open AI tarafından kullanıma sunulan ChatGPT olmuştur. Kısaca bahsetmeye çalıştığımız yapay zekâ gelişim süreçlerinde bazı temel kavramlar bulunmaktadır. YZ kışlarının tekrar bahara dönmesine neden olan bu yapay zekâ alt kavramlarını kısaca tanımlamak tartışmaların daha sağlıklı yapılmasına katkı sağlayacaktır.

1.2. Yapay Sinir Ağları

İnsan beynindeki faaliyetlerin tamamı sinir hücreleri ile gerçekleştirilmektedir. İnsan beyninde gerçekleşen olayların, tersine mühendislik yoluyla gelişen tıbbi görüntüleme aletleri sayesinde detayları tam olarak bilinmese de, genel bir şema olarak işleyişi bilinmektedir. Bir sinirsel ağ, kabaca bir davranışı ortaya koyan yapıyı belirtmektedir. YZ araştırmacıları bu mekanizmayı model alarak güncel problemlere çözümler üretmeyi başarmışlardır. Sinirsel ağlar biyolojik olarak bizde öğrenmeyi sağladıkları gibi benzeri bir modeli kullanarak oluşturulan yapay sinir ağları da YZ'yı oluşturmuş ve makine öğrenmesi yoluyla YZ alt alanlarından biri haline gelmiştir. Yapay sinir ağları, gerçek sinir ağlarında gerçekleşen elektrokimyasal işlemlerin yerine düğüm noktalarında olayların gerçekleşme olasılıklarına rakamlar atayıp bu rakamlara uygulanan çeşitli öğrenme fonksiyonları ile başarıya ulaşmayı hedeflemektedir. Makine öğrenmesi ve derin öğrenme algoritmalarının geliştirilmeleri bu yapay sinir ağlarının geliştirilmesi ile olmuştur. Özellikle 1990'lı yıllarda gerçekleşen birçok yeniliğin arka planında yapay sinir ağları ile gelişen makine öğrenmesi ve onun daha gelişmiş hali olarak ifade edebileceğimiz derin öğrenme algoritmaları bulunmaktadır (Tegmark, 2019: 99-105). Makine öğrenmesi, belirli bir sonuç elde etmek için açıkça programlanmayan veriden hareketle kendi kendine öğrenebilen yapay sinir ağları ile oluşturulmuş algoritmaları ifade eder. Görüntülerdeki nesnelerin algılanmasından doğal dillerin anlaşılmasına kadar birçok alanda kullanılmaktadır. Özellikle YZ'ya dikkatlerin çekilmesini sağlayan sanal oyuncuların programlanması makine öğrenimi sayesinde olmuştur (Yılmaz ve İyigün, 2020: 11). YZ'nın günümüzdeki en yaygın kullanım alanı olarak karşımıza "Derin Öğrenme" çıkmaktadır. Makine öğrenmesinin gelişmiş bir halini ifade eden bu alan, makine öğrenmesine göre çok daha fazla veriyle işlem yapabilmektedir. Makine öğrenmesi algoritmaları daha çok kısıtlı verilerle çalışan, bir bilgisayarın sahip olabileceği verileri işler, onlardan sonuçlar üretirken derin öğrenme algoritmaları sahip oldukları katmanlı sinir ağı mimarileri ile çok daha büyük verilerle çalışma imkanına sahiptirler. Kavramdaki "derin" sözcüğü katmanlı sinir ağlarının sayısındaki artışı ifade etmek için kullanılmaktadır. Problem ne kadar karmaşıksa oluşturulacak yapay sinir ağı modelinde o kadar çok katman kullanılabilmektedir (Yılmaz, 2020: 101).

1.3 Dar Yapay Zekâ

YZ ile ilgili genellikle dar yapay zekâ, genel yapay zekâ ve süper zekâ olmak üzere üçlü sınıflama yapılır. Bu sınıflamalar YZ'nın insan zekâsı ile ilgili yapılan kıyasına göre belirlenmektedir. Dar Yapay Zekâ, belirli bir alanda eğitilen ve geliştirilen YZ uygulamaları için kullanılmaktadır. Günümüzdeki popüler olan birçok YZ tabanlı program bu YZ sınıfının altında tanımlanmaktadır. Yarışmalarda insanları yenen, hastalık teşhis edebilen, belirli alanlarda tanımlı görevleri yerine getirebilen tüm yazılımlar için genellikle "dar yapay zekâ" tanımlaması yapılmaktadır (Demir, 2019: 60). Bilgisayar mühendisi Donald Knuth, *"Yapay zekâ bu zamana kadar özünde düşünmeyi gerektiren her şeyi başarmış ama insanların ve hayvanların düşünmeden yaptıkları birçok şeyi başaramamıştır; nasıl olduysa olmuş, zoru başarmıştır."* der. Knuth'un ifadesinden hareketle baktığımızda görsel sahneleri analiz etmekten doğal dillerin çevrilmesine, üstün zihinsel beceri gerektiren satranç, go gibi oyunlarda insanlara üstün gelmesinden, insanların hesaplamakta aciz kaldıkları devasa verileri depolama, işleme ve veriler arası bağlantı kurup sonuç çıkarabilme özelliklerine kadar tekil alanlarda çok büyük başarılar elde eden yapay zekâ tabanlı programlar insan beyninde gerçekleşen her probleme çözüm üretebilme kapasitesine ulaşamamıştır (Bostrom, 2020: 30-35).

1.4 Genel Yapay Zekâ

Öncelikle şunu ifade etmek gerekir ki ulaştığımız teknoloji ve ürettiğimiz YZ programları dikkate alındığında bir genel yapay zekâya ulaşmış değiliz. Ancak alanın uzmanlarına göre genel yapay zekâya ulaşmak artık sadece zaman meselesidir. Genel yapay zekânın yapılabileceğine inanan bilim insanları beynin bir örüntü içinde hareket ettiğini, o örüntü çözümlenebildiğinde ve teknik yeterlilikler de sağlandığında bunun gerçekleşmesinin önünde bir engel kalmayacağı düşüncesindedirler. Stephan Hawking, *"Biyolojik bir beynin başarabildikleri ile bir bilgisayarın başarabildikleri arasında derin bir farklılık olmadığına inanıyorum. Dolayısıyla buna göre bilgisayarlar teoride insan zekâsıyla yarışabilir ve onu geçebilir."* diyerek mevcut gelişmeler ışığında genel yapay zekâ ile ilgili bir gelecek perspektifi sunmuştur. Ancak göz ardı edilmemesi gereken bir husus da şudur: Bilim insanlarının YZ ile ilgili öngörüleri genellikle, insanı ne olarak tanımladıkları ve onu nasıl konumlandırdıklarına dair dünya görüşlerine göre şekillenmektedir. Genel yapay zekânın dar yapay zekâdan farkı sosyal ve duygusal zekâya sahip olması, geçmiş ve geleceği düşünme becerilerini yerine getirebilmesi aynı zamanda yaratıcılık ve özgünlük gibi insanların sahip olduğu türden çeşitli özellikleri bünyesinde barındırabilmesidir. İnsan deneyimlerinin bütün alanlarını kapsayan ve dolayısıyla en az bir insan kadar yeterliliğe sahip birçok dar yapay zekânın birleşimi olarak düşünebileceğimiz bir zekâ türü olan bir genel yapay zekâ tasavvur edilmektedir. Bilgisayarların hayatımıza dahil olmasından bu yana özellikle son elli yıllık serüvenimiz göz önüne alındığında bilgisayarlar için asla yapılamaz diye düşünülenler listesine dahil olan her ne varsa bu listedekilerin her geçen gün bir bir eksildikleri gözükmektedir (Reese, 2018: 193-201). Genel yapay zekânın yapılabilirliği hususuna bu açıdan imkansız demek çok da mümkün gözükmemektedir. Peki bir genel yapay zekâ ne zaman gerçekleştirilebilecektir? Yapılan bir ankette YZ uzmanları 2028'den önce bunun üretilme olasılığını %10, 2050'den önce üretilme olasılığını %50, yüzyılın sonunda ise %90 olarak tahmin etmektedirler (Barrat, 2020: 35).

1.5. Süper Zekâ

Süper zekâ, YZ gelişiminin son evresi olacağı düşünülen dönemi ifade eden bir kavramdır. Bu kavram, insan zekâsını aşan keşif yeteneklerine haiz ayrı bir fenomenin varlığını ifade eder. İnsan düzeyinde bir YZ'ya sahip makinelerin hayali 1940'lardan itibaren gerçekleştirilen gerek bilgisayarla ilgili gerekse yazılım ile ilgili çalışmalarda bir itici güç olarak hep var olmuştur. O dönemlerde yirmi otuz yıl içinde böyle bir icadın gerçekleşeceğine dair iyimserlik, beklenen tarihlerde istenen ilerlemeler gerçekleşmediğinden zaman zaman hayal kırıklıklarını da beraberinde getirmiştir. Günümüzde birçok bilim insanı benzeri bir hayal kırıklığının yaşanmaması için gelecekle ilgili öngörülerinde, teknolojik gelişmelerin hızı eskisine göre artmış olsa da, biraz daha temkinli olmaktadırlar. İlerlemelerin beklenenden daha yavaş gerçekleşmesinin esas nedeni, teknik zorlukların sanıldığından daha büyük olmasındandır. Bazı aşırı zor görünen problemler çok basit şekilde çözümlenebilirken, basit görünen problemlerin çözümü ise tam tersine mümkün olmayabilmektedir.

Süper Zekâyı tanımlarken Matematikçi I. J. Good çokça alıntılanan bir ifadesinde şöyle der:

"Bir aşırı zeki makineyi, ne kadar akıllı olursa olsun her insanın entelektüel faaliyetlerini misliyle aşabilecek bir makine olarak tanımlayalım. Makinelerin tasarımı bu entelektüel faaliyetlerin bir tasarımı olduğundan, bir aşırı zeki makine daha da iyi makineler tasarlayabilir; bir "zekâ patlaması" yaşanacağına şüphe yok ve insanın zekâsı da çok geride kalacaktır. Dolayısıyla ilk süper zekâ makine insanın yaratma gereksinimi duyacağı son icat olacaktır, yeter ki makine bize onu nasıl kontrol altında tutacağımızı söyleyecek kadar yumuşak başlı olsun." (Barrat, 2020:27)

Bu tür bir zekâ patlaması temelde varoluşsal riskler barındırmaktadır. Dolayısıyla böyle bir teknolojiye ulaşma ihtimali günümüz için çok düşük bir olasılık olarak gözükse de bu konuların üzerinde ciddiyetle durulması gerekmektedir. Günümüzde YZ teknolojileri ile ilgili çalışmalar yapan Stephan Hawking, Elon Musk ve Bill Gates gibi isimler böyle bir teknoloji seviyesine ulaşmanın risklerini belirtmişlerdir. Özellikle

son bir iki yıldır başta Elon Musk ve Bill Gates olmak üzere bu alanda çalışanlar uyarılarını daha yüksek sesle dile getirmekte, riskleri minimize etmek için gerekli yasal ve etik düzenlemelerin gerçekleştirilmesi, kuralların sıkılaşması gerektiğini ifade etmektedirler.

Oxford Üniversitesi'nden ahlak bilimci Nick Bostrom, "Süper zekâ konusunda anlamlı bir tartışma yapabilmenin önkoşulu, süper zekânın insanların kapasitesini adım adım arttıracak yeni bir teknoloji, yeni bir araç olmaktan ibaret olmadığını kavramaktan geçer." demektedir. Ona göre süper zekânın tamamıyla farklı bir şey olacağını idrak etmek gerekir. Bu gerçekleştiğinde artık hiçbir şeyin kontrolü insanda kalmayacak, kendi kendine kararlar alabilen ve uygulayan ayrı bir varlığın neler yapabileceğini kestirmek ve onunla mücadeleye girmek zorunda kalmak en son isteyeceğimiz şey olacaktır (Barrat, 2020: 27).

2. Mahremiyet

Mahremiyet kavramı TDK Sözlük'te, "Gizlilik" olarak tanımlanmaktadır. Kavram Arapça'da "haram" kökünden gelen, bir şeyin gizli olması, başkalarına yasaklı olması hali anlamında kullanılmıştır (Çakır, 2022: 208).

Bu kavram ilk kez, Tevrat'ın Yaratılış bölümünde anlatılan Âdem ile Havva'nın cennetten yeryüzüne indirilmesi hikâyesinde karşımıza çıkar. Oradaki anlatının benzerlerine çeşitli kutsal metinlerde de rastlanmaktadır. İlgili bölümde, Tanrı, Âdem'den bir ağaca yaklaşmamasını ve onun meyvesinden yememesini ister. Eğer o meyveden yerlerse öleceklerini ifade eder. Ancak bir Yılan onlara bu meyveden yerlerse gözlerinin açılacağını, Tanrı gibi olacaklarını söyleyerek onları meyveyi yemeğe ikna eder. Havva meyveyi koparıp yer ve Âdem'e de verir. O da meyveden yediğinde ikisinin de gözleri açılır ve birbirlerini çıplak olarak görürler. Birbirlerinin mahremine dair ulaştıkları bu bilgi ve bilinç düzeyi onları tekrar gizlenmeye iter. Yemiş yapraklarından kendilerini gizleyecek örtü yaparlar (Eski Ahit, Yaratılış, 4). Eski Ahit'teki bu anlatıda meyvenin yasaklanmasının gerekçesi her şeyin kendilerine aşikâr olacağı, ancak insanlar için mahremiyetin önemli olduğu şeklindedir. Her şeyin bilgisine sahip olanın sadece Tanrı olması gerektiği ifade edilmektedir. Gizlilik sadece insana mahsus bir özelliktir. Mahremiyetin ortadan kalkması insanın fıtratında var olan utanma duygusunu harekete geçirmekte ve insana rahatsızlık vermektedir. Her şeyin görünür olması şeklinde düşünebilecek olan bir çıplaklık, başkasının gözünde görünür olma hali, insan için tedirgin edici bir durumdur (Gündoğan, 2019: 36).

Mahremiyet, insan olmanın temel unsurlarından biridir. Mahremiyetle ilgili yasal haklar 2000 yıl önce, Yahudi hukukuna kadar dayandırılabilmektedir. Talmud'da, bir kişinin komşusunun evini gözetlememesi ve içine bakmaması gerektiği ifade edilmektedir. Yine Kur'an-ı Kerim'de:
"Ey iman edenler! Kendinizi tanıtıp izin almadan ve içinde oturanlara selam vermeden kendi evlerinizden başka evlere girmeyin. Sizin için daha iyi olanı budur; umulur ki düşünüp anlarsınız. Eğer o evlerde bir kimse bulamazsanız -size izin verilmedikçe- oralara girmeyin. Size "(Kabul edemiyoruz,) dönün" denirse hemen dönün; bu sizin için daha nezih bir davranıştır. Allah bütün yaptıklarınızı bilmektedir. İçinde kimsenin oturmadığı ve kendinize ait eşya bulunan evlere girmenizde sizin için bir sakınca yoktur. Allah açıkladığınızı da bilir, gizlediğinizi de!" (Nur Suresi, 24/27-29) buyrulmaktadır.

Mahremiyet kavramının anlam dünyası her ne kadar bireyin yaşadığı kültür dünyasına göre şekilleniyor olsa da kavramın içerdiği alanın belirlenmesinde birçok faktör etkilidir. Ancak bu kavramın içeriğinin belirlenmesindeki en önemli unsurlardan birinin dini inançlar ve algılar olduğu akılda tutulmalıdır. Bu açıdan bakıldığında mahrem kavramında kastedilen özel durumlar, sadece bireyin kendisi ile ilgili değildir (Kütükoğlu, 2021: 18).

Mahremiyet (privacy), tarih boyunca çeşitli toplumlarda ve kültürlerde farklı bağlamlarda kullanılmış bir kavramdır. Eski Roma'da kamu görevinden uzak kalmak olarak kullanılan "privatus" sözcüğü, mahrumiyet kavramına karşılık gelmektedir. Özel (private) kelimesi ise, genele ait olmayan, belirli bir şahsa, gruba veya sınıfa ait olan anlamında kullanılmıştır. Günümüzde bu kavram "özel", "yalnız bireyi ilgilendiren"

anlamında kullanılmaktadır. Bu kavram kişi açısından bir mahremiyet oluşturduğu gibi başkaları açısından da o hususta bir mahrumiyet oluşturmaktadır (İzgi, 2009: 60-61).

Genel olarak mahremiyet, kişilerin kendi kararlarını özgürce verebildikleri, başkaları ile herhangi bir yer ve zamanda diledikleri şekilde iletişim kurma ya da kurmama haklarını da içeren bir kavramdır (Koles-Kemp ve Kani-Zabihi, 2010: 97). Toplumsal yaşamın içinde mahremiyet farklı şekilleri ile karşımıza çıkabilmektedir. Kişilerin herhangi bir şekilde bilinmeden kamuya katılma hakları da mahremiyet kavramı içerisinde ele alınabilmektedir.

Mahremiyet konusu tarih boyunca önemli bir kavram olarak insanların hayatında var olsa da modernleşme süreçlerinde daha fazla dikkat çeken bir kavram haline gelmiştir. Geleneksel toplumlarda birey olgusunun zayıf olması mahremiyet kavramının da çok belirgin olmamasına neden olmuştur. Modern dönemde birey kavramı öne çıkmış, insanlar kalabalıklar içinde bireysel yaşam alanlarına geçiş sürecini yaşamışlardır. Bu dönemde bireyin başlı başına bir değer olarak belirmesi, toplum yaşantısında mahremiyet algısını belirginleştirmiş ve süreç içerisinde bireysel haklar kapsamına alınarak yasal düzenlemelerin konusu haline gelmiştir (Yüksel, 2003: 184-185).

Kişiler için mahremiyet hep aynı anlama gelmeyebilir. Mahremiyet duygusunun yoğunluğu da kişiden kişiye içinde bulunulan zamana, ortama ve duruma göre değişiklik gösterebilmektedir. Bazılarında mahremiyet duygusu daha baskın olurken bazılarında bu duygu baskın değildir. Aynı zamanda kişiler farklı türden mahremiyete ihtiyaç duyabilmektedirler (Odabaşı, 2019: 26). Özel bir oda, birçok kişinin kaldığı bir odaya kıyasla daha fazla mahremiyet duygusu oluşturur. Camdan yapılmış, her taraftan görünebilen bir evde oturan, başkalarını gören veya onlar tarafından görülen bir kimsenin mahremiyet duygusunun yoğunluğu, başkalarını görmeyen veya onlar tarafından görülmeyen bir ortamdaki kişiye göre daha az olabilecektir. Ayrıca mahremiyet türleri de bu duyguyu etkileyebilmektedir. Kişiler dışarda görülmekten rahatsız olmasalar da konuşmalarının başkaları tarafından dinlenilmesinden rahatsız olurlar. Mahremiyete yönelik tutum ve davranışları aynı zamanda kişilerin sosyal statüleri, yaşları, cinsiyetleri, yetiştikleri kültür çevreleri, inançları gibi pek çok özellik etkileyebilmektedir.

Mahremiyet aynı zamanda, özerklik hakkıdır ve başımızın çaresine bakma hakkını da içerir. Mahremiyet, kendi hakkımızdaki bilgileri kontrol etme ve o bilgilere erişimi sınırlama hakkını ifade eder. Bu hak, gizli tutulması gereken sırları gizli tutma ve bunları özel konuşmalarda paylaşma hakkını da kapsar.

Mahremiyet kavramını, yalnızca saklanacak bir şeyle ilgili de düşünmemek gerekir. Bireyin memnuniyetini artırmak için bir gereklilik de söz konusudur. Kişinin kendini gerçekleştirmesi ve bir birey olarak var olabilmesi için bu özerkliği kazanması gereklidir. Günümüzdeki anlamıyla mahremiyet kavramının daha çok modernleşme ile birlikte alan genişlemesine uğradığını söylemek mümkündür. Geleneksel toplumlarda hem fiziki şartlar gereği hem de kültürel alışkanlıklardan kaynaklı olarak bireyler açısından bugünkü kadar geniş bir mahremiyet alanından bahsetmek çok da mümkün gözükmemektedir. Birey daha çok yaşadığı toplumun bir üyesi olarak görüldüğü için bireysel sınırlarının belirginleşmesi ancak modern dönemde gerçekleşmiştir. Modernleşme dönemiyle birlikte toplumsal hayatta giderek ağırlığını arttıran mahremiyet olgusu, zamanla hukukun konusu haline gelmiş ve hak kapsamına alınarak pek çok düzenlemenin konusu olmuştur. Ancak günümüzde, mahremiyet hakkının birçok tehditle karşı karşıya olduğu düşüncesine dair görüşler yaygınlaşmaktadır (Yüksel, 2003: 184).

Adam Carlyle Breckenridge, 1970 yılında yazmış olduğu Mahremiyet Hakkı isimli eserinde o zamanki durumu şöyle ifade etmektedir:
"Hızlı bir şekilde mahremiyetin olmadığı bir çağa giriyoruz. Herkes, her zaman gözetime açıktır. Hükümetten saklanabilecek hiçbir sır kalmamıştır. Hükümet tarafından mahremiyete yönelik aşırı ihlaller, geometrik diziyle artmaktadır. Herhangi bir etkin yasal ve yargısal denetim olmaksızın, telefon dinleme ve gizli kayıt faaliyetleri önlenemez yaygın bir hal almaktadır. Hükümet birimlerindeki gizli gözetleme birimlerinden endüstri alanındaki kapalı devre televizyon devrelerine ve dinlenme odalarına kadar uzanan

gizli gözetleme, ortak bir karakter taşımaktadır. Hükümetin selameti bakımından bürolar, konferans salonları, otel odaları ve hatta yatak odaları bile gizli olarak dinlenmektedir." (1970: 7-8).

Breckendridge, her ne kadar konuyu o yıllarda devletin birey üzerindeki kontrolü açısından ele almış olsa da günümüzde özel yaşam alanına veya mahremiyete yönelik tehditler ve müdahaleler, sadece devlet ya da onun gücünü elinde tutan hükümetlerden değil, iletişim yöntemlerinin ve teknolojinin gelişmesi ile özel kişi ve kuruluşlardan da kaynaklanabilmektedir. Yapay zekâ çağı olarak tanımlanan yaşadığımız süreçler iletişim teknolojilerinde meydana gelen devasa gelişmeler sayesinde bireylerin özel yaşam alanlarına başkaları tarafından sızılabilmesini oldukça kolaylaştırmıştır. Böyle bir ortamda bireyler, görüşmelerinin ifşa edilmeyeceğinden, elektronik posta iletilerinin başkasının eline geçmeyeceğinden, özel hayatına dair telefonunda ya da bilgisayarında sakladığı bilgi ve fotoğrafların çalınmayacağından, sağlığı ile ilgili verilerin mahremiyetinin korunabileceğinden, mali durumunun ve ekonomik faaliyetlerinin başka kişi ve kuruluşlara pazarlanmayacağından emin olamamaktadırlar. Yapay zekâ çağında mahremiyet alanının daha fazla işgaline dair şikayetler her geçen gün artmakta ve bu konuda yeni etik ve hukuki düzenlemelerin yapılması zaruri hale gelmektedir.

İki yüz yıl önce, özel konular hakkında herhangi bir yakınınızla konuşmak isteseniz bunu yüz yüze yapmanız gerekirdi. Sizi dinlemek isteyen biri olursa yakından takip etmek zorunda kalır ve muhtemelen fark edilirdi. Günümüzde uzak mesafelerle konuşmayı mümkün kılan iletişim araçları, konuşmalardaki mahremiyeti yok etme potansiyeline sahiptir. Mağazalara ve binalara girişlerimizi kaydeden güvenlik kameralarından, kredi kartları ile yaptığımız harcamaların içeriklerine kadar her faaliyetimizin kaydedilmesi ve bu kayıtların başkaları tarafından ulaşılabilir olması mahremiyet ihlali endişesini günümüz dünyasının ana konularından biri haline getirmiştir. Ne yaptığımız, kimlerle ilişki içinde olduğumuz, sosyal medyada hangi görüş ve düşünceleri beğendiğimiz, nereye gittiğimizle ilgili veriler düzenli olarak kaydedilmektedir. Medeni durumumuz, kaç çocuğumuz olduğu, hangi sıklıkla hastaneye gittiğimiz, sağlık durumumuz, harcamalarımız ve daha birçok bilgi başkaları tarafından erişebilir durumdadır. Bizlerle ilgili bilgiler artık kontrolümüz altında değildir; böyle bir kontrol kaybı aynı zamanda bir mahremiyet kaybıdır (Diffie ve Landau, 1998: 125-130).

Geçmişte ağırlıklı olarak eleştiriler hükümetlerin bireylerin hayatları üzerindeki müdahalelerine dikkat çekmiş olsa da günümüzde kişilerin mahremiyetlerini ihlal eden durumlar sadece devlet birey ilişkisi açısından değil özel kişi ve kurumlardan da kaynaklanabilmektedir (Barkuş ve Koç, 2019: 35-37). Günümüzdeki internet kullanımı ile oluşan verilerimiz, sosyal medya uygulamaları üzerinden yapmakta olduğumuz paylaşımlar, kullandığımız cep telefonlarındaki işletim sistemlerinin her anımıza dair topladıkları veriler büyük şirketlerin oluşturmuş olduğu veri bankalarında toplanmaktadır. Bu verilerin başka kurum, kişi veya şirketlere pazarlanmayacağından, bir gün paylaşılmayacağından veya bizi zor duruma düşürmek için ifşa edilmeyeceğinden emin olmamız mümkün değildir.

2.1. Panoptikon Kavramı Açısından Mahremiyet

Bireylerin kişisel alanlarının korunması ve istedikleri zaman gizlilik içinde olabilmeleri oldukça önemlidir. Kişiler düşüncelerini, duygularını ve bilgilerini paylaşma veya paylaşmama hakkına sahiptirler. Mahremiyet, bir bireyin özerkliğini ve kişilik bütünlüğünü korumak için önemli bir unsurdur. Bu bağlamda, Jeremy Bentham'ın geliştirdiği panoptikon kavramı, mahremiyet kavramıyla ilginç bir bağlantı sunar. Panoptikon, hapishane kontrol mekanizması olarak tasarlanmış bir yapıdır. Merkezi bir kule etrafında dairesel olarak yerleştirilen hücrelerden oluşur. Oluşturulan bu sistemde hücrelerdeki bireyler sürekli olarak gözetlenebilmektedir. Ancak bireyler ne zaman gözetlendiklerini bilemezler. Bu belirsizlik bireylerin kendilerini sürekli olarak gözetim altında hissetmelerine ve davranışlarını kontrol etmelerine neden olur (Bentham, 1995: 5).

Panoptikon, bireylerin kendi kendini disipline etmelerini mümkün kılan bir mekanizma olarak işlev görüyor olsa da gözetim tehdidiyle karşı karşıya olunması, mahremiyetleri korumak ve bireysel alanları

sınırlamak için önlemler almayı gerektirmektedir. Önlem için fiziksel bir mekanda perdeler kullanarak iç mekanlar gizlenebilir veya kilitli kapılarla erişim sınırlanabilir. Aynı şekilde dijital ortamlarda da güvenlik önlemleri alınabilir, özel bilgilerin paylaşımını kısıtlayan gizlilik ayarları kullanılabilir veya güvenli şifrelerle hesaplar korunabilir. Ancak mahremiyet, bireylerin iç dünyalarını korumak ve özel alanlarında özgürce hareket etmek için de önemlidir. Bireylerin güvenlik ve özgürlük ihtiyaçlarına uygun bir denge sağlamak mahremiyetin korunmasında kritik öneme sahiptir.

Toplumda teknolojinin hızlı ilerlemesiyle birlikte hayatın özel alanları da gözetim ve disiplinin hakim olduğu bir alan haline gelmiştir. Günümüzde her an karşımıza çıkan ve her halimizi kayıt altına alan kameralar, elektronik ortamda yaptığımız her eylemin sensörler sayesinde veri haline dönüştürülüp kaydedilmesi sebebiyle, kullandığımız teknolojilerin özgürlük mü sağladığı yoksa mahremiyet alanlarımızı tamamen ortadan mı kaldırdığı gün geçtikçe belirsizleşmektedir. Ayrıca kişilerdeki internet ortamında özgür oldukları düşüncesi onlarla ilgili daha çok verinin toplanabilmesine de imkan vermektedir. Görüldüğü gibi yapay zekâ çağında tüm dünya bir "Panaptikon"a dönüşmekte ve bireylerin tüm yaşam alanları gün geçtikçe şeffaflaşmaktadır (İzgi, 2014: 28)

2.2. Yapay Zekâ ve Mahremiyet

Geçmiş yüzyılları düşündüğümüzde hayatımızda mahremiyet alanlarını ihlal edeceği endişesi taşıdığımız çok fazla bir şey olmayabilirdi. İnsanların hayatları o zamanlar çok az mahremiyet ihtiyacı ve dolayısıyla mahremiyet ihlali içeriyordu. Yaşam alanlarında çok az insan bulunuyor, onlar da genellikle birlikte yaşıyorlardı. Sanayi Devrimi sonrasında öncelikle şehirler kalabalıklaşmaya insanlar ise kalabalıklar içerisinde yalnızlaşmaya başladılar. Her yalnızlaşma bireyleşmeyi ve bireye ait kavramların şekillenmesinin önünü açtı. Ancak günümüzde mahremiyet kavramı kişisinin kendi özel odasının olmasının; kurduğu iletişimin gizli kalmasının; kamu içerisinde anonim kalmanın çok ötesine geçmiş durumdadır. George Orwell'ın 1984 adlı romanında öngördüğü gibi bir hayatı yaşamamak için YZ'nın mahremiyetimizden taviz vermeden nasıl kontrollü bir şekilde geliştirilebileceği sorusu her geçen gün önemli hale gelmektedir.

İngiliz Matematikçi Clive Humby 2006 yılında *"Dünyanın yeni petrolü veridir. Arıtılmadığı sürece pek bir işe yaramaz. Petrolün karlı bir hale gelmesi için benzine, plastiğe, kimyasal maddelere vb. maddelere dönüştürülmek zorunda olması gibi, verinin de bir değere sahip olması için parçalarına ayrılarak analiz edilmesi şarttır."* demiştir. Veri, YZ çağının en önemli enerji kaynağı haline gelmiştir. Bu veriler sürekli olarak büyük şirketler ve devletler tarafından depolanmakta, bizlere dair çok sayıda bilgi içeren ve çoğunlukla farkında olmaksızın verdiğimiz izinlerle elde edilen bu kayıtlar bulut teknolojisinin gelişmesi ile birlikte bilmediğimiz yerlerde depolanmaktadır (Walsh, 2020: 191-193).

İnternet bağlantıları üzerinden gerçekleştirdiğimiz her eylem bize dair bir veri üretir. Görünüşte bağlantısız büyüyen bu veri kümelerinden hareketle verileri oluşturan kişiler belirlenebilmektedir. Hatta bireylerin belirlenmesi ile kalmayıp kişilerin sosyal durumları, yaşadıkları coğrafya, davranışsal veya zihinsel özellikleri, alışveriş tercihleri, günlük programları veya alışkanlıkları tespit edilebilmektedir (Mazurek and Malagocka, 2019: 344).

YZ destekli cihazlarla ilgili gizlilik ihlallerine yönelik kamu endişesi, özellikle Google ve Apple gibi küresel şirketlerin cep telefonları için ürettikleri kişisel asistanların yaygın kullanılmaya başlanması bu endişeleri körüklemektedir. Bu cihazların bireyleri izlemesi, ortamdaki sesleri dinleyerek kaydetmesi ve sonrasında sıradan ticari ürünlerin reklamlarında bile bu verilerin kullanılması ile ilgili hikâyeler ve makaleler, bireylerin YZ'ya dair olumsuz algılarını pekiştirmekte, mahremiyetle ilgili endişelerini arttırmakta ve kişisel verilerin korunması ihtiyacını beraberinde getirmektedir.

Mahremiyet kavramı, aynı toplum içinde bile farklı gruplar tarafından farklı şekillerde algılanabilmektedir. Çevrimiçi paylaşıma katılan bireyler toplumdan dışlanmak istemezler. Kişiler aynı zamanda birey olarak topluluğun bir parçası olmak, özel şeyleri paylaşmak ve özel yaşamlarını bir dereceye kadar açmak isterler,

ancak paylaştıkları şeyleri o anda kontrol etmek istemezler. Bu kontrolsüz paylaşımlar birçok mahremiyet hakkı ihlalini de beraberinde getirmektedir. Bu durum sadece bireyin kendine dair sorumlulukları ile ilgili değil, aynı zamanda diğer bireylerin gizliliğini koruma sorumluluğunu da ifade eder. Dijital mahremiyetin genel olarak üç temel özelliğinden bahsedilebilir: bilgi gizliliği, haksız müdahaleden korunma ve bireyin kişisel verilerinin korunması. Bilgi gizliliği, bireyin etrafındaki yakın fiziksel alanın ifadesi olan mekansal gizliliği içerir. Haksız müdahaleden korunma, bireyin diğer insanlar tarafından müdahaleye karşı korunma hakkını içerir. Son olarak, bireyin kişisel veri ve kararlarının korunması, bu verilerin toplanması, korunması ve dağıtılmasını ihtiva eder (Semiz, 2018: 165).

Günümüz internet teknolojilerinin mekan ve zaman sınırını ortadan kaldırması bireylerin internet ortamlarında daha fazla vakit geçirmesine ve buna bağlı olarak paylaşımlarında daha bağımsız olmalarına neden olmuştur. Özellikle sosyal medya uygulamaları bireyler arası mahremiyet açısından büyük sorunlar ortaya çıkarmaktadır. Telefonlarımızdaki sosyal medya uygulamalarının sınırsız ve şeffaf iletişim ideali, öncelikle gerçek yaşamın örtülü ve kurallı ilişki biçimlerini transparan ve geçirgen hale getirebilmekte sonrasında ise kişisel mahrem alanlarımızın gizlilik ve özerklik özelliklerinin yitirilmesine neden olmaktadır (Budak, 2018: 168).

Bir hastane randevusuna geç kaldığınızı ve park yeri arayışında telaş içinde olduğunuzu düşünün. Arabanızı nereye park ettiğinizi sıklıkla unuttuğunuz için indirdiğiniz "Arabamı Bul" adlı bir uygulama kullanıyorsunuz. Uygulama aracınızın fotoğrafını çeker ve böylece aracınızı geri almak için doğru yeri kolayca bulmanıza olanak sağlar. Bu uygulama oldukça faydalı gözükmektedir. Ancak bu durum bir dizi mahremiyet ihlalini de beraberinde getirebilmektedir. Oluşturulan veriler ne kadar süre veri tabanında saklı kalacaktır? Bu tür veriler gelecekte nasıl karşımıza çıkacaktır? Oluşturulduktan sonra, bu tür veriler bizden habersiz başka amaçlar için kullanılabilecek midir?

Küresel şirketlerin veri tabanlarına kaydedilen dijital verilerin silinmesi ya da bu silme işleminin takip edilmesi oldukça güçtür. Bu durum "veri kalıcılığı" olarak da ifade edilmektedir (Akçalar, 2020: 3). Geçmişte kişisel bilgisayarlara kaydedilen bilgiler analog kayıtlar oldukları için kolayca yok edilebilmekte hatta depolama birimlerinin az olmasından dolayı bu verilerin silinmesi bir zaruret oluşturmaktaydı. Önceki dönemlerin aksine, oluşturulan devasa bilişim vadileri, küresel şirketlere geniş bir şekilde bu verileri depolama imkanı kazandırmıştır. Veri toplama ve analiz etme araçları için yapılan büyük ölçekli altyapı değişiklikleri, büyük miktarda dijital veri toplamayı ve analiz etmeyi yaygın hale getirmiştir. Veri depolama maliyetleri her geçen gün düşmeye devam ettiği için, küçük firmalar da artık büyük şirketlerin veri tabanlarını kiralamakta bu sayede de tüm verilerin tek elde toplanması verilerin tekelleşmesi problemini beraberinde getirmektedir. Dijital kalıcılık, gizlilik açısından endişe verici olabilir, çünkü gizlilik tercihleri zaman içinde değişebilmektedir (Tucker, 2019: 424-426).

Makine öğrenmesinin belirgin başarıları ve faydalarına rağmen, bugün kullanılan birçok makine öğrenme modeli, kötü niyetli kişilere karşı savunmasızdır. Sistemleri manipüle etmek isteyen kişiler, özel olarak tasarlanmış girişler kullanarak modellerin yanlış tahminler yapmasına neden olmak amacıyla makine öğrenme modellerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini ihlal etmek için çalışabilmektedir. YZ sistemlerine yönelik düşmanca saldırılar, makine öğrenmesinin eğitim veya test aşamasında gerçekleşebilir. Eğitim aşamasında eğitim veri kümesine zararlı veriler enjekte edilerek, giriş özelliklerini veya veri etiketlerini manipüle etmek mümkündür. Bu saldırılar, literatürde zehirleme saldırıları olarak adlandırılır ve güvenilmez kaynaklardan eğitim verileri kullanan uygulamalarda kolayca gerçekleştirilebilir. Herhangi bir hacker, bir makine öğrenme modelinin bilgisine sahipse, eğitim veri setinin orijinal dağılımını değiştirebilir (Oseni vd., 2021: 111).

2005-2013 yılları arasında ABD'de 7.859 veri ihlali kamuoyuna açıklanmış ve potansiyel istismara maruz kalan milyarlarca kişisel tanımlanabilir bilgi kaydının varlığını ortaya çıkarmıştır. Aralık 2013'te 40 milyona yakın veri kaybı yaşanmış, hackerler bu verilerden çoğunlukla banka kartı ve kredi kartı numaralarını ele geçirmiştir. 2017 yılında ise sosyal güvenlik numarası, kredi geçmişi, hatta sürücü belgesi, işlem itiraz

verileri gibi bilgiler aynı veri tabanından çalınmış ve 145 milyon kişi bu sızıntıdan etkilenmiştir. Daha da endişe verici olan ise veri ihlallerinin, büyük miktarda kişisel tanımlanabilir bilgi biriktiren kuruluşlarda meydana gelmiş olmasıdır. Bu kuruluşlar arasında perakendeciler, bilgi birikimcileri, finansal kuruluşlar ve hükümetler, okullar ve hastaneler gibi kâr amacı gütmeyen kuruluşlar bulunmaktadır. Veri ihlallerinin nedenleri de her geçen gün değişiklik göstermektedir. On yıl önce, çoğu veri kaybı, çöp kutusunda bırakılmış, parçalanmamış kayıtlar, şifrelenmemiş verilere sahip kaybolan dizüstü bilgisayarlar veya yanlışlıkla açık web'e yüklenen veriler gibi insan hataları tarafından tetikleniyordu. Son ihlaller genellikle hedeflenen hack saldırıları ve fidye yazılımı saldırılarının sonucudur (Jin, 2019: 448). Ancak yapay zekâ teknolojileri geliştikçe ve toplanan veriler arttıkça, gerçekleştirilen saldırı yöntemlerinin ve olası tehditlerin de artması beklenmektedir.

Kişiselleştirilmiş verilerin büyük veri haline getirilerek depolanması YZ tabanlı programların farklı alanlarda gelişmesine katkı sağlamakta ve milyonlarca insan bu durumdan faydalanmaktadır. Depolanan verilerin genellikle anonimleştirilerek kaydedildiği söylense de elde edilen verilerden hareketle kişiler belirlenebilmektedir. Bu sebeple YZ sistemlerinin sahip olduğu ve bizlere dair ulaştıkları anlık veriler aynı zamanda hackerler tarafından kişisel bilgilerimizin ele geçirilmesi riskini barındırmaktadır (McGraw, 2013: 92). Ayrıca hackerler YZ teknolojilerini bu tür saldırıları başlatmak için kullanma potansiyeline de sahiptirler. YZ uygulamalarının farklı alanlardaki potansiyel tehditleri arasında, YZ'nın barındırdığı güvenlik sorunları, teknolojinin kötüye kullanımından kaynaklanan güvenlik tehditleri, teknik kusurlar nedeniyle ortaya çıkan güvenlik açıkları ve gelecekte muhtemel olan süper zekânın ortaya çıkışı ile ilişkili yaşanabilecek problemler birer endişe kaynağıdır. YZ'nın nötr bir teknoloji oluşu öne sürülebilse de bize ne getireceği, nasıl kullanıldığına ve yönetildiğine bağlıdır. Kötü niyetli kişiler tarafından kötüye kullanıldığında mahremiyet ve etik sorunların ortaya çıkması kaçınılmazdır. Yapılan simülasyonlar hackerlerin YZ sistemlerini kullanarak çok az kaynakla büyük çaplı saldırılar başlatabileceğini göstermektedir. Eğer bu konu ciddiye alınmazsa, gelecekte YZ asistanlarımız saldırıya uğradığında veya ele geçirildiğinde, tüm mahrem alanlarımızın ifşa olması da kaçınılmaz olacaktır (Li and Zhang, 2017: 417).

İçinde bulunduğumuz YZ çağında internet bağlantı ağlarının yeryüzünde yaygınlaşması ile birlikte dünya tam anlamıyla küresel bir köye dönüşmüş durumdadır. Bilişim teknolojilerindeki ilerlemelere paralel olarak toplumlardaki güvenlik algısı da bu noktada değişmektedir. Yeni güvenlik algısının oluşmasında özellikle YZ teknolojilerinin ve makine öğrenmesinin gelişmiş şekli olan derin öğrenme algoritmalarının kullanılması başat unsurdur. Özellikle son zamanlarda hayatımızın her alanını kapsayan mobil uygulamalar tüm bilgilerimize nüfuz edebilmektedir. Bu durum kişisel verilerin korunması ile ilgili gerekli tedbirlerin alınmasını gerektirmektedir. Bunun doğal bir sonucu olarak hem kişisel mahremiyete hem de toplumsal mahremiyete hiç olmadığı kadar büyük önem atfedilmektedir. Bütün bu gelişmeler dikkate alındığında kişisel verilerin korunması, bilgi güvenliğinin tesis edilmesi güvenli bir toplumun inşası için gerçekleştirilecek çalışmalar her geçen gün daha fazla önem kazanmaktadır (Ağıralan, 2015: 80).

Mevcut risklerimizin yanı sıra YZ kavramlarında ifade ettiğimiz Süper Zekâ'nın geliştirilmesi, bizi bekleyen muhtemel en büyük tehlikelerden biridir. Beyne dair bilinenler arttıkça ve oradaki işleyişle ilgili bilgiler derinleştikçe YZ çalışmaları daha nitelikli hale gelmekte, derin öğrenme algoritmaları yeni nitelikler kazanmaktadır. Dünya genelinde bazı araştırma ekipleri, "makine duygusu" ve "makine farkındalığı" gibi yüksek düzeyde bilişsel zekâ üzerinde çalışmalar yapar hale gelmişlerdir. Daha önce de ifade ettiğimiz gibi genel bir YZ'ya ya da süper zekâya ne zaman ulaşacağımız bilinmemektedir. Eğer insanlar tarafından tam olarak kontrol edilemeyen kendiliğinden farkındalık yeteneğine sahip bir süper zekâ ortaya çıkarsa, bunun ciddi bir güvenlik problemi doğuracağı açıktır. Son yıllarda, büyük veri odaklı paradigmalar YZ araştırmalarına hakim olmuş ve YZ gelişiminde yeni bir patlama yaşanmıştır. Mevcut makine öğrenmesinde, veri setlerinin sayısı ve kalitesi eğitim sonuçlarını büyük ölçüde etkilemektedir ve başarılı YZ uygulamalarının çoğu büyük verilere önemli ölçüde bağımlıdır. YZ'nın, ihtiyacı olan verileri kendi kendine kaydedip işleyerek kendine malzeme olarak kullanabilmesi mahremiyet sorununun temelini teşkil etmektedir.

Gelecekte oluşturulabilecek bir süper zekânın varlığı ve nesnelerin interneti ile evlerimizdeki akıllı cihazların yaygın kullanımı birlikte düşünüldüğünde, evlerimiz artık birer Panoptikon'a dönüşmüş olacaktır. Panoptikon'da anlık gözetlemeler söz konusu iken mevcut durumda kişisel mahrem bilgilerimiz kayıt altına alınacak, yıllarca saklanabilecektir (Yüksel, 2021: 92). Bu veriler, uygun şekilde kullanıldığında günlük yaşantımızı iyileştirmektedir. Ancak, bazı özel bilgilerimizin herhangi bir şekilde aleyhimize kullanılabilir oluşu ve bu duruma dair bilgimizin olmayışı bizler için büyük tehdittir (Peppet, 2013: 98).

Bulut teknolojilerinin gelişmesiyle birlikte, birçok birey, şirket ve hükümet kuruluşu verilerini buluta taşımaktadır. Kullanımı kolay olan ve paylaşılan bir havuza anında ağ erişimi sağlamada uygun bir imkan olan bu teknolojik yenilikler özel bilgilerimizi bulutta depoladığından, mahremiyetimizin korunmasından nasıl emin olabileceğiz? Yapay zekânın daha yüksek hesaplama gereksinimleri göz önüne alındığında, bulut bilişimi birçok YZ uygulamasının temel altyapısı olarak yapılandırılmıştır. Bu nedenle bu tür YZ uygulamalarını günlük hayatımızda kullanırken mahremiyet sorunlarını tekrar düşünmemiz gerekmektedir. Bilgi çıkarma araçları giderek daha güçlü hale geldikçe, görünüşte ilişkisiz birçok veri parçası birleştirilerek bireysel davranış özelliklerinin belirlenmesi ve dolayısıyla kişisel mahremiyetin açığa çıkması mümkün hale gelmektedir. İnternet sitelerini ziyaret izleri, alışveriş süreçleri ve diğer farklı türdeki kayıt verileri bir araya getirildiğinde, artık o kişinin davranış haritasını çıkarmak, kişisel tercihlerini ve davranış alışkanlıklarını analiz etmek, her şeyini bildiğiniz ve tanıdığız bu bireyi özelleştirilmiş içeriklerle manipüle etmek mümkün hale gelmiştir (Li and Zhang, 2017: 418).

2006 yılında Netflix şirketi filmleri değerlendirmek için bir yarışma düzenlemiştir. Yaklaşık 500 bin kişinin katıldığı bu yarışmada yirmi bin civarında filme dair yüz milyona yakın değerlendirme verisi oluşmuştur. Şirket, kullanıcılarının mahremiyetini korumak için kişisel bilgiler yerine rastgele numaralar vererek verileri anonim haline getirmeyi amaçlamıştır. Ancak Teksas Üniversitesi'nden bir grup araştırmacı bu verileri başka verilerle ilişkilendirerek kişisel bilgilere ulaşmayı başarmıştır. Günümüzde sadece internet ortamında aktif olduğumuz anlarda değil çevrimdışı olduğumuz anlarda bile izlenebilir durumdayız. Özellikle son yıllarda karşılaştığımız en büyük problem bulut teknolojileri ile birlikte tüm verilerimizin tek elde toplanıyor oluşudur. Bizlere dair verilerde güvenliğimizi sağlamak için tekil verilerin toplanması bir önlem olarak düşünülmüş ve toplanan verilerin de anonimleşmesi sağlanmaya çalışılmış, bunlarla ilgili çeşitli yasal düzenlemeler gerçekleştirilmiştir. Ancak bu verilerin birbirleriyle ilişkilendirilmesi ve bunun denetiminin yapılabilmesi çok da mümkün gözükmemektedir. Şehirler ve sahip olduğumuz makineler her geçen gün daha akıllı hale geldikçe sadece kamusal alanlar değil her anımız gözlenebilir duruma gelmiştir. Android ve IOS cihazlar artık vücudumuzdaki bir organ haline dönüşmüştür. Bu cihazların sesli komutlarımıza tepki vermekte, diğer durumlarda pasif olduğu düşünülmektedir. Ancak yapılan araştırmalarda bu cihazların sürekli olarak ortamları dinlediği ve kayıt altına aldığı raporlanmaktadır (Walsh, 2020: 196-198). Yakın zamanda karşılaştığımız ilginç bir haber de evdeki robot süpürgenin çektiği fotoğrafların internet ortamına düşmesi olmuştur. Yakın gelecekte nesnelerin internetinin tam anlamıyla gerçekleşmesi ile hayatımızdaki tüm teknolojik aletler ortamlardaki tüm konuşmaları dinleyebilecek, sahip olduğumuz her şeyi gözleyecek ve bunları hayatımızı kolaylaştırmak adına hepimizi buna gönüllü kılacaktır ve halihazırda kılmaktadır da (URL-3).

Bazı uzmanlar, dijital mahremiyetimizi savunma savaşının çoktan kaybedildiğini düşünmektedir. Facebook, Google, Microsoft gibi küresel teknoloji devleri sahip olduğumuz tüm verileri geri dönülemez bir şekilde zaten ele geçirmiş durumdadır. Kendimizi ve çocuklarımızı akıllı kol saatlerine, navigasyon uygulamaları ile gittiğimiz her yerin kayıt altına alınmasına, yaptığımız online alışverişler ile tüketim alışkanlıklarımıza dair verilerin paylaşılmasına, e-postalarımızda uygulanmasını istediğimiz filtreleme özellikleri ile e-postalarımızın içeriklerinin görülmesine çoktan izin vermiş durumdayız. Bu verilerin aleyhimizde

[3] Nesnelerin İnterneti (IoT), fiziksel nesnelerin internet üzerinden birbirleriyle ve diğer bilgisayarlarla iletişim kurabilme yeteneği olarak tanımlanır. Bu nesneler, sensörler, yazılım, veri depolama ve ağ bağlantısı gibi teknolojileri kullanarak bilgi toplayabilir, işleyebilir ve paylaşabilirler. Bu sayede fiziksel nesneler, düşük maliyetli hesaplama, bulut teknolojileri, büyük veri, analitik ve mobil teknolojiler aracılığıyla verileri minimum insan müdahalesiyle paylaşabilir ve toplayabilir.

kullanılmaması için yapabildiğimiz tek şey ise ihlaller gerçekleştiğinde şirketlerin karşılaşacağı yaptırımları ağırlaştırmak olmaktadır ki bunun da ne kadar çözüm üreteceği şüpheli gözükmektedir (Barkuş ve Koç, 2019: 39). Böyle bir ortamda duygusal, sosyal ve ekonomik durumlarımıza dair verilerimiz üzerindeki kontrolümüz her geçen gün kaybolmaktadır. Bu bağlamda bizlere tanınan hukuki haklar uygulamaların kullanımlarının başındaki verdiğimiz izinlerle giderek anlamını yitirmektedir.

Mahremiyet hakkının temel niteliği, kişilerin kendilerine dair bilgilerin dolaşımı üzerinde kontrol yeteneğine, kişisel özgürlükleri muhafaza etme imkanına sahip olmalarıdır. İnsanların, kendilerine ilişkin verileri üzerinde denetimi kaybetmeleri, verilerin başka şahıs, kurum ve şirketlerin kontrolü altına girme riskini de ortaya çıkarmaktadır. Bizlere dair toplanan veriler nicel olarak arttıkça ve YZ teknolojileri ile bunlar nitelikli veriler haline getirildikçe verilerimiz eskiden olduğu gibi parçalı olmaktan çıkmakta ve bizlere dair her türlü bilginin başkaları tarafından ulaşılabilir, yorumlanabilir, sistematik olarak dosyalanabilir hale gelmesine neden olmaktadır. Bu sistemler sayesinde kişisel bilgilerin mahremiyetini muhafaza etmek ve mevcut verilere eklemeler ve çıkarmalar yaparak verileri değiştirmek; bu verileri sosyal medya platformları eliyle çok geniş bir kitlelere iletmek mümkün hale gelmiştir. Verilerimizi tek elde toplayan; bu veriler arasında bizlerin görmekte ve kurmakta zorlanacağımız ilişkileri kurabilen ve yorumlayabilen günümüz yapay zekâ teknolojileri için, kişisel mahremiyet alanlarımızı muhafaza etmek imkansızlaşmaktadır (Yüksel, 2003: 80).

Tüm bu olumsuzluklara rağmen mahremiyet alanlarını korumak için birkaç yöntem geliştirilmiştir. Makine öğrenmesi gizlilik ihlalleri, genellikle kaydedilen farklı tür verilerimiz arasında aşırı uyum ve kullanılan veri mimarileri ile ilgili bazı sorunlarla karşı karşıyadır. Son araştırmalar, farklılaşan gizlilik mekanizmalarının bu sorunları çözme potansiyeline sahip olduğunu göstermektedir. İlk olarak, bir modelde dengeyi korumak için eğitim verileri, farklılaşan gizlilik mekanizması kullanılarak veri evreninden yeni örnekler alınarak oluşturulabilmektedir. Buna ek olarak da gizliliği korumak için veri grubuna sahte veriler eklenebilmektedir. Bu tür yanıltıcı verilerin ortama eklemlenmesi ile oluşturulan modellere gürültülü öğrenme modelleri denmektedir. Gürültü eklenmiş modellerle oluşturulan öğrenme algoritmaları, veriler arasındaki aşırı benzerlikleri ortadan kaldırmak için yeni verilerle beslenerek algoritmaların kararlılıkları arttırılabilmektedir. Bu farklılaşan gizlilik uygulamaları, rastgeleleştirme, gizlilik koruma yeteneği ve algoritma kararlılığı gibi farklılaşan gizlilik özelliklerinden yararlanarak derin öğrenme ile ilgili sorunların çözülebileceğini göstermektedir (Zhu vd., 2022: 2825).

Sorunları azaltmanın bir başka yolu da bilgisayarlarımızı virüslerden koruyan programların bir benzerini YZ ile üretmek ya da bu tür programları mahremiyet problemlerinin oluşmasını engellemek için eğitmek olacaktır. Halihazırda mevcut tarayıcılarımız bilgisayarlarımızdaki olağan dışı durumlarda bizlere bildirim göndermekte, riskli sitelere ulaşmak istediğimizde bize engel olmakta ya da gerekli uyarıları yapmaktadır. Virüslere karşı geliştirilen bu önlemlerin benzerlerini derin öğrenme algoritmaları sayesinde kullanıcılar için kişi mahremiyet riski teşkil edecek durumları analiz etmek, bu noktada kullanıcıya gerekli uyarıları yapmak ve bu hususlarda YZ tabanlı teknolojileri kullanmak mümkündür. Derin öğrenme algoritmaları bizlerin takip etmekte zorlandıkları veri akışlarını, verilerin içeriklerini ve olası riskleri algılama bu riskleri analiz ederek kullanıcıları uyarma ve bu şekilde programlanma potansiyelini barındırmaktadır. Bu algoritmaların eğitimlerinde kullanılacak verileri hazırlamak, kişilerin online ortamlarda hizmete ulaşmak için düşünmeden mahremiyet alanları ile ilgili verdikleri izinlerin ve gelecekte yaşayabilecekleri sıkıntıların önüne geçmek mümkündür. Bu tür programların hazırlanması için oluşturulacak protokollerin interdisipliner bir bakış açısıyla hazırlanması problemlerin azaltılması ya da başka problemlerin ortaya çıkışının önlenmesi açısından önemlidir.

2.3. Mahremiyetle İlgili Yapılan Düzenlemeler

Modern topluma geçiş aşamalarında bireye verilen değerin öneminin artması bireysel hak ve özgürlüklerin de her geçen gün önem kazanmasına neden olmuştur. Başlarda bireylerin hakları kapsamında ele alınan mahremiyet hakkı, sonraki yıllarda özel bir hak kapsamına alınmış, ülkelerin anayasaları ve kanunları

tarafından düzenlenmiş, gittikçe globalleşen dünyada uluslararası düzenlemelerin konusu olmuştur (Yüksel, 2003: 186). İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." (URL-4) şeklinde düzenlenmiştir. Ülkemizin 1954'te onaylayıp 1987'de de bireysel başvuru hakkını tanıdığı Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi:

"Özel ve aile hayatına saygı hakkı 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. 2. 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." (URL-5) demektedir.

Avrupa Birliği Temel Haklar Şartı'nın 7-8. Maddelerinde:
"Özel ve aile yaşamına saygı: Madde7: Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir. Madde 8: Kişisel bilgilerin korunması 1. Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir. 2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir. 3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir." (URL-6)

ifadeleri yer almaktadır. Benzer bir şekilde Türkiye Cumhuriyeti Anayasası 17., 20. ve 22. Maddelerinde: *"Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir. Tıbbi zorunluluklar ve kanunda yazılı haller dışında, kişinin vücut bütünlüğüne dokunulamaz; rızası olmadan bilimsel ve tıbbi deneylere tabi tutulamaz..(Madde17) 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. (Madde 20 Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır."* (Madde 22) (URL-7) denilmektedir.

Kişisel bilgilere çeşitli şekillerde ulaşma ihtiyacı tarihin her döneminde olmuştur. Eskiyle kıyaslandığında bireylere dair her türlü bilgiye ulaşmak her geçen gün daha kolay hale gelmektedir. Kişisel bilgileri toplamak teknolojinin de gelişimiyle daha da artmıştır. Dolayısıyla kişisel veriye olan ihtiyaç gelişen teknolojinin hem en büyük gereksinimi hem de en çok istismara açık alanı haline gelmiştir. İnsanlara dair verilerin korunması, özel hayatın gizliliğinin muhafazası kapsamında her geçen gün yeni bir düzenlemeye ihtiyaç duyulmaktadır. Devletlerin vatandaşlarının güvenliği için bireyleri gözetleme, onlara dair verileri kaydetme yetkisi, bireylere ait mahremiyet haklarının ihlal edilmeden gerçekleşmesi için gerek uluslararası alanda gerekse ülkemizde görüldüğü gibi pek çok düzenleme yapılmıştır. Diğer ülkelerle kıyaslandığında bu düzenlemeler ülkemizde göreceli olarak biraz daha geç gerçekleşmiştir. Zira teknolojinin gelişmesi ile birlikte bu alan dinamik bir şekilde yeni düzenlemeler gerektirmektedir. Ülkemizdeki son düzenleme 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu ile yapılmıştır (Yavuz, 2022: 65-67).

Dijitalleşmenin toplumun her noktasına ulaşması ve yapay zekâ tabanlı teknolojilerin her geçen gün bireysel kullanımda yaygınlaşması, mahremiyet problemlerini doğurmakta ve devletlerin bu noktada hukuki düzenlemeler yapmasına yol açmaktadır. Ancak yapay zekânın hızlı dönüşümü ve teorik de olsa gelecekte sahip olması beklenen muhtemel nitelikleri göz önüne alındığından teorik ve hukuksal düzenlemeler ne kadar kapsamlı şekilde düzenlenmiş olursa olsun her daim yeni düzenlemelere ihtiyaç olacak gibi gözükmektedir. Bu durumda mahremiyet haklarının korunması noktasında toplumları tatmin edecek düzenlemelerin problemler çıkmadan gerçekleştirilmesi, bunun için de yapay zekâ geliştirme süreçlerinin düzenlenmesi ve denetim mekanizmalarının buradan başlanarak yapılması büyük önem arz etmektedir.

Sonuç

Günümüz ve yakın gelecek için hala birçok soru ve sorun bulunmaktadır. Yapılan literatür taramasında öne çıkan ve üzerinde yeterli tartışma yapılmadığı düşünülen bazı sorular şunlardır: "Mevcut yasalar altında YZ geliştirilmesine devam edilmeli midir yoksa gerekli düzenlemeler daha etkili hale getirilmeye mi çalışılmalıdır? Bireyler hem kolaylık hem de gizlilik talep ettiğinde firmalar nasıl veri teknolojisi ve veri politikası seçmelidirler? YZ tabanlı uygulamaların mahremiyet ve veri güvenliği açısından getirdiği riskleri nasıl dengelenecektir? Yasama organlarına bu süreçler için sahada karşılaşılan problemler sonrasında mı gerekli düzenlemeler için baskı yapılmalı yoksa problemlerin çıkmasını beklemeden ülke çapında yasaklanması için mi harekete geçilmelidir? Herhangi bir ulusal yasaklama ülkemizin küresel teknoloji geliştirme rekabetinde geri kalmasına neden olmayacak mıdır?" Bu sorular, ekonomi, bilgisayar bilimi, bilgi bilimi, istatistik, pazarlama ve hukuk gibi birçok disiplinden araştırmacıların interdisipliner bir bakış açısıyla yapmaları gereken çalışmaları her geçen gün daha da önemli hale getirmektedir ve bu türden çalışmaların sayısı ve niteliği arttırılmalıdır.

Bireyler dahil oldukları dijital dünyada teknolojinin imkanlarından koşulsuz ve sınırsız faydalanabilmek için mahremiyet haklarından gönüllü olarak vazgeçebilmektedirler. Onlara dijital dünyada bir başına olmadıkları, bir Panoptikon'un içinde olduklarının sık sık hatırlatılması gerekmektedir. Bireylere veri güvenliği ve yapay zekâ teknolojilerinin sahip olduğu niteliklerle ilgili farkındalıklarının arttırılması için nitelikli ve bilinçlendirici eğitimler verilmesi, okullarda ders olarak okutulması, bireysel farkındalık oluşturacak etkinliklerin geliştirilmesi gelecekte oluşabilecek problemlerin azaltılmasında etkili olacaktır.

Hükümetlere karşı şeffaflık ve sorumluluk konusunda genellikle bir güven eksikliği söz konusudur. Mahremiyetle ilgili yaşanabilecek problemlerin herhangi bir denetim mekanizmasından uzak oluşu ayrıca YZ teknolojilerinin geliştirilme süreçlerinin ticari sır kapsamında ele alınması ve yine hükümetlerin ve şirketlerin bu tür programları genellikle gizli yürütüyor olmaları karşımızda bir problem alanı olarak hep var olacaktır. Firmaların kişisel verilerin gizliliği ve veri güvenliği konusunda taşıdıkları risk için tam olarak sorumlu tutulması gerekmektedir. Bunun için de öncelikli olarak firmaların veri toplama, veri depolama ve veri kullanma mekanizmalarına yönelik denetim mekanizmaları kurulmalı, veri toplayan ve saklayan mekanizmalar süreklilik esasıyla bağımsız kurumlarca denetlenmelidir.

Güvenlik, etik ve mahremiyet ihlali ile ilgili tehditler konusundaki endişelere rağmen, YZ'nın bu konularda yapılacak çalışmalarda güvenlik sağlamaya yardımcı olabileceği değerlendirilmektedir. Yapay zekâ teknolojilerinin avantajlarından yararlanılarak, dijital ortam için güvenlik ve mahremiyet korumasının arttırılması ve bu yönde teknolojiler geliştirmesi de mümkün olabilecektir. Bu kapsamda devlet eliyle araştırmacıların desteklenmesi bu süreçlerin devletin himayesinde ve teşviği ile devam etmesi de ayrıca önemlidir. Gerekli düzenlemeler yapılırsa YZ'nın mahremiyetle ilgili problemlerin azaltılması konusunda fayda sağlama potansiyelinin de yüksek olduğu gözden kaçmamalıdır.

KAYNAKÇA

Ağıralan, Erkan (2015). Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi. Yüksek Lisans Tezi. Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü.
Akçalar, Aslıhan (2020). Dijital Mahremiyet : 21. Yüzyıl Bilgi Profesyonellerinin Yetkinlikleri. Yüksek Lisans Tezi. İstanbul: Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü.
Barkuş, Fatma ve Koç, Mustafa M. K. (2019). "Dijital Mahremiyet Kavramı ve İlgili Çalışmalar Üzerine Bir Derleme". Bilim, Eğitim, Sanat ve Teknoloji Dergisi, 3(1): 35-44.
Barrat, James (2020). Yapay Zekâ ve İnsanlık Çağının Sonu Son İcadımız. İstanbul: Pegasus Yayınları.
Bentham, Jeremy (2020). The panopticon writings. Verso Books
Boden, Margaret (2016). ARTIFICIAL INTELLIGENCE A Very Short Introduction. New York: Oxford University Press.
Bostorn, Nick (2020). Süper Zekâ. İstanbul: Koç Üniversitesi Yayınları.
Breckenridge, Adam Carlyle (1970). The Rİght to Privacy. Lincoln: Universty of Nebraska Press.
Budak, Hatice (2018). "Sosyal Medya İletişiminde Mahremiyetin Serüveni". İnsan ve Toplum Bilimleri Araştırmaları Dergisi, 7(1), 146-170.
Büyükuslu, Ali Rıza (2020). Koronavirüs Sonrası Yeni Dünya Düzeni Ekonomi Devket Yapay Zekâ. İstanbul: Der Yayınları.
Coşkun, Osman ve Kuşçu, Ertan (2021). "Artificial Intelligence's Pupil Natural Language Processing". Turkophone, 8(3): 116-129.
Curzon, James vd. (2021). "Privacy and artificial intelligence". IEEE Transactions on Artificial Intelligence, 2(2): 96-108.
Çakır, Pervin ve Temir, Erkam (2022). "Sosyal Medyada Benlik Sunumu ve Mahremiyet Kavramı ile İlişkisi: Nicel Bir Araştırma". Yeni Medya, 13: 205-228.
Dawoud, Muhammed (2017). Privacy Preserving Search and Data Retrıeval From Data Clouds. Doktora Tezi. İstanbul: İstanbul Teknik Üniversitesi.
Demir, Ozan (2019). "Sürdürülebilir Kalkınma İçin Yapay Zekâ". Yapay Zekâ ve Gelecek. Ed. Gonca Telli. İstanbul: Doğu Kitap Evi, 44-63.
Diffie, Whitfield, and Landau, Susan (1998). Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge: The MIT Press.
Gelbal Odabaş, Özlem (2019). Ergenler İçin Sosyal Medya Mahremiyeti Koruma Becerileri Ölçeği. Yüksek Lisans Tezi. Tokat: Tokat Gaziosmanpaşa Üniversitesi Eğitim Bilimleri Enstitüsü.
Gündoğan, Ali Osman (2019). "Başlangıçtan Günümüze Mahremiyetin İdrak Edilişi". Mahremiyet Hayatın Sırları ve Sınırları. Ed. Nazife Şişman. İstanbul: İnsan Yayınları.
Hughes-Roberts, Thomas, & Kani-Zabihi, Elahe (2014). "On-line privacy behavior: Using user interfaces for salient factors". Journal of Computer and Communications, 2: 220-231.
İzgi, M. Cumhur (2009). Etik Açıdan Yaşlı Mahremiyeti: Huzurevi Öğrneğinde Hizmet Alanlar ve Verenler Açısından Bir Değerlendirme. Doktora Tezi. Ankara: Ankara Üniversitesi Sağlık Bilimleri Enstitüsü.
İzgi, M. Cumhur (2014). "Mahremiyet kavramı bağlamında kişisel sağlık verileri". Türkiye Biyoetik Dergisi, 1(1): 25-37.
Jin, Ginger Zihe (2017). "Artificial Intelligence and Consumer Privacy". The Economics of Artificial Intelligence: An Agenda. University of Chicago Press, 439-462.
Kutlusoy, Zekiye (2019). "Felsefe Açısından Yapay Zekâ". Yapay Zekâ ve Gelecek. Ed. Gonca Telli. İstanbul: Doğu Kitap Evi, 25-43
Kütükoğlu, Elif (2021). Kuşaklar Bağlamında Sosyal Medya ve Mahremiyet. Konya: Eğitim Yayınevi.
Li, Xiuquan, and Zhang, Tao (2017). "An exploration on artificial intelligence application: From security, privacy and ethic perspective". 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (28-30 April 2017). IEEE: 416-420
Mazurek, Grzegorz and Małagocka, Karolina (2019). "Perception of Privacy and Data Protection in The Context of The Development of Artificial İntelligence". Journal of Management Analytics, 6(4): 344-364.
McCarthy, John vd. (2006). "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence". AI Magazine, 27(4): 12-14.

McGraw, Deven (2013). "Policy Frameworks to Enable Big Health Data". On Tuesday, September 10th, 2013, the Future of Privacy Forum joined with the Center for Internet and Society at Stanford Law School to present a full-day workshop on questions surrounding Big Data and Privacy, 90-93
Oseni, Ayodeji (2021). "Security and privacy for artificial intelligence: Opportunities and challenges". J.ACM, 37(4): 111-146.
Peppet, Scott R. (2013). "Sensor Privacy as One Realistic & Reasonable Means to Begin Regulating Big Data". On Tuesday, September 10th, 2013, the Future of Privacy Forum joined with the Center for Internet and Society at Stanford Law School to present a full-day workshop on questions surrounding Big Data and Privacy: 98-101.
Reese, Byron (2018). Yapay Zekâ Çağı. İstanbul: Say Yayınları.
Sönmez, Onur (2020). Ulusal Güvenlikte Yapay Zekâ Kullanımı ABD ve Çin Örnekleri. Ankara: Nobel Bilimsel Eserler.
Tegmark, Max (2019). Yaşam 3.0 Yapay Zekâ Çağında İnsan Olmak. İstanbul: Pegasus Yayınları.
Topal, Çağatay (2017). "Alan Turing'in Toplumbilimsel Düşünü: Toplumsal Bir Düş Olarak Yapay Zekâ". DTCF Dergisi, 57(2): 1340-1364.
Tucker, Catherine (2019). "Privacy, Algorithms, and Artificial Intelligence". The Economics of Artificial Intelligence: An Agenda. University of Chicago Press: 423 – 437
Turing, Alan Mathison (1936). "On computable numbers, with an application to the Entscheidungsproblem". Proceedings of the London: 345-363.
Turing, Alan Mathison (1950). "Computing Machinery and Intelligence". Mind.49: 433-460.
Türkoğlu, Hülya Semiz (2018). "Sosyal Medya Üzerinden Mahremiyet Farkındalığı ve Değişimin Ölçümlenmesine Yönelik Bir Araştırma". Connectist: Istanbul University Journal of Communication Sciences, 54: 163-189.
Walsh, Toby (2020). 2062: Yapay Zekâ Dünyası. İstanbul: Say Yayınları.
Yavuz, Baturalp (2022). "Gözetim ve Mahremiyet Toplumu". Yaşar Hukuk Dergisi, 4(2): 60-82.
Yılmaz, Mustafa K. ve İyigün, N. Öykü (2020). Oyun Değiştiren Güç: Yapay Zekâ. İstanbul: Beta Kitap.
Yılmaz, Mustafa K. ve İyigün, N Öykü (2020). YAPAY ZEKÂ: Güncel Yaklaşımlar ve Uygulamalar. İstanbul: Beta Kitap.
Yüksel, Mehmet (2003). "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi". Ankara Üniversitesi SBF Dergisi, 58(1): 183-212.
Yüksel, H. (2021). "Sosyal Medya Ortamında Mahremiyet Sorunu: Facebook ve WhatsApp Platformları". Kastamonu İletişim Araştırmaları Dergisi, 7: 86-108.
Yüksel, Mehmet (2003). "Modernleşme ve Mahremiyet". Kültür ve İletişim, 6(1) (11): 75-108.
Zhu, Tianqing vd. (2020). "More than privacy: Applying differential privacy in key areas of artificial intelligence". IEEE Transactions on Knowledge and Data Engineering, 34(6): 2824-2843.
İnternet Kaynakları:
URL-1: "What is artificial intelligence". https://www-formal.stanford.edu/jmc/whatisai.pdf. (Erişim: 08.09.2023)
URL-2: "Yapay Zeka Zaman Çizelgesi". https://turkiye.ai/kaynaklar/yapay-zeka-zaman-cizelgesi. (Erişim: 08.09.2023)
URL-3: "Robot Süpürge". https://www.hurriyet.com.tr/dunya/robot-supurgenin-cektigi-mahrem-goruntuler-facebooka-dustu-buyuk-skandal-infiale-neden-oldu-42191686. (Erişim: 21.07.2023)
URL-4: "İnsan Hakları Evrensel Beyannamesi". https://hsk.gov.tr/Eklentiler/Dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf. (Erişim: 08.09.2023)
URL-5: "Avrupa İnsan Hakları Sözleşmesi". https://hsk.gov.tr/Eklentiler/Dosyalar/3fdd972e-8566-4b8a-9ffe-d9205f4e51cd.pdf. (Erişim: 08.09.2023)
URL-6: "Avrupa Birliği Temel Haklar Şartı". http://www.ceidizleme.org/ekutuphaneresim/dosya/687_1.pdf. (Erişim: 08.09.2023)
URL-7: "Anayasa". https://www.mevzuat.gov.tr/#anayasa. (Erişim: 08.09.2023)