T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Radyo, Televizyon ve Sinema Anabilim Dalı

Yeni Medya İletişim ve Habercilik Bilim Dalı

YAPAY ZEKÂ ÇAĞINDA SOSYAL GÜVENLİK: SOSYAL MEDYA PLATFORMLARINDA VERİ GİZLİLİĞİ VE GÜVENLİK SORUNLARI, FIRSATLAR VE ZORLUKLAR

Yüksek Lisans Tezi

Husam Berdi Radhi RADHI

Danışman

Dr. Öğr. Üyesi Özlem Tuğçe KELEŞ

İstanbul – 2025

EZ TANITIM FORMU

Yazar Adı Soyadı	**:**	Husam Berdi Radhi RADHI
Tezin Dili	**:**	Türkçe
Tezin Adı	**:**	Yapay Zekâ Çağında Sosyal Güvenlik: Sosyal Medya Platformlarında Veri Gizliliği ve Güvenlik Sorunları
Enstitü	**:**	İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsü
Anabilim Dalı	**:**	Radyo, Televizyon ve Sinema
Tezin Türü	**:**	Yüksek Lisans
Tezin Tarihi	**:**	21.04.2025
Sayfa Sayısı	**:**	124
Tez Danışmanları	**:**	Dr. Öğr. Üyesi Özlem Tuğçe KELEŞ
Dizin Terimleri	**:**	Yapay Zekâ, Sosyal Güvenlik, Veri Gizliliği Sosyal Medya Platformları
Türkçe Özet	**:**	Bu tez, yapay zekâ çağında sosyal medya platformlarının sosyal güvenlik, veri gizliliği ve güvenlik üzerindeki etkilerini analiz etmeyi amaçlamaktadır. Çalışmada, teknolojik gelişmelerin sosyal güvenlik yapısında oluşturduğu değişimler incelenmekte, ortaya çıkan fırsatlar ve riskler değerlendirilmektedir.
Dağıtım Listesi	**:**	1. İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsüne 2. YÖK Ulusal Tez Merkezine

Husam Berdi Radhi RADHI

T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Radyo, Televizyon ve Sinema Anabilim Dalı

Yeni Medya İletişim ve Habercilik Bilim Dalı

YAPAY ZEKÂ ÇAĞINDA SOSYAL GÜVENLİK: SOSYAL MEDYA PLATFORMLARINDA VERİ GİZLİLİĞİ VE GÜVENLİK SORUNLARI, FIRSATLAR VE ZORLUKLAR

Yüksek Lisans Tezi

Husam Berdi Radhi RADHI

Danışman

Dr. Öğr. Üyesi Özlem Tuğçe KELEŞ

İstanbul – 2025

BEYAN

Bu tezin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez olarak sunulmadığını beyan ederim.

Husam Berdi Radhi RADHI

…/…/2025

T.C.

İSTANBUL GELİŞİM ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Husam Berdi Radhi RADHI' nın **"Yapay Zeka Çağında Sosyal Güvenlik: Sosyal Medya Platformlarında Veri Gizliliği ve Güvenlik Sorunları, Fırsatlar ve Zorluklar"** adlı tez çalışması, jürimiz tarafından Radyo, Televizyon ve Sinema Anabilim Dalı Yeni Medya İletişim ve Habercilik Bilim Dalı YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan _____

Doç. Dr. Güven ÖZDOYRAN

Üye _____

Doç. Dr. Taylan MARAL

Üye _____

Dr. Öğr. Üyesi Özlem Tuğçe KELEŞ

(Danışman)

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

.... / .... / 20..

Prof. Dr. İzzet GÜMÜŞ

Enstitü Müdürü

ÖZET

Günümüz bilgi çağında Hayatımızın ayrılmaz bir parçası haline gelen yapay zeka teknolojileri ile kişilerin özel hayatları ve tercihleriyle ilgili farklı yöntemlerle veri toplanmakta, bununla birlikte yapay zekâ gibi ileri teknolojilerin etkin bir şekilde nasıl kullanılabileceği üzerinde durulmaktadır. Özellikle yapay zekâ temelli çözümler, otomatik tehdit tespiti, siber güvenlik uygulamaları ve veri analitiği gibi alanlarda birçok güvenlik iyileştirmesi sunabilir. Ancak, bu teknoloji kullanılırken etik sorunlar, insan hatalarının azaltılması, gizlilik endişeleri ve eğitim gibi zorluklar tartışılmaktadır. Ayrıca yapay zekânın tahminler ve doğruluğu kesinlik kazanmamış hakkında da sonuç vermesi mümkündür. Bu verilerin toplanması, değiştirilmesi, işlenmesi, aktarılması ve bu verilerden elde edilen sonuçlara göre çıkarım yapılması gibi süreçlerde, çeşitli hukuki sorunlara yol açabilmektedir. Yapay zekâ teknolojileri özellikle kişisel verilerin korunması bağlamında önemli sorunlara neden olabilir, zengin ve çok çeşitli kişisel verilerden yararlanarak önyargılı ve hatta ayrımcı kararlar verebilmektedir. Günümüzde kişisel verilerin korunması kanunları ile korunmaya çalışılmasına rağmen, insanların yalnız kalma hakkıyla birlikte kimliğini, gizlilik politikasını ve Bağımsızlığını korumak için düzenlenip uygulamaya alınmasına rağmen bu kanunlar yapay zekâ teknolojilerinin getirdiği risklerden kişileri korumada yetersiz kalmaktadır.

Bu tezin amacı, yapay zekâ çağında sosyal güvenlik kavramını, sosyal medya platformlarındaki veri gizliliği ve güvenlik sorunları üzerinden analiz etmek, zorlukları ve yararları açıklamaktır. Sosyal medya kullanımının artmasıyla veri gizliliği ve güvenlik sorunları görünür hale gelmiştir. Yapay zekâ uygulamalarının bu konudaki etkileri incelenerek sosyal güvenlik açısından rolü değerlendirilecektir. Çalışmada yasal ve etik zorluklar, gelecekteki yönler, teknoloji ve yenilikler, hakkında bahsedilecektir. Veri toplama ve işleme süreçlerinin yasalara ve bireysel haklara etkisi, yapay zekanın gizliliği artırma ve güvenlik potansiyeli, sosyal medya veri koruma politikalarının gelişimi değerlendirilecektir.

Yapay Zekâ döneminde kişisel güvenliği artırmak ve toplumu korumak adına sosyal medya platformlarında, teknolojinin kullanımında toplumsal ve bireysel güvenliğin karşı karşıya kaldığı yarar ve zararları belirlemek amacıyla nitel araştırma yöntemlerinden söylem analizi Kullanılmaktadır. Mahremiyetle ilgili konular ve

sosyal medya etik yasaları ve kuralları gibi konuları içeren akademik literatürdeki önemli literatürün gözden geçirilmesini desteklemektedir. Raporlar, resmi dergiler ve akademik araştırmalar kullanılır ve önceki çalışmalarla karşılaştırılır.

Sonuç olarak, eğitim ve bilinçlendirme faaliyetleri yürütülmektedir. Bu, tekniklerin farkındalığının ve anlaşılmasının artması açısından çok önemlidir. Kullanıcılar sosyal medya platformlarındaki güvenlik risklerine göz önünde bulundurarak, teknoloji şirketleriyle iş birliği içinde daha güvenli dijital ortamların oluşmasına yardımcı olabilir. Aynı zamanda internette veri ve mahremiyetin korunmasına yönelik etkili hukuki kuralların ve politikaların geliştirilmesinin önemine de vurgulanıyor.

Anahtar Kelimeler: Yapay Zekâ, Sosyal Güvenlik, Veri Gizliliği Sosyal Medya Platformları

SUMMARY

Artificial intelligence has become an integral part of daily life, utilizing various methods to collect data on individuals' behaviors, preferences, and private lives. While AI-powered solutions contribute significantly to security advancements in areas such as data analytics, automated threat detection, and cybersecurity, they also introduce several challenges. Key concerns include privacy risks, ethical dilemmas, reducing human error, and the need for comprehensive education on these technologies. AI systems, despite their capabilities, may generate unverifiable inferences and predictions, raising critical legal and regulatory issues. One of the most pressing concerns is the impact of AI on personal data protection. AI can process vast amounts of personal data, sometimes leading to biased or discriminatory decisions. While existing data protection laws are designed to safeguard individuals' privacy, autonomy, and identity particularly the right to privacy many of these regulations remain insufficient in addressing the risks associated with AI-driven technologies.

This thesis aims to explore the intersection of artificial intelligence and social security by analyzing data privacy and security concerns on social media platforms. With the growing use of social media, issues related to data protection have become more prominent. The study examines the effects of AI-driven applications on these concerns and evaluates their role in enhancing or threatening social security. Ethical and legal challenges, technological innovations, and future directions in this field will be assessed. Additionally, the research will discuss the impact of data collection and processing on individual rights, the potential of AI to improve security and privacy, and the importance of developing effective policies for protecting social media users' data.

The study employs discourse analysis as a qualitative research method to identify both the opportunities and challenges associated with using AI to enhance security and protect society. A comprehensive literature review will be conducted, incorporating academic research, official reports, and legal regulations on privacy, social media ethics, and AI governance. Comparisons with previous studies will further support the analysis.

The findings highlight the necessity of education and awareness campaigns to improve public understanding of AI-related security risks. Collaboration between policymakers, technology companies, and users is essential for creating safer digital environments. Furthermore, the research emphasizes the importance of implementing robust policies and legal frameworks to protect online data privacy effectively.

Keywords: Artificial Intelligence, Social Security, Data Privacy, Social Media Platforms

İÇİNDEKİLER

ÖZET ..... **i**
SUMMARY ..... **iii**
İÇİNDEKİLER ..... **v**
KISALTMALAR ..... **ix**
TABLOLAR LİSTESİ ..... **x**
ÖNSÖZ ..... **xii**
GİRİŞ **1**

BİRİNCİ BÖLÜM
LiTERATÜR TARAMASI

1.1. Önceki Çalışmalar 5
1.1.1. Yapay Zekâ Çağında Kişisel Veri .....
1.1.2. Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Öneriler 7
1.1.3. Yapay Zekânın Hukuki Statüsü ve Kişilik Hakkı Kapsamında Değerlendirilmesi 8
1.1.4. Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi 10
1.1.5. Yapay Zekâ Teknolojilerinin Kişisel Verilerin Korunmasına Etkileri, Var olan Problemler ve Çözüm Tavsiyeleri 12
1.1.6. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk 14
1.1.7 Sosyal Medyada Kişisel Verilerin Korunması Sorunu 15
1.2. Önceki Çalışmaların Boşluk Analizi 17
1.2.1. Sosyal ve psikolojik boyutlar 17
1.2.2 Sosyal güvenlik yönü 17
1.2.3 Teknik ve prosedürsel zorluklar 17
1.2.4. Yasal ve etik yön 17
1.2.5 Pratik ve toplumsal uygulamalar 18
1.2.6 Kapsamlı çözümlerin eksikliği 18

İKİNCİ BÖLÜM
YAPAY ZEKÂ VE SOSYAL GÜVENLİK

2.1. Yapay Zekânın Tanımı ve Tarihçesi 20
2.2. Sosyal Güvenliğin Tanımı ve Tarihçesi 29
2.2.1 Çağdaş sosyal güvenlik yapılarının ortaya çıkışı 31
2.2.2 Arap Dünyasındaki Modern Sosyal Güvenlik Sistemleri 32

2.2.3 Yirmi Birinci Yüzyılda Sosyal Güvenlik Sistemlerinin Dijital Dönüşümünün Evrimi 33
2.3. Yapay Zeka Teknolojisinin Sosyal Güvenlik Üzerindeki Etkileri ve Toplumsal Yansımaları 35
2.4. İnsan Güvenliği ve Yapay zekâ İlişkisi: 1994 UN İnsan Güvenliği Raporunun Perspektifinden 37

ÜÇÜNCÜ BÖLÜM
VERİ GİZLİLİĞİ VE GÜVENLİK SORUNLARI

3.1. Veri Gizliliği: Tanımlar ve Kavramlar 40
3.2. Gizlilik Tanımları ve Kavramları 42
3.3. Sosyal Medya Platformlarının Veri Güvenliği ve Veri Gizliliği Üzerindeki Etkisi 43

DÖRDÜNCÜ BÖLÜM
SOSYAL MEDYA PLATFORMLARI:TANIMLAR VE KAVRAMLAR

4.1. Sosyal Medya Platformlarının Tanımı ve Kavramları 45
4.2. Sosyal Medya Platformlarının Özellikleri 46
4.3. Sosyal Medya Türleri ve Örnekleri 47
4.3.1 Facebook'un Sosyal Medya Stratejilerindeki Rolü 47
4.3.2 Twitter'ın sosyal medya platformlarında bilgi aktarımı alanındaki stratejik konumu 48
4.3.4 Instagram'ın Sosyal Medya Yönetimindeki Rolü ve Etkileşim Gücü 48
4.3.5 YouTube'un Sosyal Medya Yönetimindeki Stratejik Kullanımı 49
TikTok'un Sosyal Medya Yönetimindeki Rolü .4.3.6 50
4.4. Sosyal Medya Platformlarinda Veri Gizliliği ve Güvenlik Sorunlarinin Firsatlari ve Zorlukları 50
4.4.1 Yapay zekânın veri analitiğinde sunduğu fırsatlar 50
4.4.2 Yapay zekânın güvenlik sorunlarında ve tehdit algılama sistemlerinde kullanımı 51
4.4.3 Sosyal medya platformlarının veri güvenliği ve kişisel gizlilik düzenlemeleri 54
4.4.3.1. Yerel ve uluslararası veri koruma yasaları 55
4.4.3.2. Sosyal medya platformlarının veri güvenliği ve kişisel gizlilik düzenlemelerine uyması 55
4.4. Veri Gizliliği ve Güvenliği Düzenlemeleri 56
4.4.1. Genel Veri Koruma Y ö netmeliği(GDPR) 56

4.4.2 Kaliforniya Tüketici Gizliliğini Koruma Yasası .(CCPA) 58
4.4.3 . Bilgi güvenliği yönetimi için ISO/IEC 27001 standartları 61
4.5. Yapay Zekânın Etik ve Yasal Boyutları 63
4.5.1. Sosyal medya platformlarında güvenlik politikalarının uygulanması 66
4.6. Sosyal Medya Güvenliği İçin En İyi Uygulamalar 67

BEŞİNCİ BÖLÜM
YAPAY ZEKÂ ALANINDA HÜKÜMET STRATEJİLERİ VE POLİTİKALAR

5.1. Hükümetin Dokümanlarının Analizi 69
5.1.1 ABD'de Yapay zeka alanında araştırma ve geliştirmeye yönelik . ulusal stratejik plan)2023(..... 69
5.1.2 Avrupa Birliği ve .Üye Devletler 72
5.2. Yapay Zekâ Sistemlerinin Yüksek Riskli ve Yasaklanmış Yapay Zekâ Uygulamaları Olarak Sınıflandırılması 73
5.2.1 Genel amaçlı yapay zekâ modelleri 73
5.3. Çin'in Yapay Zekâ Stratejik Öncelikleri 74
5.4. Türkiye'nin 2021-2025 Ulusal Yapay Zekâ Stratejisi 78
5.6. Yapay zekâ alanında Katar Ulusal Stratejisi 79
5.7. Suudi Arabistan'da Yapay Zekâ Stratejileri 80
5.8. Yapay Zekâ Stratejisinin Temel Boyutları 81
5.9. Yapay Zekânın Sosyal Güvenliği Hükümet Belgelerinin Analizinin Bulgularının Özeti ve Tartışılması 82
5.10. Yapay Zekâ Stratejilerinin Analizi 82
5.10.1 Amerika Birleşik Devletleri 82
5.10.2 Avrupa Birliği 82
5.10.3 Çin 83
5.10.4 Türkye 83
5.10.5 Katar 84
5.10.6 Suudi Arabistan Krallığı 84
5.11. Ülkelerin Kapsamlı Karşılaştırması 85
5.11.1 Etik ve yasal yönler 86
5.11.2 Ortak fırsatlar ve zorluklar 87
5.11.3 Sosyal güvenlik boyutları çerçevesinde stratejik yaklaşımlar 87
5.12. Yapay Zekânın Sosyal Güvenlik Bağlamındaki Etkileri Hakkında Örnek Analizi 88
5.13. Yapay Zekânın Sosyal Güvenlik Stratejisi Bulgularının Özeti ve Tartışılması 91
5.14. Yapay Zekâ Çağında Sosyal Güvenliğin Sağlanması İçin Öneriler 93

SONUÇLAR VE ÖNERİLER 95
KAYNAKÇA 101

KISALTMALAR

AI	**:**	Artificial Intelligence
YZ	**:**	Yapay Zekâ
KVKK	**:**	Kişisel Verileri Koruma Kurumu
GPU	**:**	Graphics Processing Unit
SNAPC	**:**	Social Network Analysis for Privacy and Confidentiality
ANN	**:**	Artificial Neural Network
NLP	**:**	Natural Language Processing
CNN	**:**	Convolutional Neural Network
CAN	**:**	Controller Area Network
LLN	**:**	Low-Power and Lossy Networks
GPT-311M	**:**	Generative Pre-trained Transformer 311M
APC	**:**	Advanced Process Control
GDPR	**:**	General Data Protection Regulation
ABD	**:**	Amerika Birleşik Devletleri
RMF	**:**	Risk Management Framework‹
CCPA	**:**	Bulletin Board System
CIA	**:**	California Consumer Privacy Act
EU	**:**	Çok Faktörlü Liderlik Anketi
GDPR	**:**	European Union
ISO/IEC 27001	**:**	The globally recognized framework for information security management
LLM	**:**	Large Language Model
SB 1121	**:**	Senate Bill 1121

TABLOLAR LİSTESİ

Tablo 1. Ülkelerin kapsamlı karşılaştırması..... 85

ÖNSÖZ

Son yıllarda siber güvenlik ve yapay zeka alanları önemli ve önemli gelişmelere sahne oldu. Teknolojik gelişme ve dijital dönüşümün hızlanmasıyla birlikte, sosyal medya platformlarının ve yapay zeka tekniklerinin rolünü incelemek ve sosyal güvenlik üzerindeki etkisinin boyutunu derinlemesine göstermek gerekli hale geldi. Veri gizliliği ve güvenliği konuları, bireysel gizlilik haklarını ciddi şekilde etkileyen sosyal medya platformlarında büyüyen bir endişeye yol açtı ve yapay zekanın bu platformlardaki rolü, sağladığı fırsatlar ve sağladığı zorluklar açısından değerlendirilmelidir. tarafından empoze edildi.

yapay zeka çağında sosyal medya platformlarında sosyal güvenlik kavramının güvenlik ve veri gizliliği konularının analizi yoluyla fırsatları ve zorlukları ortaya çıkarmaktır Bu tezin konusu, yapay zeka çağında sosyal medya platformlarının kullanımının artmasıyla birlikte sosyal güvenlik konularının ele alınmasına yönelik acil ihtiyaçtan doğmuştur. Büyük veri ve algoritmik karar verme mekanizmalarının günlük hayatımıza hızla entegre olması, Veri güvenliği ve mahremiyeti konusunda yeni hukuki ve etik tartışmaları tetikledi

Bu tezin hazırlanması sürecinde değerli rehberlikleri ve destekleri için Türkiye'deki Gelişim Üniversitesi öğretim üyelerine en içten şükranlarımı sunarım. Danışmanım Dr.Öğr.Üyesi Özlem Tuğçe Keleş 'e de değerli tavsiyeleri ve özenli incelemesi için teşekkür ederim. Ulusal Güvenlik Kurumu'na ve Irak İçişleri Bakanlığı ‘na, veri güvenliği konusunda değerli bilgiler sağlamadaki önemli katkıları için derin şükranlarımı sunarım. Onların desteği ve bilgi paylaşımı, bu çalışmayı daha kapsamlı ve gerçekçi hale getirmenin anahtarıydı.

GİRİŞ

Teknolojinin sürekli gelişmesiyle, toplumlar hızlı bir değişim içindedir ve hukuk sistemleri de bu değişimi aynı hızla takip etmek zorundadır. Bununla beraber yapay zekâ üzerine yapılan çalışmalar, Teknolojik yeniliklerin en dikkat çeken unsurlarından biri olarak değerlendirilebilir. Nitekim sanayi devrimiyle hayatımıza giren makinelerin, kendi karar mekanizmalarıyla insan gibi düşünme ve hareket edebilme yeteneklerine sahip olması fikri ürkütücü gelebilir. Ancak bu ilerlemeye, gerekli hukuki altyapının sağlanarak hukuk sistemlerinin hazırlıklı olması sağlanmalıdır.

Veri devrimi ve yapay zeka ve internet teknolojilerinin bir sonucu olarak insanlar sosyal medya platformlarındaki özel hayatları hakkındaki bilgiler, bireyler ve hizmet sağlayıcılar için izin verilebilir bir ortam halini almıştır., dev internet ve iletişim şirketleri, hükümetler ve onların istihbarat ve bilgi servisleri için de meydana geldi. Daha sonra kitlesel casusluk, veri paylaşımı, dijital mahremiyet ve pazarlamanın, sosyal, politik, ticari, mesleki ve kişisel ihlalleri yaygınlaştı. (Saad A. M., 2021, p. 9)

Yapay zekâ tarafından sunulan yararlar ve zorlukların çeşitli yönlerinin ayrıntılı bir şekilde incelenmesini hedeflemektedir. Ayrıca, bu tez ile daha önceki çalışmaların sonuçlarını entegre bir şekilde karşılaştırarak detaylı bir sonuca ulaşılmasını sağlayacaktır.

Çalışmanın ilk kısmında, yapay zekâ tanımlanacak ve elli yıl öncesinden günümüze kadar gerçekleşen gelişmelerin geçmişi incelenecek. Sosyal güvenlik üzerinde yapay zekânın genel etkileri gözden geçirilirken, büyük verilerin analiz edilmesi yoluyla hedef grupların nasıl doğru bir şekilde belirleneceği ve sosyal hizmetlerde sunulan verimliliğin artırılabileceği, Birleşmiş Milletler İnsan Güvenliği Raporu 1994 perspektifinden, daha sonrasında ise yapay zekânın insan güvenliğinin yedi boyutunu nasıl etkileyebileceği gözden geçirilecek ve bu konuda insanların güvende olması ile yapay zekâ arasındaki ilişki tartışılacak.

İkinci bölümde, Sosyal medya platformlarında veri gizliliği ve güvenliği ile birlikte mahremiyetin tanımı ve ilgili kavramları tartışmaya devam edilecek. Yapay zekâda Veri koleksiyonu ve işleme yöntemleriyle, bu zaman diliminden kaynaklı veri güvenliği tehditleri ve gizlilik ihlalleri üzerinde bir değerlendirme yapılacak. Bununla beraber, ayrımcılığın ve algoritma tabanlı önyargıların ortaya çıkarabileceği dengesiz veri kullanımının sosyal güvenliği nasıl etkilediği de ayrıca ele alınacak.

Üçüncü bölümde, sosyal medya platformları kavramı tanımlanarak, türleri ve avantajları belirlenerek tanıtılacaktır. Yapay zekânın sunduğu fırsatları incelemek için, sosyal medya platformları ve veri analizinin yanı sıra tehdit tespit sistemlerinde ve güvenlik uygulamalarında da kullanılması düşünülebilir. Sosyal medya platformlarında kullanıcı deneyimini nasıl iyileştirebileceğini araştırmak için yapay zekâ çözümlerine ve kişisel veri koruma teknolojilerindeki yeniliklere odaklanılacak. Yapay zekânın yasal ve etik boyutlarındaki zorluklar üzerine tartışılacağı gibi, veri gizliliği ve güvenlik düzenlemelerini de değerlendirilecek. Sosyal medya platformlarında, güvenlik politikalarının uygulamaya konmasıyla ilgili olarak yapay zekâ araçlarını güvenli bir şekilde kullanma ve kullanıcıların verilerini koruma yöntemleri tartışılacak.

Dördüncü bölümde, 18 hükümetin uyguladığı stratejiler belgeleri ile analiz edilerek, zorluklar ve insan güvenliğinin yedi boyutu altındaki farklı stratejik yönlere dair bir inceleme yapılacaktır. Yapay zekâ çağında sosyal güvenliği sağlamak için önerilerde bulunulacak, mevcut politikaların karşılaşabileceği zorlukların üstesinden gelme ve nasıl iyileştirilebileceği değerlendirilecektir.

Son olarak, Sosyal medyada kişisel veri koruma ve güvenliğine dair önemli konulara odaklanarak, hızla değişen bu çağda, sosyal güvenliği geliştirmek için önerilerde bulunarak, yapay zekânın sosyal güvenlik üzerindeki etkisine ilişkin kapsamlı ve derinlemesine bir görünüm sağlamayı amaçlamaktadır.

Tezin Amacı

Yapay zekâ çağında sosyal güvenlik kavramının sosyal medya platformlarındaki güvenlik sorunları ve veri gizliliğinin analizini yaparak, fırsatları ve zorlukları ortaya koymaktır. Sosyal medya platformlarının daha yaygın hale gelmesiyle birlikte, güvenlik ve veri koruma sorunları giderek daha fazla önem kazanmaktadır, Bu konuda yapay zekâ uygulamalarının etkisi de ele alınarak, sosyal güvenlik açısından yapay zekânın rolü incelenecektir. Bu incelemeler için aşağıdaki hususlara odaklanılabilir:

- Sosyal güvenliği artırmak için, yapay zeka kullanımının avantajları ve zorlukları analiz edilerek teknolojinin etkili bir şekilde uygulanması üzerine çalışmalar yapılmaktadır.

- Sosyal medya platformlarında yapay zekâ teknolojisinin kullanma şeklini anlamak ve bu kullanımın sunabileceği yararları ile karşılaşabilecek zorlukları değerlendirmektir.
- Bu teknolojinin kullanım imkanlarını açıklamak ve yapay zekâ çağında sosyal güvenliğin karşılaştığı zorlukları ortaya çıkarmaktır.
- Sosyal medya platformlarında güvenlik sorunları ve veri gizliliğinin analiz edilmesi, bu çerçevede yapay zekânın sunabileceği potansiyel çözümleri ve olası engelleri belirlemeyi amaçlamaktadır.
- Toplumdaki algının yapay zekâya olan etkisini ve güvenlik ile veri gizliliğine dair farkındalığı incelemektir.

Tezin Önemi

Yapay zekâ çağında sosyal güvenliğin dinamiklerini anlamak için bu tez önemli katkılara sahiptir. Sosyal medyanın sürekli kullanımı ve buna bağlı olarak işlenen büyük veri miktarı, güvenlik sorunları ve veri gizliliğini temel bir konu haline getiriyor. Tezin önemi şu temel noktalarda vurgulanabilir:

- Veri Gizliliği ve Güvenlik:

Veri güvenliği ve gizliliği konularında farkındalık yaratmayı hedefleyerek sosyal medya platformlarında kullanıcı verilerinin nasıl toplandığı, işlendiği ve saklandığıyla ilgili detaylı bir analiz sunmaktadır. Bu nedenle, kullanıcıların kişisel bilgilerini güvenli bir şekilde korumak için mevcut yasal düzenlemeler ve uygulamalar incelenecektir.

- Yapay Zekâ ve Sosyal Güvenliği:

İnsan güvenliğinin yedi boyutunu (politik, ekonomik, gıda, çevresel, toplumsal, sağlık ve kişisel) analiz ederek, Yapay zekanın insan güvenliği üzerindeki etkilerini hem olumlu hem de olumsuz sonuçlarını inceleyerek araştıracak.

- Fırsatlar ve Zorluklar:

Sosyal medya platformlarının sunduğu fırsatlar ve karşılaştığı sorunlar detaylı olarak incelenecektir. Yapay zekâ teknolojilerinin sosyal medya platformlarında nasıl uygulanabileceğini, bu uygulamanın toplum ve özelinde kullanıcılar üzerindeki etkisini analiz edecektir.

- Politik ve Stratejik Öneriler:

Politika yapıcıları ve strateji geliştirenleri yapay zekâ ve sosyal güvenlik konularında yönlendirmektir. Yapay zekâ, veri güvenliği ve gizliliğiyle ilgili öneriler sunarak dijital ortamın daha adil ve güvende olmasına yardımcı olacaktır.

Tezin Yöntemi

Analizin temel amacı yapay Zekâ Çağında Sosyal Güvenlik, Sosyal Medya Platformlarında Veri Gizliliği ve Güvenlik Sorunları, Fırsatlar ve Zorluklar'dır. Bununla birlikte söylem analizi yöntemi ile sosyal medya platformlarının kullanıcı sözleşmeleri önerisi incelenecektir.

- **Varsayımlar**

Sosyal medya platformları veri güvenliği açısından güvenli olduklarını iddia etseler de veri işleme konusunda güvenli değil.

- **Sınırlılıklar**

Çalışmanın sınırlılıkları, yapay zekâ teknolojisinin sosyal medya platformlarında kullanımının yeni olması ve henüz tam olarak anlaşılmamış olmasıdır. Ayrıca, sosyal etik ve siyasi sonuçları öngörmek zor olabilir.

- **Veri Toplama Tekniği**

Nitel araştırma yöntemi olarak söylem analizi yapılacaktır.

BİRİNCİ BÖLÜM

LITERATÜR TARAMASI

1.1. Önceki Çalışmalar

Önceki çalışmalar, genel olarak yapay zeka ve sosyal medya arasındaki ilişkiyi incelemiş, ancak sosyal güvenlik boyutuna sınırlı bir şekilde değinmiştir. Bu tez çalışması, veri gizliliği ve güvenliği konuları çerçevesinde sosyal güvenlik konularına odaklanarak literatüre katkı sağlamayı amaçlamaktadır. Aşağıda tezime katkıda bulunan çalışmaların yönleri yer almaktadır.

1.1.1. Yapay Zekâ Çağında Kişisel Veri

Araştırmanın Özeti

Yapay Zekâ (YZ) teknolojisinin gelişimini ve üç temel kategoriye ayrılmasını ele almaktadır: Dar Yapay Zekâ, Genel Yapay Zekâ ve Süper Zekâ. Son yıllarda YZ mantık, etik, hukuk, ekonomi ve sanat gibi birçok alanda kapsamlı araştırmaların konusu hâline gelmiştir. Ancak bu teknolojilerin gelişimi, özellikle veri gizliliği ve güvenliği açısından birçok etik ve hukuki sorunu beraberinde getirmektedir. YZ sistemleri büyük ölçüde kişisel verilere dayanmaktadır ve bu verilerin toplanması, işlenmesi ve depolanması süreçleri giderek daha kritik bir hâle gelmektedir. Kişisel verilerin işlenmesiyle ilgili ulusal ve uluslararası düzenlemeler yapılmış olsa da YZ teknolojilerinin hızla ilerlemesi, mevcut yasal çerçevelerin yetersiz kalmasına neden olmaktadır. bu araştırma, YZ'nın mahremiyet kavramıyla ilişkisini, bireylerin kişisel verilerine yönelik riskleri ve bu riskleri azaltmaya yönelik çözüm önerilerini incelemektedir. Araştırmada nitel araştırma yöntemi kullanılmış, literatür taraması yapılmış ve kavramlar akademik çerçevede değerlendirilmiştir.

Yazarlar: Hüseyin Ensari. (Ensari, 2023, p. 6)

Araştırmanın Amacı

Bu araştırmanın temel amaçları şunlardır:

- YZ'nın geliştirilme süreçlerinde ortaya çıkan veri gizliliği risklerini belirlemek,
- Kişisel verilerin, bireylerin bilgisi veya farkında olmadan verdikleri izinler aracılığıyla bulut teknolojisinde toplanmasını ve depolanmasını analiz etmek,

- YZ’nın bu verileri kullanarak gelişmesi ortaya çıkabilecek hukuki ve etik sorunları ele almak,
- Veri mahremiyetinin korunmasına yönelik öneriler sunmak ve sosyal bilimcileri bu konuda bilinçlendirmek.

Literatür Taraması ve Tez ile İlişkisi

Sanayi Devrimiyle birlikte önce şehirler kalabalıklaştı. Ardından insanlar kalabalıklar içerisinde yalnızlaşmaya başladı. Her yalnızlaşma bireyselleşmeyi ve bireye ait kavramların şekillenmesine neden oldu. Ancak günümüzde mahremiyet kavramı kişinin kendine ait bir odaya sahip olması anlamına geliyor İletişimlerinin gizliliği kalabalığın içinde anonim bir figür olarak kalmanın ötesine geçiyordu. George Orwell'in 1984 adlı eserinde betimlediği türde bir yaşamı engellemek amacıyla, yapay zekânın bireylerin gizliliğini ihlal etmeden nasıl kontrol altında geliştirilebileceği giderek daha fazla önem kazanmaktadı. (Ensari, 2023, p. 16)

Araştırma, yapay zekâ gelişmeleriyle veri gizliliği arasındaki ilişkiyi hukuki ve teknik boyutlara odaklanarak ele alıyor ve yapay zekânın gizliliği tehdit eden ek bir faktör haline geldiğini gösteriyor. Dolayısıyla bu araştırma, gizlilik konularının netleştirilmesi açısından tezi destekliyor. Sadece teknik yönüyle ilgili değil, bunun da ötesine geçerek sosyal medya platformlarındaki bireylerin sosyal güvenliğini etkiliyor.

Bulguların Özeti

Günümüzde kişisel verilerin korunmasına yönelik yeterli ve güncel yasal çerçevelerin bulunmadığını ortaya koymuştur. Mevcut düzenlemelerin, veri toplama ve analiz yöntemlerindeki hızlı gelişmelere ayak uyduramadığı, bunun da bireysel mahremiyeti tehdit ettiği vurgulanmaktadır.

Boşluk Analizi

Kişisel verilerin korunmasını ağırlıklı olarak hukuki ve teknik yönleriyle ele almıştır. Ancak, bu sürecin bireyler üzerindeki sosyal ve psikolojik etkileri detaylı bir şekilde incelenmemiştir.

Tezimin katkısı, bu boşluğu doldurarak sosyal medya platformlarında yapay zekâ ve veri güvenliği konusunun bireylerin sosyal güvenliği üzerindeki etkilerini analiz etmektir.

1.1.2. Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Öneriler

Araştırmanın Özeti

Günümüzde yapay zekâ teknolojisi bireylerin özel hayatları, davranışları ve tercihleri hakkında çeşitli yöntemlerle veri toplayarak doğruluğu kesinleşmemiş çıkarımlarda bulunabilmesi ve bu sürecin veri güvenliği, mahremiyet ve hukuki düzenlemeler açısından doğurduğu riskleri ele almaktadır. Yapay zekâ teknolojileri, kişisel verilerin korunması kapsamında önemli sorunlara yol açmakta ve bireylerin onaylarına dayanarak çeşitli verileri işleyerek önyargılı, ayrımcı ve müdahaleci kararlar alabilmektedir. Mevcut kişisel verilerin korunması yasaları, bireylerin mahremiyetini ve kimlik haklarını güvence altına almak amacıyla düzenlenmiş olsa da yapay zekâ teknolojilerinin hızla gelişmesi, bu yasal düzenlemelerin yetersiz kalmasına neden olmaktadır. Bu çalışma, yapay zekâ uygulamalarının kişisel veri güvenliğini nasıl tehdit ettiğini incelemekte ve bu tehditlere karşı olası çözüm önerileri sunmayı amaçlamaktadır. Çalışma, nitel bir araştırma yöntemi kullanılarak gerçekleştirilmiştir. Bulgular, yapay zekânın gelişimi ile birlikte kişisel verilere yönelik ihlallerin niteliğinin değiştiğini, kişisel haklar ve mahremiyet ile ilgili risklerin arttığını göstermektedir. Hassas ve hassas olmayan veriler arasındaki farkların giderek azaldığı, yapay zekânın veri işleme süreçlerinde şeffaflık ve hesap verebilirlik sorunlarının devam ettiği vurgulanmaktadır.

Yazarlar: **Yiliyaer** Abudureyimu. (Abudureyimu, 2021, p. 766)

Araştırmanın Amacı

Yapay zekâ uygulamalarının kişisel verilerin korunmasına yönelik oluşturduğu riskleri belirlemek ve bu riskleri azaltmaya yönelik öneriler geliştirmektir. Çalışma, yapay zekânın veri toplama, işleme ve sonuç üretme süreçlerinde ortaya çıkan hukuki ve etik sorunları analiz etmeyi hedeflemektedir.

Literatür Taraması ve Tez ile İlişkisi

Yapay zeka çağında kişisel verilerin korunmasına yönelik düzenlemeler, iki temel kategori altında incelenebilir. İlk kategoriyi oluşturan Kıta Avrupası Hukuk Sistemi, kişisel verilere sosyal ve insan odaklı bir perspektifle yaklaşarak, bu verileri bireyin kişilik hakları ve temel insan hakları kapsamında değerlendirir. Bu yaklaşımda, kişisel veriler anayasal düzeyde bir insan hakkı olarak tanımlansa bile, koruma altına

alınan asıl değerin bireyin özel yaşamının gizliliği (mahremiyet) olduğu vurgulanmaktadır . (Abudureyimu, 2021, p. 769)

Yapay zekâ teknolojisindeki gelişmelerin büyük ölçüde kişisel verilere dayandığını ve bu verilerin nasıl toplandığını gösteren bir faktör haline geldiğini gösteriyor. Dolayısıyla bu araştırma, kişisel verilerin gizlilik konularının netleştirilmesi açısından tezi destekliyor. Gizlilik konularının işlenmesini düzenlemeye yönelik çok sayıda ulusal ve uluslararası mevzuat bulunmasına rağmen, yapay zekâ sistemlerinin gelişim süreçlerinin kontrol edilememesi, Bu koşullar altında, giderek artan zorlukları aşmak adına mevzuatın yetersizliği dikkat çekiyor

Bulguların Özeti

Yapay zekâ uygulamalarının kişisel verileri korumak için gerekli güvenlik önlemlerinin yetersiz olduğunu bireysel mahremiyete yönelik ciddi tehdit oluşturduğu ortaya çıkmaktadır. Yapay zekâ algoritmalarının kara kutu problemi, şeffaflık eksikliği, önyargılı ve ayrımcı kararlar alma riski gibi kritik sorunları devam etmektedir. Ayrıca, kişisel verilerin ihlal edilmesi durumunda delil elde etmenin teknik olarak zor olması ve yüksek maliyet gerektirmesi, hukuk sistemlerinin bu ihlalleri tespit ve kontrol etmesini zorlaştırmaktadır.

Boşluk Analizi

Yapay zekâ teknolojilerinin kişisel verilerin korunması üzerindeki hukuki ve teknik etkilerini detaylı bir şekilde incelemiş olsa da, veri ihlallerinin bireyler üzerindeki sosyal ve psikolojik etkileri yeterince ele alınmamıştır. Tezin katkısı, bu boşluğu doldurarak, sosyal medya platformlarında yapay zekâ destekli veri güvenliği süreçlerinin bireylerin sosyal güvenliği üzerindeki etkilerini analiz etmek ve bu bağlamda öneriler geliştirmektir.

1.1.3. Yapay Zekânın Hukuki Statüsü ve Kişilik Hakkı Kapsamında Değerlendirilmesi

Araştırmanın Özeti

Yapay zekâ teknolojisindeki hızlı gelişmeler, sadece teknik alanlarda değil, hukuk ve insan hakları gibi alanlarda da önemli tartışmalara yol açmıştır. Hukuki açıdan bakıldığında, yapay zekâya kişilik özellikleri tanınıp tanınamayacağı ve bu bağlamda hangi hukuki statüye sahip olacağı önemli bir soru olarak karşımıza çıkmaktadır. Eğer

yapay zekâ varlıklarına bir tür kişilik tanınacaksa, bu kişiliğin kapsamı ve sınırları belirlenmelidir. Bu çalışma, yapay zekâ kavramını ve medeni hukukta kişilik kavramını inceleyerek, yapay zekânın hukuki statüsü üzerine geliştirilen kişilik modellerini ele almaktadır. Özellikle elektronik kişilik modeli öne çıkmakta olup, bu modelin avantajları ve eksiklikleri değerlendirilmiştir. Yapay zekâya kişilik tanınması hangi haklara sahip olabileceği ve hangi sorumluluklarla karşı karşıya kalacağı çalışmanın temel konusunu oluşturmaktadır.

Yazarlar: Ahmet Said BER. (Ber, 2022, p. 57)

Araştırmanın Amacı

Yapay zekânın yasal statüsünü ve kişilik hakları çerçevesinde nasıl değerlendirilebileceğini ortaya koymayı amaçlamaktadır. Yapay zekâ varlıklarının hukuki kişiliğe sahip olup olmayacağı, sahip olursa hangi hak ve sorumluluklara tabi olacağı gibi sorulara yanıt aranmaktadır. Ayrıca, bu tür bir hukuki statünün bireylerin kişilik hakları ve sosyal güvenlik üzerindeki etkilerini de ele almaktadır.

Literatür Taraması ve Tez ile İlişkisi

Önerilen kişilik modellerinin bu mevzuat kapsamında incelendiğinde, elektronik kişilik modeli önemli bir çözüm olarak dikkat çekmektedir. Ancak, şu an için genel çerçevede sunulan bu modelde doldurulması gereken önemli eksiklikler mevcuttur. Sicil ve sigorta sistemlerinde yapılan iyileştirmelerle belirsizlikler kısmen azaltılsa da hukuki işlemler ve sorumluluk konuları öncelikli olarak ele alınmalıdır. Yapay zekânın küresel kullanımı ve uluslararası etkisi göz önüne alındığında, yalnızca ulusal hukuk kurallarının geliştirilmesi yeterli olmayacak, aynı zamanda uluslararası anlaşmalar racılığıyla hukuki uyum sağlanması kritik önem taşımaktadır. (Ber, 2022, p. 94)

Yapay zekâ kavramına ve medeni hukukta kişilik kavramına genel bir bakış açısından incelenmekte, yapay zekânın tüzel kişiliği sorununa odaklanmaktadır. Dolayısıyla bu araştırma, yapay zekânın hukuki statüsünü ve bireylerin kişilik hakları ve sosyal güvenlik üzerindeki etkilerini açıklığa kavuşturması açısından tezi desteklemektedir. Özellikle sosyal medya platformlarında yapay zekânın gelişmesiyle, İnsan haklarını güvence altına almak için zorunlu olan tüm hukuki düzenlemeler kapsamlı bir şekilde incelenmektedir.

Bulguların Özeti

Yapay zekâ teknolojilerinin gelişmesiyle birlikte yeni hukuki çerçevelere duyulan ihtiyacı vurgulamaktadır. Bireylerin kişisel hakları ve sosyal güvenlikleri açısından risk oluşturan yapay zekanın yol açtığı insan hakları ihlallerine yönelik mevcut hukuk sistemleri kapsamlı çözümler üretememektedir. Elektronik kişilik modeli, yapay zekâlar için hukuki bir çerçeve sunma konusunda umut vaat etse de hukuki boşluklar ve uygulama zorlukları nedeniyle henüz tam anlamıyla işler hâle getirilememiştir.

Boşluk Analizi

Yapay zekânın hukuki yönlerine ağırlık vermekte ancak toplumsal etkilerini yeterince ele almamaktadır. Yapay zekâların pratik kullanımları, etik boyutu ve sosyal sonuçları gibi konulara daha fazla odaklanılması gerekmektedir. Tezin katkısı, bu boşluğu doldurarak, yapay zekânın sosyal medya platformlarında bireylerin hakları ve sosyal güvenlik üzerindeki etkilerini analiz etmeyi amaçlamaktadır. Böylece hem hukuki hem de toplumsal boyutları içeren kapsamlı bir değerlendirme sunulacaktır.

1.1.4. Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi

Araştırmanın Özeti

Günümüzde siber risklerin değişen yapısı, analitik ve yapay zekâ uygulamalarıyla kişisel verilerin işlenmesinin yaygınlaşması, sektörel düzenlemelerin artması ve veri işleme ortamlarının çeşitlenmesi, geleneksel veri koruma yaklaşımlarının yetersiz kalmasına neden olmuştur. Bu bağlamda, veri koruma ve mahremiyet konularında ortaya çıkan yeni riskler ve sorunlar karşısında hesap verebilirlik ilkesi etkin bir çözüm olarak öne çıkmaktadır. Hesap verebilirlik ilkesi sadece mevzuata uyum sağlamaktan öte, veri sorumlularının kişisel verilerin korunmasına yönelik uygun ve etkin tedbirleri almasını ve gerektiğinde bunu ispat etmesini zorunlu kılan bir paradigma değişikliğini ifade etmektedir. Bu ilke, veri sorumlularının mahremiyet yönetim süreçlerini sürekli gözetmelerini, etkin bir şekilde uygulamalarını ve düzenli olarak denetlemelerini gerektirmektedir. Bu çalışmanın amacı, hesap verebilirlik ilkesini veri koruma hukuku kapsamında karşılaştırmalı bir şekilde incelemek, ilkenin temelini ve kapsamını açıklığa kavuşturmak, diğer veri koruma ilkeleriyle ilişkisini belirlemek ve veri sorumluları ile veri işleyenler üzerindeki normatif etkisini analiz etmektir.

Yazarlar: Mehmet Bedii Kaya. (Kaya, 2021, p. 1860)

Araştırmanın Amacı

Hesap verebilirlik ilkesinin kişisel verilerin korunmasındaki rolünü derinlemesine incelemek ve bu ilkenin veri koruma hukukundaki konumunu netleştirmektir. Araştırma kapsamında, hesap verebilirlik ilkesinin:

- Temel yapısı ve kapsamı,
- Diğer veri koruma ilkeleriyle ilişkisi,
- Veri sorumluları ve veri işleyenler üzerindeki normatif etkisi

Literatür Taraması ve Tez ile İlişkisi

Veri sorumlusu, gizlilik uyum programını etkin bir biçimde sürdürmeli ve yetkili veri koruma kurumunun talebi halinde bu programı sunuma hazır bulundurmalıdır. Bu program yerel yasal düzenlemeler, uluslararası taahhütler, sözleşmeye dayalı şartlar ve özdenetim mekanizmalarını kapsamalıdır. Veri sorumlusunun bir diğer kritik sorumluluğu ise, kişisel verileri önemli ölçüde etkileyen bir güvenlik ihlali yaşanması ilgili otoriteleri derhal bilgilendirmektir. İhlalin veri sahiplerinin haklarını riske atma potansiyeli varsa, veri sorumlusu aynı zamanda etkilenen bireylere açıklamakla yükümlüdür.(Kaya, 2021, p. 1867)

yapay zekâdaki gelişmeler ve hesap verebilirlik ilkesi arasındaki ilişkiyi inceleyerek yeni riskler ile zorluklar karşısında etkili bir çözüm olduğu kanıtlandı. Bu araştırma, hesap verebilirlik ilkesinin veri denetleyicilerinin yasalara veya düzenlemelere uymak için etkili ve uygun önlemler almasını gerektirdiğinden, veri korumada önemli bir değişikliği belirtir. Bu nedenle bu araştırma, veri sorumluları ve işleyicileri bağlamında hesap verebilirlik ilkesi aracılığıyla yapay zekânın sosyal güvenliği iyileştirmedeki zorluklarını ve fırsatlarını açıklığa kavuşturmak açısından tezi desteklemektedir. Sadece teknik tarafı etkilemiyor, aynı zamanda sosyal güvenliği de etkiliyor.

Bulguların Özeti

Hesap verebilirlik ilkesinin benimsenmesinin yapay zekâ destekli sistemlerde kişisel verilerin korunmasını önemli ölçüde artırabileceğini göstermektedir.

- Yapay zekâ sistemlerinde karar alma süreçlerinin şeffaf olmaması, veri sahiplerinin haklarının ihlal edilmesine yol açabilmektedir. Ancak hesap

verebilirlik ilkesi, veri sorumlularını karar alma mekanizmalarına ilişkin daha fazla bilgi paylaşmaya zorlayarak, bireylerin haklarını koruma noktasında önemli bir güvence sağlamaktadır.

- Veri işleme süreçlerinin şeffaf hâle getirilmesi, veri güvenliği düzenlemelerinin etkinliğini artırmakta ve veri ihlallerinin önüne geçilmesine katkıda bulunmaktadır.
- Yapay zekâ teknolojilerinin karar alma süreçlerinde hesap verebilirliğin sağlanması, algoritmik önyargılar ve ayrımcılık risklerini azaltmaktadır.

Boşluk Analizi

Hesap verebilirlik ilkesinin düzenleyici ve yasama yönlerine odaklanmış olmakla birlikte, ilkenin uygulanmasına ilişkin teknik zorlukları yeterince ele almamaktadır. Özellikle, yapay zekâ sistemlerinin hesap verebilir olmasını sağlayacak teknik mekanizmalar ve uygulamalar hakkında daha fazla araştırmaya ihtiyaç duyulmaktadır.

Bu eksiklik, Tezin katkısı alanı sunmaktadır. Hesap verebilirlik ilkesi, yalnızca düzenleyici çerçeveyle değil, aynı zamanda teknik ve sosyal güvenlik boyutlarıyla da ele alınmalıdır. Bu bağlamda, sosyal medya platformlarındaki veri güvenliği süreçlerinde hesap verebilirlik ilkesinin nasıl daha etkili hâle getirilebileceği konusunda yeni öneriler geliştirmek,

1.1.5. Yapay Zekâ Teknolojilerinin Kişisel Verilerin Korunmasına Etkileri, Var olan Problemler ve Çözüm Tavsiyeleri

Araştırmanın Özeti:

Teknolojinin hızla gelişmesinin, kişisel verilerin gizliliğini tehdit etmek ve bireylerin şeref ve haysiyetine dayalı yaşam hakları ile özgürlüklerini ihlal etmek gibi dezavantajlara yol açtığını göstermektedir. Özel hayatın gizliliği, insanların en temel haklarından biri olup, bu hak günümüz teknolojileri ile farklı bir boyut kazanmıştır. Yapay Zekâ (YZ) gibi teknolojilerin gelişimi, kişisel verilerin kontrolünün her geçen gün kaybolmasına neden olmakta ve bu sorun ciddi bir veri koruma ihtiyacı doğurmaktadır. Yapay zekâ, derin öğrenme ve makine öğrenme sistemleri gibi yöntemlerle verileri saklama, işleme ve analiz etme gibi işlemleri çok hızlı bir şekilde gerçekleştirebilmekte, ancak şeffaflık ve hesap verebilirlik gibi teknik dezavantajları da beraberinde getirmektedir. YZ sistemlerinin kullanımıyla kişisel verilerin

korunması ilke ve kurallarına aykırı veri işleme faaliyetleri gerçekleşebilir, mevcut düzenlemelerin, hızla gelişen YZ sistemlerine karşı yetersiz kaldığını ve veri koruma prosedürlerinin henüz yeterli olmadığını vurgulamaktadır. Çözüm önerileri, YZ sistemlerinin şeffaflık ve hesap verebilirlik ilkesine uygun hale getirilmesini ve gelişen teknolojiler karşısında mevcut düzenlemelerin güçlendirilmesini içermektedir.

Yazarlar: Zeynep Öğretmen Kotil. (Kotil, 2022, p. 15)

Araştırmanın Amacı

Yapay zekâ tekniklerinin kişisel verilerin korunmasına etkisini araştırmayı ve bu alandaki mevcut sorunlara çözüm önerileri sunmayı amaçlamaktadır.

Literatür Taraması ve Tez ile İlişkisi

Yalnızca hukuki düzenlemelerin bireyleri korumak, belirli bir alanı regüle etmek veya bu kuralların etkin bir şekilde uygulanmasını sağlamak için yetersiz kaldığı açıktır. Bu süreçte kültürel değerler ve siyasi yönetim dinamikleri de belirleyici faktörler olarak öne çıkmaktadır. Bağlayıcı nitelik taşıyan hukuki düzenlemeler, ilgili konunun kamuoyu gündeminde kalmasını temin edebilir ve uyumu artırmak amacıyla çeşitli teşvik mekanizmalarının devreye alınmasına katkıda bulunabilir. (Kotil, 2022, p. 216)

Kişisel verilerin hukuka uygun olarak korunması genel düzenlemeler ve hükümler kapsamında hukuki sorumluluk şartları incelenmiş ve sosyal güvenlik ilkelerinin uygulanması söz konusu olup, bu araştırma, yasal düzenlemeler, karar verme ve yargı görüşleri açısından bir tezi desteklemekte ve yapay zekâ sistemlerinin sosyal iletişim platformlarında karşılaştığı güncel sorunları ele alan çözümler bulmaktadır.

Bulguların Özeti

YZ sistemlerinin kullanımında kişisel verilerin korunmasına yönelik politikaların önemli eksiklikler taşıdığını ve bu eksikliklerin düzenlemeler ile giderilmesi gerektiğini ortaya koymaktadır.

Boşluk Analizi

Sosyal ve psikolojik etkileri yeterince ele almadan yalnızca teknik sorunlar ve çözüm önerileri üzerinde durmaktadır. Bu nedenle, sosyal ve psikolojik etkilerin incelenmesi konusunda eksiklikler bulunmaktadır.

1.1.6. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk

Araştırmanın Özeti:

YZ sistemlerine karşı kişisel verilerin nasıl korunacağı, YZ sistemlerinin hangi nedenlerle bu yükümlülüklerden vazgeçebileceği ve bu vazgeçmelerden meydana gelen hukuki sonuçlar değerlendirilmiştir. Bu değerlendirme üç bölüm halinde olup birinci bölümde kişisel veri ifadesinin tanımlanmasıyla birlikte kişisel verilerin neden korunması gerektiği ve bu korunum ile ilgili prosedürlerin gelişim süreci değerlendirilirken 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile bu kanun hazırlanırken esas alınan ilgili mevzuatın 95/46/AT Sayılı Maddesi ve bu maddeyi yok sayan Avrupa Veri Koruma Tüzüğü karşılaştırılmıştır. İkinci bölümde Kişisel Verilerin Korunması ile ilgili önemli terimlere değinilmiş ve veri ihlalinin nasıl gerçekleştiği açıklanmıştır. Son bölümde ise Kişisel Verilerin Korunması Kanunu'nda yer alan prosedürlerle birlikte bunların ihlalinden doğan hukuki süreçler incelenmiştir. Yine bireylerin bu tip bir hak ihlali izlemesi gereken hukuki yollar bu bölüm içerisinde açıklanmaya çalışılmıştır.

Yazarlar Kemal Küçük kavruk .(Küçükkavruk, 2023, p. 7)

Araştırmanın Amacı

Kişisel verilerin korunmasının ihlalinden kaynaklanan hukuki sorumluluğu tartışmayı amaçlamaktadır.

Literatür Taraması ve Tez ile İlişkisi

İdari tedbirlerin temel hedefi, ilgili bireylerin bilinçlenmesini sağlayarak alternatif bir perspektif geliştirmek ve bu sayede olası hatalar ile veri ihlallerini önlemektir. Aynı zamanda, veri sızıntılarını en kısa sürede tespit ederek denetim ve güvenlik sistemlerini aktif hale getirmeyi amaçlar. Veri ihlallerini risk değerlendirmesi yoluyla engelleme çabaları, yönetsel önlemler kapsamında değerlendirilir. Üçüncü tarafların veya veri sorumlusu kontrolündeki yetkisiz personelin önceden kaydedilmiş verilere erişimini sınırlandırmak ise teknolojik önlemlere dayanır. Bu bağlamda, bilişim altyapısındaki açıkları azaltmada teknolojik düzenlemelerin etkinliği vurgulanmalıdır. (Küçükkavruk, 2023, p. 61)

Veri korumada önemli bir değişim olduğunu göstermekte ve ilgili mevzuattaki gelişmeleri gözden geçirmektedir. Bu nedenle bu araştırma, idari prosedürler

açısından olası bir hatayı önlemek ve insanları eğiterek ve sayısını artırarak veri sızıntısını önlemek tezini desteklemektedir. Ayrıca mevcut yargı kararlarını ve farklı yazarlı görüşleri gözden geçirir, yasal dayanakları ve mevcut yasal yöntemleri analiz eder.

Bulguların Özeti

Yapay zekâ teknolojilerinin hızla gelişmesiyle birlikte kişisel verilerin korunmasını sağlayacak daha katı yasal düzenlemelere duyulan ihtiyacı vurgulamaktadır.

Boşluk Analizi

Genellikle yasal yönlere odaklanmakta olup, veri korumasının iyileştirilmesi için teknik ve prosedürel çözümler üzerine bir tartışma sunmamaktadır. Bu eksiklik, veri güvenliği alanındaki iyileştirmelere dair öneri ve çözümlerin eksik kaldığını göstermektedir.

1.1.7. Sosyal Medyada Kişisel Verilerin Korunması Sorunu

Araştırmanın Özeti

Sosyal medya, bireylerin yaşamında önemli bir yer tutan ve toplumsal etkileşimi şekillendiren, bireyi pek çok yönden etkileyen güçlü bir araç hâline gelmiştir. Sosyal medya platformları, kullanıcıların kişisel verilerini toplamakta, işlemek ve üçüncü taraflarla paylaşmak suretiyle çıkar sağlamaktadır. Bu süreçte bireyler, çoğu zaman kendi özel yaşamlarına dair pek çok veriyi ya gönüllü olarak ya da bilgi eksikliğiyle paylaşmaktadır. Günümüzde mahremiyetin giderek yok olduğu ve hiçbir şeyin gizli kalamayacağı görüşleri öne çıkmaktadır. Bu araştırmanın amacı, sosyal medyada kişisel verilerin bireyler için oluşturduğu riskleri ve bu verilerin kullanılması halinde toplumu etkileyecek sorunları belirlemektir. Ayrıca yalnızca yasal düzenlemelerin bu sorunları çözmede yeterli olmayacağı savunulmuş ve felsefi-etik bir yaklaşımın önemine vurgu yapılmıştır. Araştırma üç ana bölümden oluşmaktadır. İlk bölümde kişisel verilerin korunması hakkının tarihsel süreci ele alınmış, bu hakkın diğer temel haklarla ilişkisi açıklanmış ve kişisel verilerin korunmasına yönelik hukuki düzenlemelere dair bilgiler sunulmuştur. İkinci bölümde ise sosyal medya kavramı, bu kavramın tarihsel gelişimi ve platformların gizlilik politikaları üzerinde durulmuştur. Ayrıca büyük veri ve veri madenciliği gibi teknolojilerin kişisel verilerin korunmasındaki riskleri nasıl artırdığına dikkat çekilmiştir. Üçüncü bölümde, sosyal medya platformlarında kişisel

verilerin korunması ihtiyacı, temel hak ve özgürlükler bağlamında incelenmiş ve veri gizliliğini sağlamak için alınması gereken önlemler tartışılmıştır. Son olarak, yasal düzenlemelerin dışında toplumu bilinçlendirme, insan hakları bilgisi ve etik değerlerin önemi vurgulanarak, kişisel veri ihlallerinin engellenmesi için alınması gereken toplumsal önlemler üzerinde durulmuştur.

Yazarlar: Damla Sabiha Varol. (Varol, 2023, p. 15)

Araştırmanın Amacı

Sosyal medyada bireylerin gönüllü ya da yeterince bilgi sahibi olmadan paylaştıkları kişisel verilerin, bireyler için oluşturduğu riskleri ve bu verilerin kullanılması toplumu etkileyecek sorunları tespit etmektir. Ayrıca, yalnızca yasal düzenlemelerin bu sorunları çözmede yeterli olmayacağı savunulmuş ve kişisel verilerin korunması gerekliliği bir insan hakkı olarak ele alınmıştır. Araştırma, kişisel verilerin korunmasının, bireylerin diğer temel hak ve özgürlüklerini zarar görmeden sağlanması gerektiğini vurgulamaktadır.

Literatür Taraması ve Tez ile İlişkisi

Kişisel verilerin korunmasının gerekliliği, bu verilerin bir bireyle doğrudan ilişkilendirilebilir olması ve belirlenebilir bir kişiye ait olmasından kaynaklanır verilerin kötüye kullanılması halinde bireyin temel hak ve özgürlüklerinin zarar görebileceği veya kişisel potansiyelini gerçekleştirmesinin engellenebileceği riskiyle açıklanabilir. Ayrıca, bu verilerin korunması sırasında bireyin diğer temel haklarına zarar verilmemesi esastır. Bu nedenle, hangi kişisel veri türünün hangi koşullarda istisna kapsamına alınacağı, belirlenen kriterler ışığında titizlikle değerlendirilmelidir. (Varol, 2023, p. 44)

Araştırmada temel sorunlar hak ve özgürlükler konusunda ele alınmış ve bazı sosyal medya platformlarının gizlilik politikalarını incelenmiştir. Bu sebeple bu araştırma, sosyal güvenlik için gerekli önlemler ve toplumsal farkındalığın artırılması, etik bilgiler İnsan hakları ihlallerini önlemek ve insan haklarını izlemek için yasal Önlemler açısından tezi destekler

Bulguların Özeti

Sosyal medya platformlarının, kullanıcılarının kişisel verilerini koruma noktasında ciddi eksiklikler taşıdığını ortaya koymuştur. Kullanıcı verilerinin korunması

adına mevcut hukuki çerçevelerin ve gizlilik politikalarının yetersiz kaldığı belirtilmiştir.

Boşluk Analizi

Veri koruma ile ilgili hukuki ve etik yönleri yeterince ele almadan teknik sorunlara odaklanmıştır. Bu yönüyle çalışmada, hukuki düzenlemelerin dışında toplumun bilinçlendirilmesi ve etik bilgilerin artırılması gerektiği vurgulanmıştır.

1.2. Önceki Çalışmaların Boşluk Analizi

1.2.1. Sosyal ve psikolojik boyutlar

Çoğu çalışmada yapay zekânın etkilerinin sosyal ve psikolojik boyutlarının analizi eksiktir. Araştırma büyük ölçüde teknolojik ve hukuki unsurları merkezine alarak ilerlemektedir. yapay zekânın sosyal medya platformlarındaki sosyal etkileşimler ve bireylerin psikolojik refahı üzerindeki etkileri görmezden gelinmektedir. Yapay zekâ uygulamalarının bireysel benlik gelişimi, psikolojik eğilimler ve toplumsal istikrar üzerindeki etkileri genellikle yeterince dikkate alınmamaktadır.

1.2.2. Sosyal güvenlik yönü

Sosyal medya platformlarında yapay zekâ konusunda sosyal güvenliğe yeterince odaklanılmaması, sosyal istikrar ve bireylerin hakları üzerinde geniş etkilere yol açabilir. Yanlış bilginin yayılması, yapay zekânın sosyal güvenliğe yönelik potansiyel tehditleri ve toplumsal eşitsizlik üzerindeki etkisi gibi konuların ayrıntılı incelenmeye ihtiyacı var.

1.2.3. Teknik ve prosedürsel zorluklar

Kişisel verilerin korunması ve muhasebe ilkelerinin uygulanmasına ilişkin sorunların çözümünde teknik çalışmalar çoğu zaman yetersiz kalmaktadır. Büyük veri ve şifreleme teknikleri ile uğraşmak gibi veri güvenliği, sosyal güvenlik ve gizlilikle ilgili yasaların uygulanmasında zorluklar yaşanmaktadır.

1.2.4. Yasal ve etik yön

Çalışmalar büyük oranda yasal ve etik yönlere odaklanmaktadır ve bunlar genellikle yüzeyseldir. Kişisel verilerin korunmasına yönelik yasal çerçevelerin yetersiz analizi ve yapay zekâ kullanımına ilişkin etik zorluklar buna neden olarak gösterilebilir.

1.2.5. Pratik ve toplumsal uygulamalar

Yapay zekânın sosyal gerçeklikte nasıl uygulandığına ve pratik etkilerinin değerlendirilmesine ilişkin analiz eksikliği maalesef mevcuttur ki bu da maalesef yapay zekânın sosyal ve ekonomik sistemleri iyileştirme veya karmaşıklaştırmadaki rolü göz ardı edilmektedir.

1.2.6. Kapsamlı çözümlerin eksikliği

Hali hazırdaki araştırmalar, bazı teknik ve hukuki sorunlara kapsamlı çözümler yerine, kısmi çözümler sunmaktadır. Sosyal medya platformlarında veri koruma, kişisel veri konuları ve sosyal güvenlikte tüm boyutlarıyla ele alan entegre çözümlere ihtiyaç var.

Gerekli çalışma

- Yapay zekânın ruh sağlığı ve sosyal ilişkilere etkilerini, kişisel verilerin bireylerin benlik ve toplumsal algılarını nasıl etkilediğini kapsayacak şekilde çalışmaların genişletilmesi, sosyal güvenlik açıklarının yanı sıra sosyal ve psikolojik alanlardaki analizlerin geliştirilmesi.
- Teknolojinin toplumsal gelişimi, kişisel bilgilerin korunmasını, kaynakların dağılımını ve sosyal hakları nasıl etkilediğini konu alan, sosyal medya platformlarında yapay zekâ araştırmaları çerçevesinde sosyal güvenlik üzerine bir çalışma.
- Koruma ve güvenlik standartlarının uygulanmasındaki teknik ve prosedürlere dayalı zorluklara ilişkin detaylı araştırmalar yapmak ve Bu sorunların aşılmasına yönelik gerçekçi çözümler geliştirmek.
- Sosyal güvenliğin sağlanması için mevcut mevzuatın daha detaylı analiz edilmesi, yasal değişiklik önerileri getirilmesi, Yapay zeka teknolojilerinin gelişmesi, veri gizliliğinin sağlanması için bireylerin çaba sarf etmesini gerektirmekte ve Sorunlarına kapsamlı ve eksiksiz çözümler sunmak gerekmektedir.
- Yapay zekânın pratik uygulamaları üzerine çalışmalar geliştirmek, toplumsal gerçeklik üzerindeki etkilerini analiz etmek ve bu teknolojinin etkin ve yararlı bir şekilde uygulanmasına yönelik stratejiler önermek.

- Sosyal medya platformları çerçevesinde yapay zekâ ve Kişisel bilgiler korunması sorunlarına yönelik teknik, etik ve hukuki önlemleri içeren kapsamlı çözümler sunmak.

İKİNCİ BÖLÜM

YAPAY ZEKÂ VE SOSYAL GÜVENLİK

2.1. Yapay Zekânın Tanımı ve Tarihçesi

Yapay zekâ, insanların akıllı olduğunu düşündüğü eylemleri gerçekleştirebilen makineler yapma bilimi olarak tanımlanabilir. Bu alanda çalışanlardan biri olan Russell Bell, bunu daha basit bir ifade ile sıradan makinelerin bilim kurgu filmlerinde gördüğümüz makineler gibi davranmasını sağlama girişimi olarak tanımlamıştır.

Bu nedenle yapay zekâ. insanlar için tanımlanan düşünme, öğrenme, iletişim gibi bir takım yetenekleri bilgisayar ve diğer makinalara kazandırmak ve böylece onlara zeka statüsü vermek olan bir bilim olarak ortaya çıkmıştır. Günümüz teknolojisinde bilgisayarlar zor ve karmaşık sayısal işlemleri insanlardan giderek daha hızlı çözebilmektedir. Ancak yine de küçük çocuk tarafından büyük bir beceriyle gerçekleştirilebilen basit şeyleri, örneğin iletişim, düşünme ve hatta aile üyelerini tanıma gibi büyük ölçüde yapamazlar.

Bilgisayar, adından da anlaşılacağı üzere, sayıları hesaplar ve bu sonuçları kullanır, ancak düşünmez veya algılamaz. İnsan zihni, birbirine çok karmaşık bir ağ şeklinde bağlı milyarlarca nörondan oluşur ve birçoğu onu bu evrendeki en karmaşık şeyler arasına yerleştirir, bu yüzden onu taklit etmeye çalışmak insanların imkanlarının ötesindedir. (Nour, 2005, s. 7)

Doğru veya yanlışa yönlenmeden hali hazırdaki analiz etme, problemi çözme ve hatta çözümleri devamlarına aktarma düşüncesi çerçevesinde bir olgusal karaktere kavuşan zekâ, insan taraflı yaşamda kalma içgüdüsünün eylemsel bu sadece bir yansıma. Dünya'daki yaşam koşulları bile, hayvanlar, böcekler ve bitkilerde dahil olmak üzere problem çözme güdüsüne dayalıdır, hayvanlar yiyecek ararken problem çözerler, böcekler eko sistem içerisinde problem çözmeye mahkumdurlar, bitkiler de bir problem çözme karmaşasında yeterlilikleri oranında varlıklarını sürdürürler.

Buna göre, zekâ kavramını sadece insanlar için tanımlamak doğru olmasa da, en azından Dünya dışı daha üstün bir varlıkla karşılaşılmadığı sürece Dünyadaki yaşamı yönlendirmede üstünlüğe sahip olan insan, bu kavramın da teorik ve pratik mucidi, kaderini tayin etme rolüne sahip bir aktörü olmuştur. (Köse, 2022, s. 14)

Genel olarak bakıldığında, yapay zekâ, bir bilgisayarın veya programın insan davranışını veya düşüncesini eşleştirme ve insan görevlerini yerine getirme yeteneğidir. Yapay zekâ, her görev için kendini programlanmak yerine, kendi başına cevaplar bulabilir ve sorunları çözebilir. Yapay zekâ, bilişsel modelleme, veri işleme süreçlerinde model tanımlama, öğrenme algoritmaları, görsel veri analizi ve dil işleme tekniklerini entegre biçimde kullanır.

Yapay zekâ sistemleri, karmaşıklıklarından dolayı bir insanın denetleyemediği ve çözemediği görevleri çözmek için kullanılabilir. AI sistemleri çok yönlüdür ve farklı görevleri yerine getirebilir. Bununla birlikte, bilimsel bir bakış açısından, Yapay zek teriminin tanımı, insan zekâsının tanımı kadar bulanıktır. (mpdv, 2024)

Yapay zekâ sistemleri, veriler ve algoritmalar kullanarak çalışır. İlk olarak, yığın miktarda veri toplanır ve eğitim olarak bilinen bir süreçte kalıpları tanımak ve tahmin etmek için bilgileri kullanan matematiksel algoritmalara veya modellere uygulanır. Algoritmalar eğitildikten sonra, sürekli olarak yeni verilerden öğrendikleri ve bunlara uyum sağladıkları farklı uygulamalar içinde konumlandırılırlar.bu yapay zekâ sistemlerinin dil işleme, görüntü tanıma ve veri analizi gibi karmaşık işlemleri zamanla daha yüksek doğruluk ve verimlilikle gerçekleştirme kabiliyetini sürekli geliştirir. (Ellen Glover, 2024)

Yapay zekâ ilk olarak 1956 Yılında Dartmouth Konferansı'nda bir grup bilgisayar bilimcinin yapay zekânın doğuşunu duyurmasıyla ortaya çıktı ve o zamandan günümüze kadar yapay zekâ, insanlık tarihi için parlak bir geleceğin habercisi oldu. Yapay zekâ, özellikle 2015 Yılından itibaren son birkaç yılda önemli boyutlarda yaygınlaştı. paralel veri işleme konusunda neredeyse sınırsız depolama kapasitesiyle birlikte daha yüksek hız, düşük maliyet ve üstün performans avantajı sunmaktadır. (GPU) ve her türlü görüntü, finansal işlemler, harita verileri vb. büyük veri akışlarının ortaya çıkması sayesinde bu yaygınlaşma gerçekleşti.

1956 Yılında Yapay Zekâ'ya öncülük eden bilim insanlarının hayali insan zekasıyla aynı özelliklere sahip yeni, karmaşık bilgisayarlar inşa etmekti. Buna istinaden Genel Zekâ adı verilen kavram, bir insanın tüm duyu ve düşüncelerine sahip bir makine tasarladılar. Günümüzde bu kavram bilim kurgu olmaktan çıkıp gerçeğe dönüştü ve yapay zeka projelerine teknolojik yatırım yolculuğu başladı. (Bilal, 2019, s. 33)

Yapay Zekâ Zaman Çizelgesi

Yıllar boyunca, dikkat çeken gelişmelerden bazıları şunlardır:

1950

Alan Turing, 'Computing Machinery and Intelligence' (Hesaplama Makineleri ve Zeka) adlı çalışmasını yayınlayarak Turing testini ortaya atmış ve yapay zeka kavramının önünü açmıştır.

1951

Marvin Minsky ve Dean Edmonds, SNARC adını verdikleri ve 40 nöronu simüle etmek için 3.000 vakum tüpü kullanan ilk yapay sinir ağını (ANN) geliştirdiler.

1952

Arthur Samuel, bilgisayarların kendi kendine öğrenme yeteneği kazanmasına öncülük eden ve dünyanın ilk kendi kendini gelişmekte olan dama oyunu programını geliştirmiştir.

1956

- Yapay zeka' terimi, John McCarthy, Marvin Minsky, Nathaniel Rochester ve Claude Shannon tarafından 1958'de düzenlenen öncü çalıştaya atfedilir.
- Frank Rosenblatt, topladığı verileri değerlendirerek öğrenebilen ve modern sinir ağlarının temelini oluşturan erken bir yapay sinir ağı (ANN) olan perceptron'u geliştirdi.
- Lisp programlama dili John McCarthy tarafından icat edildi ve esnekliği ve benzersiz yetenekleri nedeniyle yapay zeka araştırmalarında hızla tercih edilen araç haline geldi.

1959

- Arthur Samuel, Bilgisayarların programcılarını alt edebileceğini çığır açan makalesinde göstererek bu alanda devrim yarattı ve disiplinin temelini oluşturan öncü terim olan makine öğrenimi'ni ortaya attı.
- Oliver Selfridge, olaylardaki kalıpları bulmak için kendini uyarlayıp geliştirebilen bir modeli tanımlayan ve makine öğrenimine önemli bir katkı sağlayan

Pandemonium: A Paradigm for Learning (Pandemonium: Öğrenme İçin Bir Paradigma) adlı çalışmasını yayımladı.

1964

Bobrow tarafından 1960 yıllarda geliştirilen STUDENT programı, doğal dilde sunulan matematiksel problemleri anlayıp çözebilen ilk sistem olması nedeniyle doğal dil işleme alanında bir dönüm noktası olarak kabul ediliyor.

1965

Dendral projesi, Feigenbaum ve ekibi tarafından geliştirilen ve organik kimya alanında uzmanlaşmış ilk yapay zeka sistemidir. kimyagerlere bilinmeyen bileşikleri analiz etmede çığır açıcı bir araç sağlamıştır.

1966

Joseph Weizenbaum, insanlarla etkileşime geçebilen ve gerçek эмоции taşıyormuş izlenimi verebilen efsanevi ELIZA programını tasarlayarak yapay zeka tarihinde önemli bir dönüm noktası yaratmıştır.

Stanford Araştırma Enstitüsü'nün geliştirdiği Shakey robotu, yapay zeka, navigasyon, bilgisayarlı görü ve doğal dil işleme teknolojilerini entegre eden ilk mobil akıllı sistem olarak otonom araçların gelişimine öncülük etmiştir.

1968

Winograd'un SHRDLU'su, blok dünyasında kullanıcı talimatlarını işleyebilen ve akıl yürütme yeteneği sergileyen ilk çok modlu yapay zeka örneği olarak yapay zeka araştırmalarında yeni bir çığır açmıştır.

1969

- Arthur Bryson ve Yu-Chi Ho, çok seviyeli yapay sinir ağlarının geliştirilmesine olanak sağlayan geri yayılım algoritmasını tanımlayarak, perceptron teknolojisini aşan ve derin öğrenmenin temellerini atan önemli bir adım atmışlardır.
- Minsky ve Papert'in 'Perceptrons' kitabı, basit sinir ağlarının teorik sınırlarını ortaya koyarak, nöral ağ araştırmalarında geçici bir gerilemeye yol açmış ve sembolik yapay zeka çalışmalarının ön plana çıkmasını sağlamıştır.

1973

Lighthill Raporu olarak bilinen (Yapay Zekâ: Genel bir Araştırma) çalışması, İngiliz yetkililerin yapay zeka çalışmalarına bakışını kökten değiştirmiş ve bu alandaki devlet finansmanının dramatik şekilde azalmasına neden olmuştur.

1980

Lisp makinelerinin ticarileşmesi yapay zekâ endüstrisinde önemli bir yenilik dalgası başlatmış olsa da bu pazarın beklenmedik şekilde çöküşü, erken dönem yapay zekâ teknolojilerinin karşılaştığı zorlukları gözler önüne sermiştir.

Danny Hillis'in 1981'de geliştirdiği paralel işlemcili bilgisayar mimarisi, günümüz GPU teknolojilerinin öncüsü niteliğinde olup, yapay zekâ algoritmalarının işlenmesinde devrimsel bir yaklaşım sunmuştur.

1984

Marvin Minsky ve Roger Schank, Yapay Zekayı Geliştirme Derneği toplantısında AI winter (Yapay Zekâ Kışı) terimini ortaya attılar ve iş dünyasını, yapay zekâ ile ilgili aşırı beklentilerin hayal kırıklığına ve sektörün çöküşüne yol açabileceği konusunda uyardılar ve bu öngörü üç yıl sonra gerçekleşti.

1985

Judea Pearl, bilgisayarlarda belirsizliği tanımlamak için istatistiksel teknikler sunan Bayes ağları ve nedensel analiz yöntemini tanıttı.

1988

Peter Brown ve ekibi, daha yaygın olarak incelenen makine çeviri yöntemlerinden birinin yolunu açan Dil Çevirisine İstatistiksel Bir Yaklaşım adlı çalışmayı yayınlayarak en çok incelenen makine çevirisi yöntemlerinden birine zemin hazırladı.

1989

LeCun, Bengio ve Haffner'ın konvolüsyonel sinir ağlarıyla el yazısı tanıma sistemleri geliştirmesi, nöral ağ teknolojilerinin teoriden pratiğe geçişinde dönüm noktası oluşturmuş ve endüstriyel uygulamaların önünü açmıştır.

1997

1997'de Hochreiter ve Schmidhuber tarafından önerilen LSTM mimarisi, tekrarlayan ağlardaki gradyan kaybolması sorununa radikal bir çözüm getirerek, uzun zaman aralıklarında bağımlılıkları öğrenme konusunda benzersiz bir yetenek kazandırmıştır.

- IBM'in Deep Blue'su, tarihi rövanş maçında Dünya Satranç Şampiyonu Garry Kasparov'u yendi bu, turnuva koşulları altında yarışan dünya satranç şampiyonunun bir bilgisayar tarafından ilk yenilgisiydi.

2000

Montreal Üniversitesi ekibinin yayınladığı bu makale, sinir ağlarının dil modellemede ilk başarılı uygulaması olarak, kelime gömme tekniklerinin ve modern dil modellerinin teorik temelini oluşturmuştur.

2006

- Fei-Fei Li'nin öncülük ettiği ImageNet projesi, 2009'da tanıtılan devasa görsel veritabanıyla yapay zekâ alanında bir dönüm noktası oluşturmuş, görüntü tanıma algoritmalarının gelişimini hızlandıran yıllık bir benchmark yarışmasının temelini atmıştır.
- IBM Watson, başlangıçta en önemli bilgi yarışması kabul edilen Jeopardy'de bir insanı yenme hedefiyle tasarlandı. 2011 yılında bu soru-cevap bilgisayar sistemi, yarışmada tüm zamanların en iyi (insan) şampiyonu Ken Jennings'i mağlup etti.

2009

2009 tarihli bu seminal çalışma, CUDA mimarisinin derin öğrenme problemlerine uygulanmasıyla, tek bir GPU'nun 100 CPU çekirdeğinin işlem gücüne eşdeğer performans sunabileceğini deneysel olarak kanıtlamıştır.

2011

- Schmidhuber ekibinin geliştirdiği evrişimli sinir ağı, Alman Trafik İşaretleri Yarışması'nda %99.46 doğruluk oranıyla insan performansını geride bırakarak, derin öğrenmenin pratik uygulamalardaki üstünlüğünü kanıtlamıştır.
- Apple'ın 2011'de tanıttığı Siri, doğal dil işleme teknolojilerini tüketici elektroniğiyle buluşturarak, kişisel asistanlar çağını başlatan ve günlük yaşamda yapay zeka kullanımını yaygınlaştıran ilk büyük ölçekli uygulama olmuştur.

2012

2012 ImageNet yarışmasında %16.4 hata oranıyla birinci olan AlexNet, 1.2 milyon görüntü üzerinde eğitilerek, derin evrişimsel ağların pratik uygulanabilirliğini kanıtlamış ve endüstride yapay zeka tabanlı görüntü analizi çağını başlatmıştır.

2013

- Çin'in Tianhe-2 süper bilgisayarı, 33.86 petaflopluk hızıyla dünyanın en hızlı bilgisayar sistemi unvanını üçüncü kez üst üste korudu ve dünya süper bilgisayar hızını ikiye katlamış oldu.
- DeepMind'in 2015'te Nature'da yayınladığı makale, derin pekiştirmeli öğrenmenin oyunlarda insanüstü performansa ulaşabileceğini kanıtlayarak, yapay zekanın karmaşık ortamlarda özerk öğrenme yeteneğini ilk kez somut şekilde göstermiştir.

2014

- Ian Goodfellow liderliğindeki ekip, üretici ve ayırt edici ağların rekabetine dayanan devrim niteliğindeki Üretici Çekişmeli Ağlar (GAN) mimarisini geliştirerek, gerçekçi görüntü sentezinden derin sahte içerik üretimine kadar geniş bir uygulama yelpazesinin önünü açmıştır.
- Kingma ve Welling, varyasyonel otomatik kodlayıcıları (VAE) tanıtarak makine öğreniminde yeni bir çağ başlatmış, bu yöntemle metin, görüntü ve video üretiminde istatistiksel olarak anlamlı çıktılar elde edilebilmiştir.
- Facebook'un geliştirdiği DeepFace sistemi, derin evrişimsel ağlar kullanarak yüz tanımada %97.35 doğruluk oranına ulaşmış ve insan seviyesindeki tanıma performansına erişen ilk ticari uygulama olmuştur.

2016

- AlphaGo'nun Lee Sedol'a karşı kazandığı zafer, yapay zekanın sadece hesap gücüyle değil, yaratıcı strateji geliştirme yeteneğiyle de insan zekasını aşabileceğini göstererek, Go gibi sezgisel karmaşıklığı yüksek oyunlarda yeni bir çağ başlatmıştır.
- Uber, Pittsburgh'da vip hizmetlerde kullanılmak üzere sürücüsüz araç pilot programını başlattı.

2017

- Stanford'da yapılan araştırmada, görüntülere kademeli gürültü ekleme ve bu süreci tersine çevirme prensibine dayanan yeni bir derin öğrenme yaklaşımı ortaya kondu. Bu yöntem, modern görüntü oluşturma sistemlerinin temelini oluşturdu.
- 2017'de Google Brain ekibi, dil işlemede devrim yaratan Transformer mimarisini tanıttı. Bu model, öz-dikkat mekanizması sayesinde büyük ölçekli metin işleme yeteneklerinde yeni bir çağ başlattı.
- Ünlü teorik fizikçi Stephen Hawking, yapay zekanın kontrolsüz gelişiminin insanlık için varoluşsal risk oluşturabileceğine dikkat çeken tarihi bir uyarı yaptı.
- 2018'de uluslararası bir konsorsiyum tarafından geliştirilen CIMON, Uluslararası Uzay İstasyonu'nda görev yapan ilk yapay zeka destekli robot asistan oldu.
- OpenAI'ın ilk nesil GPT modeli, büyük dil modelleri alanında önemli bir kilometre taşı oldu ve sonraki tüm gelişmeler için referans noktası oluşturdu.
- Japon şirketi Groove X, insan duygularını tanıyıp yanıt verebilen ilk nesil kişisel robotlardan Lovot'u piyasaya sürdü.

2019

- Microsoft, 17 Milyar parametreli Turing Doğal Dil Üretimi (Turing Natural Language Generation) adlı üretken dil modelini başlattı.
- Google Al ve Langone Tıp Merkezi'nin derin öğrenme algoritması, potansiyel akciğer kanseri tespitinde radyologlardan daha başarılı oldular.

2020

- Oxford araştırmacıları, acil servislerde kullanılmak üzere geliştirdikleri Curial AI ile hastaların rutin verilerini analiz ederek COVID-19'u %90 doğrulukla ve hızlı şekilde tespit edebilen bir sistem oluşturdu. Bu yöntem, geleneksel PCR testlerine alternatif olarak hastane kaynaklarının optimizasyonunu sağladı.
- OpenAI, 175 milyar parametre kapasitesiyle şimdiye kadarki en gelişmiş dil modeli olan GPT-3'ü tanıttı. İnsan benzeri metinler oluşturabilen bu model, doğal dil işlemede yeni bir standart belirledi ve çeşitli sektörlerde uygulama alanı buldu.
- NVIDIA Omniverse platformunun beta sürümü, gerçek zamanlı 3B simülasyon ve işbirliği için yeni bir altyapı sundu. Endüstriyel tasarımdan film prodüksiyonuna

kadar geniş kullanım alanıyla dikkat çeken platform, fiziksel ve dijital dünyaların entegrasyonunu sağladı.

- DeepMind'in AlphaFold sistemi, CASP14 yarışmasında protein yapılarını atomik doğrulukla tahmin ederek bilim dünyasında büyük yankı uyandırdı. Bu başarı, ilaç keşif süreçlerinde devrim yapma potansiyeli taşıyor.
- OpenAI'ın DALL-E modeli, metin açıklamalarından orijinal görseller oluşturma yeteneğiyle yaratıcı endüstrilerde yeni olanaklar sundu. Bu çok modlu sistem, yapay zekanın sanatsal yeteneklerini gözler önüne serdi.
- California Üniversitesi araştırmacıları, elektronik bileşenler yerine pnömatik sistemlerle çalışan dört ayaklı bir robot geliştirdi. Geleneksel robotlardan farklı olarak esnek yapısı sayesinde dar alanlarda ve hassas ortamlarda kullanıma uygun bu tasarım, robotik alanında yeni bir yaklaşımı temsil ediyor.

2022

- Google Yazılım Mühendisi Blake LEMOINE, Lamda'nın sırlarını açıkladığı ve O'nun bilinçli olduğunu söylediği için işten çıkarıldı.
- DeepMind, yeni, etkili ve kanıtlanabilir doğru algoritmalar keşfettiği AlphaTensor u tanıttı.
- Intel tarafından geliştirilen FakeCatcher, derin öğrenme tabanlı bir algoritmayla çalışarak gerçek zamanlı deepfake tespitinde %96 doğruluk iddiasıyla dikkat çekti. Sistem, geleneksel yöntemlerden farklı olarak şu teknikleri kullanıyor:
- OpenAl, Yapay Zekânın yasal olduğunu söyleyerek 30 Kasım'da GPT-3,5 dil modeli için sohbet tabanlı bir arayüz sunan ChatGPT'yi piyasaya sürerek yapay zekânın kitleler için erişilebilir Gelişiminde önemli rol oynamıştır.

2023

- OpenAl, hem metin hem de görsel verileri işleyebilen GPT-4 çok modlu LLM'yi ilan etti. Microsoft, ChatGPT'yi arama motoru Bing'e entegre etti ve Google, GPT sohbet robotu Bard'ı ilan etti.
- Elon MUSK, Steve WOZNIAK ve diğer binlerce imza ile birlikte GPT-4'ten daha büyük yapay zekâ sistem eğitimlerinin altı ay süreyle durdurulmasını istedi.

2024

Üretken yapay zekâ araçları, iyileştirilmiş model mimarileri, verimlilik kazanımları ve daha iyi bir eğitim hızlı bir gelişim gösterdi. Sezgisel arayüzler, enerji tüketimi, önyargı ve iş kaybı gibi devam eden kaygılara rağmen yaygın bir benimsenme sağladı. (Karjian, 2024)

2.2. Sosyal Güvenliğin Tanımı ve Tarihçesi

Tarih boyunca toplumların yaşadığı değişimlerin sonucu olarak sosyal güvenlik kavramı da, özellikle 20. Yüzyıl'ın başlangıcından itibaren hızlı bir şekilde gelişmiştir. Sanayi Devrimi üretim sistemlerinde köklü dönüşümlere yol açarak modern toplumların ekonomik ve sosyal yapısını şekillendirmiştir. Bu tarihsel dönüşüm sürecinde ortaya çıkan çalışma koşulları ve sosyal eşitsizlikler, zamanla işçi hakları hareketlerinin gelişmesine zemin hazırlamıştır. İnsan Güvenliği: İnsan güvenliği, 1994 Birleşmiş Milletler İnsan Güvenliği Raporu'nda belirtildiği üzere yedi temel boyuttan oluşmaktadır. Bu boyutlar ekonomik, çevresel, sağlık, kişisel, gıda, topluluk ve siyasi güvenliktir. İnsan güvenliği, Bireylerin temel ihtiyaçlarının sistematik olarak karşılanması ve yaşam standartlarının sürdürülebilir şekilde iyileştirilmesine odaklanmaktadır. Barış, yalnızca savaşın ve çatışmanın bulunmaması anlamına gelmez. aynı zamanda toplumda adaleti, güvenliği ve uyumu sağlayan ifade eder. Barış, pozitif ve negatif açılardan değerlendirilebilir. Negatif olarak savaşın yokluğunu ifade ederken, pozitif olarak da sosyal adaletin, eşitliğin ve insan haklarının korunmasını da temsil edebilir. İnsan güvenliği, güvenliği en basit haliyle yeniden tanımlama çabasını temsil eder. Öncelikle devletin değil, bireyin güvenliğini sağlamayı amaç edinen analitik bir araçtır. Bireylerin güvenliğine yönelik tehditleri azaltmayı amaç edinen alternatiflerin araştırılması, politika eylem ve önerilerinin merkezi bir hedefi haline gelir. Yapılan araştırmalar insanlardaki güvensizlik nedenlerinin sosyal, ekonomik ve politik koşullarla çevre ve gıdaya kadar, genişletilmiş insan güvenliği açısından olduğu tespit edilmiştir. İnsan güvenliği tanımının sınırlarının belirlenmesine bağlı olarak uygulanmasıyla oluşturulan politika girişimleri, askeri güce geleneksel odaklanmanın çok ötesindeki düşünceleri bir araya getirerek, orduların yerini tamamen almasa da ordulara verilen önemi büyük ölçüde azaltmıştır. Bu sebeple insan güvenliği: insan merkezli çok boyutlu birbirine bağlı evrensel bir prensip olarak, güvensizliğe katkıda bulunan her bir parametrenin azaltılmasının bir sonucu olarak elde edilen toplam kazanımları yansıtır.

Uygulamada, Human Security raporunda da belirtildiği gibi, her bir özel bağlamda bir güvensizlik çekirdeğini dikkate almaya ihtiyaç vardır. NHDR 'lerde olduğu gibi ülke bazında da bir yaklaşım bunu yapmaya yardımcı olur. (Undp.org, 2006, s. 5)

İnsan güvenliğinin temellerini, Birleşmiş Milletler 'in barış, kalkınma ve güvenliğe yönelik müdahalelerinin genel çabalarıyla izlemek mümkündür. İnsan güvenliği kavramı, hakların ve yetkilerin bir önceliğine dayanır ve bu ilkenin benimsenmesi yoluyla ifade edilir ve yasalaştırılır. Dönüm noktası niteliğindeki İnsan Hakları Evrensel Beyannamesi'ne göre doğuştan gelen hakları sayesinde her bir insana garanti edilen temel sosyal-politik ve ekonomik koşulların ifade edilmesinde ilk ve en vurgulu adımdır. İnsan Hakları Evrensel Beyannamesi'nin 3. Maddesi'nde, Yaşamak, özgürlük ve Bireysel güvenliği herkesin hakkıdır denilmektedir. Bu tür açıklamalar, insan haklarının küresel yönetim yapılarında kurumsallaştırılmasının temellerini oluşturmuştur. İnsan güvenliği, evrensellik ve temel kabul üzerine kuruludur . (Undp.org, 2006, s. 25)

21. yüzyılın dijital teknolojik uygarlığında yaşayan milyonlarca insan için, uygun bilgiye erişme fırsatı ve hakkının yanı sıra mevcut verileri işleme, filtreleme ve yorumlama yeteneği, su, gıda ve yakıtın yanı sıra neredeyse birincil bir gereklilik haline geldi. Çoğunlukla Twitter, Facebook, Amazon, Microsoft, Apple veya Alpha bet (Google grubunun ana şirketi) gibi ABD'li teknoloji devleri olmak üzere, Günümüz dijital ekosisteminde internet servis sağlayıcıları ve platform operatörleri, bilgi güvenliği ve doğruluğu konusunda kritik bir sorumluluk üstlenmektedir. Ancak küresel ölçekte etkili olan düşünce liderleri ve veri denetleyicileri ekonomik kaygılarla ilgili tüm bu beklentileri gerçekten karşılamıyor, çeşitli yasal boşluklardan yararlanıyor. İngiltere ve Amerikan vatandaşlarının büyük çoğunluğu Zuckerberg'in Amerikan Kongresi'nin kısıtlanması çağrısına katılması en önemli sonuçlarından biri olarak gösterilebilir. Bir yandan, ABD başkanlık seçimlerini çevreleyen iyi bilinen skandallar, 2016 Brexit referandumu ve özellikle 2020'lerin başında İnternet trollerinin çoğalması, çok sayıda komplo teorisi ve sahte haber nedeniyle, İngilizlerin ve Amerikalıların çoğunluğu veri yönetimi, bilgi paylaşımı ve İnternet hizmetlerinin kontrolü ve denetimi konusunda daha katı yasalar istemektedir. Küresel boyutta olmasa da, en azından kendi ülkelerinin siber uzayı ile ilgili olarak hak sahibi olmak istemişlerdir. (Babos T. T., 2021, s. 69)

Günümüzün temelden değişen dijital ekosistemi, insanlığa benzer, hatta daha büyük ve hatta daha derin bir bilimsel-teknolojik ve sosyal-psikolojik zorluk sunuyor. Ne de olsa, nükleer enerjiyi ve dolayısıyla nükleer silahları kullanmanın amacı ve yöntemi, Soğuk Savaş'ın uzun yıllarında olduğu gibi, II. Dünya Savaşı'nın son yılında birkaç düzine üst düzey karar verici ve uzman çevresinde yoğunlaşırken, günümüzün ikincil sanal evreni, gerçek bir emniyet supabı ve kullanımının sınırı olmaksızın herkes tarafından erişilebilir Ya iyilik ya da kötülük için. Yapay zekânın kullanılmayan potansiyelini veya insan toplumlarımızın temel ihtiyaçlarını, güvenliğini ve fiziksel varlığını belirleyen bilgisayarlar tarafından yönlendirilen kritik altyapıların güvenlik açıklarını bir düşünün. (Babos T. T., 2021, s. 70)

Sosyal güvenlik kavramının tarihçesi. eski toplumların bireyleri yoksulluktan ve ekonomik sorunlardan korumak için işbirliği ve sosyal dayanışmaya dayandığı uzak tarihsel dönemlere kadar uzanmaktadır. Bununla birlikte, sosyal güvenliğin düzenlenmiş resmi bir sistem olarak gelişip ortaya çıkması yalnızca modern zamanlarda gerçekleşmiştir.

2.2.1. Çağdaş sosyal güvenlik yapılarının ortaya çıkışı

- **On Dokuzuncu Yüzyıl**

Bu sistemin amacı, işçi sınıfının koşullarını iyileştirmek ve toplumsal gerilimleriyle birlikte dönemin sosyalist hareketlerinin etkisini azaltmaktı.

Almanya, yaşlı nüfusun sosyal güvenliğine yönelik tarihi bir adım atarak 1889 yılında dünyanın ilk yaşlılık sigortası sistemini hayata geçirdi. Bu yenilikçi sosyal politika, Şansölye Otto von Bismarck'ın öncülüğünde şekillendi. Sistemin temelleri ise daha önce, 1881'de İmparator I. Wilhelm'in Bismarck'ın tavsiyesiyle parlamentoya gönderdiği resmi yazıda atılmıştı. İmparator bu belgede, Çalışma yeteneğini yaşlılık veya engellilik nedeniyle kaybeden vatandaşların, devlet himayesine alma hakkı bulunmalıdır, ifadelerine yer vererek, modern sosyal devlet anlayışının ilk somut örneğini ortaya koymuştu. (Ssa.gov, 2024)

- **Yirminci Yüzyıl**

Yirminci Yüzyıl, dünya çapında sosyal güvenlik sistemlerinin çoğalmasına tanıklık etti:

Amerika:

Sosyal Güvenlik Yasası, 1935 yılında Başkan Franklin D. Roosevelt'in yönetimi altında, Büyük Buhran'ın etkilerini değerlendirmek için Yeni Anlaşma'nın bir parçası olarak oluşturuldu. Federal yaşlılık yardımları sistemi düzenleyerek ve çeşitli devletlerin bağımlı ve sakat çocuklar, körler, yaşlılar, anne ve çocuk refahı, halk sağlığı ve işsizlik tazminatı yasalarının idaresi için daha geçerli hükümler sağlayarak genel refahı sağlama yasası. Sosyal Güvenlik Kurulu oluşturarak, geliri artırmak ve bunun gibi amaçlar için bu yasalara ihtiyaç duyuldu. (Ssa.gov, 2024)

Britanya:

BEVERIDGE Raporu 1942'de başlatıldı ve tüm vatandaşları kapsayan kapsayıcı Toplum ve İnsan Güvenliği Sistemini geliştirilmesinin temeli oldu. Bu rapora göre hayırseverliğin yeterli olmadığı tutarlı bir hükümet planının tek yeterli önlem olacağı vurgulandı. Savaşın patlak vermesiyle Beveridge kendini Whitehall'da çalışırken buldu ve burada sosyal hizmetlerle ilgili bir soruşturmaya yönetmekle görevlendirildi. Vizyonu, Beş Dev'in hastalık, cehalet, tembellik, sefalet ve yoksulluk dediği şeyle savaşmaktı. (Parliament, 2024)

Türkiye Cumhuriyeti:

Türkiye Cumhuriyeti'nin temel hukuk metni olan Anayasa'nın 60. maddesi, sosyal güvenlik hakkını vatandaşların temel hakları arasında düzenlemektedir. Ayrıca anayasasında kanunla onaylanmış insan haklarına dair milletlerarası sözleşmeleri milli kanunların üzerinde hiyerarşik bir yere yerleştirmiştir (AY m. 90/son). Türk devleti ayrıca Avrupa İnsan Hakları Mahkemesi'nin yargı yetkisini kabul etmiş, Anayasa Mahkemesi'ne kişisel başvuru hakkını anayasal bir hak olarak kabul ederek adil yargılama hakkının hayata geçirilmesi yolunda önemli adımlar atmıştır. (Arastirma.disk., 2015, s. 181)

2.2.2. Arap Dünyasındaki Modern Sosyal Güvenlik Sistemleri

Arap ülkeleri yirminci yüzyılda modern sosyal güvenlik sistemlerini uygulamaya başladı:

Mısır:

İlk sosyal güvenlik yasası 1959'da kuruldu. 1959 yılında Sosyal Dayanışma Bakanlığı tarafından yürürlüğe konulan bu sistem, aile bakımından yoksun çocukların,

özellikle de insana yakışır ebeveynliğe sahip çocukların, ailenin amaçlarının bütünlüğünü ve geçerliliğini sağlayan koşul ve kriterlere göre seçilen ailelere, onları sömürmeden veya kişisel çıkarlar gözetmeksizin bağlanması esasına dayanmaktadır.

Ürdün:

Sosyal Güvenlik Sistemi 1978 yılında kurulmuştur. 1978 tarihli 30 sayılı Sosyal Güvenlik Kanunu çıkarılmış ve bu kanun kapsamında malullük, yaşlılık, ölüm ve iş kazası sigortaları uygulanmaya başlanmıştır. (S S Corporation, 2024)

Körfez Ülkeleri:

Kamu ve özel sektördeki işçiler için kapsamlı sigorta sistemleri benimsendi ve yürürlüğe konuldu.

2.2.3. Yirmi Birinci Yüzyılda Sosyal Güvenlik Sistemlerinin Dijital Dönüşümünün Evrimi

Yirmi birinci Yüzyıl, sosyal güvenlik sistemlerinin nasıl yönetildiği ve sunulduğu konusunda radikal değişikliklere tanıklık etti ve dijital teknoloji bu dönüşümlerin arkasındaki birincil itici güç haline geldi. Artık sadece kâğıt belgelere ve uzun bürokratik prosedürlere dayanan geleneksel yöntemler değil, en son teknolojik gelişmelerden yararlanan akıllı sistemlere dönüşmüştür. Bu dönüşüm süreci geleneksel sosyal güvenlik mekanizmalarının dijital teknolojilerle yeniden yapılandırılmasını zorunlu kılmıştır. Özellikle büyük veri analitiği ve yapay zeka uygulamaları, kaynakların daha adil dağıtılmasında hayati rol oynamaya başlamıştır

- **Program yönetimini iyileştirmek ve yolsuzluğu azaltmak için teknolojiyi kullanmak**

Dijital dönüşümden önce, sosyal güvenlik sistemlerinin yönetimi büyük oranda manuel süreçlere dayanıyordu ve bu da onları yolsuzluğa ve kötü yönetime karşı savunmasız hale getiriyordu. Ancak teknolojinin gelişmesiyle birlikte bu sistemler daha Şeffaf ve etkin olacak şekilde tasarlanmıştır.

Örneğin, birçok ülke, yararlanıcıların kaydedilmesine ve dosyalarının anında izlenmesine olanak tanıyan entegre dijital veri tabanlarını benimsemiştir. Bu kurallar, tüm veri hareketliliği bilgisayarlı sistemler aracılığıyla izlendiği için veri manipülasyonunu azaltmaya yardımcı olur. Örneğin Hindistan'da Aadhaar sistemi, kamu sektörü sunum reformları, mali bütçe yönetimi, sosyal ve finansal içerme,

erişilebilirliği artırma ve sorunsuz ve insan merkezli yönetimi teşvik etmek adına stratejik bir politika aracıdır. Aadhaar Programı'nın kalıcı bir finansal adres olarak, yoksul ve savunmasız grupların topluma finansal katılımını ve dolayısıyla eşitlik ve adaleti kolaylaştıracak bir araç olduğu söylenebilir.

Aadhaar Programı piyasaya yeni girmesine rağmen şimdiden önemli başarılar elde etmiş ve dünyanın biyometrik tabanlı tanımlama sistemi konusunda rakiplerinin çok önünde kendine yer bulmuştur. (Uidai.gov, 2024)

- **Elektronik ödeme sistemlerinin geliştirilmesi**

Dijital dönüşümün sosyal güvenlik sistemlerindeki en önemli etkilerinden biri nakit yerine elektronik ödeme sistemlerine olan güvenin artmasıdır. Bu değişiklik sadece yardımların dağıtımını hızlandırmakla kalmadı, aynı zamanda şeffaflığı artırarak yolsuzluğun önüne geçti. Örneğin, Kenya gibi birçok Afrika ülkesinde, sosyal yardımları dağıtmak için M-Pesa gibi mobil ödeme sistemleri uygulamaya konulmuştur. Bu sistemler, bireylerin bankacılık altyapısının olmadığı uzak bölgelerde bile kolayca yardım almalarını sağlar. Ayrıca, kişisel kazanç için kullanabilecek aracılara olan bağımlılığı azaltmaya da yardımcı olurlar. İsveç gibi gelişmiş ülkelerde, elektronik ödeme sistemleri, emekli maaşlarının ve sosyal yardımların dağıtılması için önemli bir araç haline geliştir. Fonlar, hızlı ve güvenli sistemler kullanılarak doğrudan yararlanıcıların banka hesaplarına aktarılarak Zaman ve emek açısından ciddi kazanımlar elde edilmektedir

Mart 2007'de, bağışçı tarafından finanse edilen bir pilot projenin ardından Safaricom, M-PESA olarak bilinen yeni bir cep telefonu tabanlı ödeme ve para transferi hizmeti başlattı.10 Hizmet, kullanıcıların cep telefonlarında kayıtlı bir hesaba para yatırmalarına, bakiyeleri SMS teknolojisini kullanarak diğer kullanıcılara göndermelerine (mal ve hizmet satıcıları dahil) ve mevduatları normal parayla değiştirmelerine olanak tanır. Kullanıcıların hesaplarından kesilen ücretler, e-float veya e-para (M-PESA bakiyelerinin ifade edildiği para birimi) gönderildiğinde ve nakit çekildiğinde tahsil edilir. (Jack, 2011, p. 6)

- **Yapay zekâ kullanarak veri analizi**

Sosyal güvenlik sistemlerinde dijital dönüşümün en belirgin gösstergelerinden biri, verileri analiz ederek en çok ihtiyaç duyan grupları belirlemek için yapay zekânın kullanılmasıdır. Bu teknoloji, sağlık verileri, istihdam kayıtları ve vergi kayıtları gibi

birden çok kaynaktan büyük miktarda veri toplamaya dayanır. Bu veriler daha sonra acil desteğe ihtiyaç duyanları veya yoksulluğa karşı en savunmasız olanları belirlemek için gelişmiş algoritmalar kullanılarak analiz edilir.

Örneğin, Amerika Birleşik Devletleri'nde Sosyal Güvenlik programı, milyonlarca yararlanıcının verilerini analiz etmek ve gelecekteki ihtiyaçlarını tahmin etmek için yapay zekâ kullanır. Bu sistem, sosyal programların sürdürülebilirliğini sağlamaya ve kaynak tahsisini iyileştirmeye yardımcı olur. Yapay zekâ, yetkilendirme uygulamalarındaki anormal kalıpları da algılayabilir ve bu da dolandırıcılık girişimlerinin tespit edilmesine katkıda bulunur.

2.3. Yapay Zeka Teknolojisinin Sosyal Güvenlik Üzerindeki Etkileri ve Toplumsal Yansımaları

Zamanımızda yapay zeka alanındaki hızlı gelişmeler, özellikle Üretken Yapay Zeka (Generative Artificial Entelliğince) teknolojilerinin toplumsal ve bireysel yaşamda giderek daha fazla yer edinmesine yol açmaktadır. Bu dönüşüm, çeşitli alanlarda etkilerini göstermektedir: teknolojilerin getirdiği etik ve toplumsal sorumlulukları dikkate almanın yanı sıra bizlere sağladığı faydalar da en önemli konular arasındadır. Birçok farklı alanda etkisi bulunan yapay zekâ, insanlar ve sosyal güvenlik üzerinde olumlu ve de olumsuz etkileri mevcuttur. Güvenlik sektörü, bunların önde gelenleri arasında yer almaktadır. Yapay zekâ, insanların fiziksel güvenliğini tecrübeli insan güvenlik uzmanlarından daha etkili bir şekilde sağlamak için güvenlik kameralarının izlenme yeteneklerini artırabilir. Bununla birlikte, yapay zekâ ayrıca yüz tanıma ve kişisel verilerin izlenmesi gibi konularda ciddi mahremiyet kaygılarına neden olabilmektedir. Yapay zekânın insan ve insanın sosyal güvenliğine olan etkisi incelenirken, bu olumlu ve olumsuz Sonuçların adil ve dengeli bir şekilde analiz edilmesi ve gerekli düzenlemelerin titizlikle uygulanması büyük önem taşımaktadır.

Yapay zekâ, ekonomik büyümeyi destekleme, bireylerin refahını artırma ve sosyal kalkınmayı güvence altına alma konusunda büyük bir potansiyele sahiptir. Ancak, yapay zekâ ile ilgili tartışmalarda verimlilik ve kârlılık odaklı bir yaklaşım benimsenmesi, onun toplumsal yapıya olan derin etkilerinin göz ardı edilmesine neden olmaktadır.

Toplumların yapay zekânın getirdiği dönüşümlere uyum sağlama kapasitesinde ciddi boşluklar yaratırken, bireylerin yeteneklerini geliştirmeye yönelik yatırımların yetersiz kalmasına yol açmaktadır. Sonuç olarak, sosyal eşitsizlikler hızla büyümekte ve ekonomik dengesizlikler giderek derinleşmektedir. (Suncem Koçer, 2024, s. 16)

Yapay zekânın ulusal güvenlik üzerindeki etkisi tartışıldığında, devletlerin kendi sınırları içinde geliştirilen yapay zekâ teknolojilerini denetleme, takip etme ve hatta kamulaştırma olasılığı gündeme gelebilir. Aynı şekilde, uluslararası alanda bazı ülkeler, diğer devletlerin yapay zekâ çalışmalarını istihbarat faaliyetleri çerçevesinde ele geçirme veya etkisiz hale getirme stratejileri geliştirebilir. Ancak, mevcut istihbarat servisleri açısından açık bir tehdit olarak değerlendirilmemekte, ancak gelecekte bu bakış açısının değişme olasılığı bulunmaktadır. Bu bağlamda, bürokrasinin katılığından bağımsız hareket edebilen istihbarat servisleri, yapay zekâ üzerine akademik araştırmalar yürüten uzmanları veya bilgisayar mühendisliği alanında öne çıkan öğrencileri, sosyal ağ analizleri yoluyla potansiyel hedefler olarak belirleyebilir. Neticede, aksi bir senaryonun yaşanması, istihbarat alanında ciddi bir başarısızlığa yol açabilir.

Ulusal niceliksel teknoloji kaynaklarının (Üniversiteler, laboratuvarlar ve şirketler) paylaşılması, bu sektör düzeyinde birlikte çalışma hazırlanması ve personelin anında yetiştirilmesi ile çözümün ve çalışmanın yapılabilirliğinin anında değerlendirilmesi önemli bir adım olacaktır. Bu alanda en etkili birimlere bakıldığında dünyanın en etkili birimleri birbirinden farklılaşacak. Dünyanın en etkili birimleri yeterince trend tarafından yakından takip edilecek. (Gençoğlu, 2023, s. 14)

Yapay zeka teknolojisi sosyal ve ekonomik olmak üzere birçok alanda büyük değişikliklere yol açtı., askeri ve uluslararası alanları da kapsamaktadır. Bu teknoloji, hem ekonomik büyümeyi ve verimliliği artıracak ancak sosyal sorunlar, özellikle istihdam ve gelir eşitsizliği gibi konulara da neden olabilecektir. Yapay zekâ teknolojisinin uluslararası arenada yaygınlaşması, ülkelerin ekonomik ve askeri potansiyellerini etkileyerek yeni güç dengelerinin ortaya çıkmasına neden olabilecektir. Yapay zekâ teknolojisiyle ilgili etik kaygılar ve güvenlik sorunları da son derece önemlidir. Veri gizliliği, algoritmaların karar verdiği zamanlarda önyargılı kararlar ve adil olmayan sonuçlar gibi hususlar özellikle dikkate değerdir.

Otomatik silah sistemleri gibi askeri uygulamalar ve yapay zekâ sistemlerinin güvenliği ve siber güvenlik konularında etik Problemler bulunuyor. bu konuları değerlendirin ve yapay zekâ teknolojisinin insan merkezli ve adil bir şekilde geliştirilmesi, yasa koyucular, uygulayıcılar, bilim insanları, Sektör liderleri ve toplum kuruluşları için önemli bir görev olarak karşılaşılmaktadır. Yapay zekâ ayrıca sosyoteknik bir alandır. Sadece yatırımcıların, girişimcilerin, yazılım mühendislerinin değil. kamu otoritelerinin, sosyolog ve psikologların, avukatların, sosyal araştırmacılar ve hatta felsefecilerin dahil olması gereken bir teknoloji alanıdır. Kamu ve sivil toplumun yoğun kontrolüne ihtiyaç duyan yapay zekâ sistemlerinin, gelecekte toplumlara yapacağı etkiler konusunda net bir düşünce maalesef bulunmamaktadır. (Kurtuluş, 2023, p. 12)

Siber suç türleri

2000 yılında ABD Adalet Bakanlığı on bir türü onayladı:

- Bilgisayar verilerinin çalınması.
- Şifre trafiği.
- Hacker operasyonları ve Korsanlık
- Bilgisayar kullanarak ticari sırları çalmak.
- Taklit ticari markalar.
- Bilgisayar kullanarak para sahteciliği yapmak.
- Çocuk istismarının cinsel görüntüleri.
- İnternet dolandırıcılığı.
- İnternet üzerinden sıkıntı.
- İnternet üzerinden bomba tehditleri.
- İnternet üzerinden patlayıcı, ateşli silah veya uyuşturucu ticareti ve yasadışı fonlar. (Al-Hashemi, 2018, p. 24)

2.4. İnsan Güvenliği ve Yapay zekâ İlişkisi: 1994 UN İnsan Güvenliği Raporunun Perspektifinden

1994 Raporu, İnsan güvenliğini, güvenli limanlardan ziyade insanlarla, silahlardan ziyade gelişmeyle özdeşleştiren yeni bir tanım sunuyor. İnsan güvenliğinin

hem ülkelerin kendi içindeki güvenlik sorunlarını hem de küresel ölçekteki endişe verici gelişmeleri birlikte ele almaktadır. Rapor, bu endişeleri yeni bir sürdürülebilir insani gelişme düşüncesi, potansiyel barış getirisini yakalamak, yeni bir kalkınma iş birliği biçimi ve Küresel İşletme Yeniden Yapılandırma Sistemi aracılığıyla Hedefleri gerçekleştirir. (Birleşmiş Milletler, 1994)

1994 senesinde Birleşmiş Milletlerce yapılan İnsan Güvenliği Raporu, güvenlik tanımının sadece askeri tehditleri önlemekten ibaret olmadığını ve aynı zamanda ekonomik, gıda, sağlık, çevre gibi konuları da içerdiği görülebilmektedir. Bu rapor, daha bütüncül ve İnsan odaklı bir yaklaşımın seçilmesi gerektiğini vurgulayarak, bireylerin ve toplumların güvenliğinin sağlanmasına katkıda bulunmuştur.

Son yıllarda yapay zekânın insan güvenliği üzerindeki etkileriyle önemli bir rol oynadığı görülmektedir. 1994 BM raporu değerlendirildiğinde, yapay zekânın insan güvenliğine katkı sağlayabilecek alanlar olduğu kadar, aynı zamanda potansiyel tehditlerinin de mevcut olduğunu görülebilir.

- Sosyal Güvenlik: Yapay zekâ ve sosyal medya platformları, kişisel güvenliği önemli ölçüde artırabileceği gibi aynı zamanda ciddi tehditlere de yol açabilir. Örneğin, yapay zekânın veri analizi ve yüz tanıma gibi alanlarda kullanılması, güvenlik tehditlerinin hızlı bir şekilde tespit edilip önlenmesine yardımcı olabilir. Yine de, bu teknolojilerin gizlilik ihlallerine sebep olabileceği ve bireyleri haksız casusluğa maruz bırakabileceği söylenebilir.
- Ekonomik Güvenliği: Yapay zekâ destekli sosyal medya, e-ticaret ve hedefli reklamcılık gibi yeni ekonomik fırsatlarla bireylerin ekonomik güvenlik düzeyi arttırılmaktadır. Buna rağmen, yapay zekânın yaygın kullanımı özellikle rutin becerilere dayanan sektörlerde bazı grupları işgücü piyasasından geride bırakabilir ve ekonomik açığı artırarak ekonomik güvenliği olumsuz etkileyebilir.
- Kişisel güvenlik: açısından sosyal medya platformları, bireyler arasındaki etkileşimi güçlendirirken, aynı dönemde düşünce ve bilgi alışverişine olanak sağlıyor. Bu yönüyle yapay zekâ, toplumda tehdit oluşturabilecek şiddet ya da nefret gibi unsurları tanımlamak ve incelemek için yardımcı olabilir. Bu platformlar, bir araç olarak kullanıldığında sahte haberleri yayma ve

dezenformasyon, toplumların istikrarını bozma ve toplumsal güvenliği tehlikeye atma potansiyeline sahip olabilir.

- Siyasi Güvenlik: Sosyal medya platformları, siyasal nüfuzları nedeniyle insan güvenliğinde oldukça anahtar rol oynamaktadırlar. Yapay zekâ, seçim veri analizini geliştirerek ve seçim manipülasyonunu tespit ederek demokratik süreçleri iyileştirip güçlendirebilir. Aynı zamanda, bu araçlar siyasi güvenliği tehdit eden bir şekilde de kullanılabilirler seçim sonuçlarını etkilemek için büyük ölçekli dezenformasyon kampanyalarına ve siyasi yanlış bilgi yayılmasına yol açabilirler.
- Sağlık Güvenliği: Yapay zekâ, sağlık hizmetlerinde büyük bir devrim yaparak hasta takibi, erken Erken tanı ve tedavi planlama gibi alanlarda önemli faydalar sağlayabilir. Örneğin, sosyal medya üzerinden yayılan bir hastalık belirtisi gelişimini izleyen yapay zekâ algoritmaları, salgın hastalıkları erken dönemde tespit edip önleyebilir.
- 1994 Birleşmiş Milletler İnsan Güvenliği Raporu'nda geniş güvenlik anlayışı yeniden gözden geçirilmelidir. Yapay zekanın insan güvenliği ve güvenliği üzerindeki etkilerini dikkatli bir şekilde kontrol etmek için kapsamlı politika ve düzenleyici önlemler alınmalıdır. Bireylerin güvenliğini sağlamak, teknolojik yeniliği teşvik etmekten çok daha fazlasını gerektirir. Bu yeniliklerin insan merkezli bir yaklaşımla etkin bir şekilde entegre edilmesi de önemlidir.

ÜÇÜNCÜ BÖLÜM

VERİ GİZLİLİĞİ VE GÜVENLİK SORUNLARI

3.1. Veri Gizliliği: Tanımlar ve Kavramlar

Veri gizliliği, dijital zamanda bireylerin kişisel bilgilerinin korunmasıyla ilgili temel bir kavramdır. Temel olarak bireylerin kişisel verilerinin nasıl toplandığını, işlendiğini, saklandığını ve paylaşıldığını kontrol etme hakkı göz önünde bulundurulmalıdır. Dijital teknolojinin hızla gelişmesiyle birlikte, Tabii, işte tamamen farklı bir şekilde yeniden yazılmış hali, Günümüzde dijital dünyada veri gizliliği, her zamankinden daha kritik bir konu haline gelmiştir. İnternetin, sosyal medya platformlarının ve Yapay zeka teknolojisinin kullanılmaya başlanmasıyla birlikte kişisel verilerin toplanması ve kullanımı önemli ölçüde artmış, bu da bireylerin mahremiyetinin olası ihlalleri konusunda endişeleri artırmıştır.

Bu bağlamda, veri gizliliği kavramının zaman içerisinde değişim geçirdiği belirtilebilir. Örneğin, yirminci yüzyılda, veri gizliliği tamamen kişisel bir konu olarak görülüyordu, ancak teknolojinin ilerlemesi ve internet'in günlük yaşama girmesiyle birlikte, bu gizlilik bir bütün olarak toplumları etkileyen kamusal bir konu haline geldi. Altmışlı ve yetmişli yıllarda, şirketler ve devlet kurumları büyük miktarda veri toplamaya başladı ve ABD'de 1974 Gizlilik Kalkanı Yasası ve Avrupa Birliği'nde Genel Veri Koruma Tüzüğü (GDPR) gibi yeni yasaların kabul edilmesine yol açtı.

Bilgi teknolojileri ve bilgisayar sistemlerindeki verilerin, değiştirme, izinsiz giriş, ifşa edilme veya yok edilme gibi tehditlere karşı korunması olarak tanımlanan bir kavramdır. Bu, bilgisayar sistemlerindeki verilerin gizlilik, erişilebilirlik ve bütünlüğünü korumak için çeşitli teknolojik, organizasyonel ve yasal önlemleri kapsar. Veri güvenliği, kişisel verilerin ve finansal bilgilerin korunmasını değil aynı zamanda kurumsal verileri ve hassas bilgilerini de içerir. Bu, güvenlik duvarları, kimlik doğrulama, şifreleme, güvenlik politikaları ve yetkilendirme prosedürleri gibi farklı güvenlik önlemlerini içerebilir. Kişisel veri kavramına ilişkin olarak şunu açıkça söyleyebiliriz. genellikle adı, sosyal güvenlik numarası, banka kartı numarası, telefon numarası, web sitesi, posta adresi, doğum tarihi ve İnternet protokol adresleri gibi kişinin tanımlanmasına imkân tanıyan her türlü bilgiyi içerir ve buna da {IP} denir. (Ahmed H. H., 2020, s. 12)

Dijital çağda veri gizliliği her zamankinden daha önemli hale gelmiştir Gizlilik kavramı bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlar ve izinsiz erişimlerin önüne geçmeyi hedefler Örneğin özel bir mesaj gönderdiğini düşün Eğer yeterli güvenlik önlemleri alınmazsa bu mesaj başkaları tarafından okunabilir Bu yüzden bilgi güvenliğini oluşturan tüm unsurlar birbirine bağlıdır ve gizlilik ihlali tüm sistemi riske atabilir ,Bilgilerin korunması için şirketler ve kurumlar etkili gizlilik politikaları uygulamalıdır Aksi takdirde rakip firmalar veya kötü niyetli kişiler hassas verilere erişebilir Örneğin yeni bir ürün geliştiren bir firmanın bilgileri sızdırılırsa rakipler bu bilgileri kullanarak avantaj elde edebilir Bu nedenle gizliliğin ihmal edilmesi ciddi güvenlik sorunlarına yol açabilir

Gizlilik ilkesi üç temel noktaya odaklanır Yetkisiz kişilerin verilere erişmesini önlemek bilgilerin orijinal halini korumak ve verilerin güvenli bir şekilde saklanmasını ve paylaşılmasını sağlamak Kurumlarda çalışan herkes verilerin kopyalanmasını değiştirilmesini veya çalınmasını önlemek için dikkatli olmalıdır Kişisel bilgilerin yanlış ellere geçmesi hem bireyler hem de kurumlar için büyük riskler doğurur, Bilgilerin izinsiz kullanımı değiştirilmesi veya silinmesi bilgi güvenliğini doğrudan etkiler Bu yüzden verilerin korunması herhangi bir sektörde en önemli konulardan biri olarak görülmelidir Kurumlar gizlilik ilkelerini doğru bir şekilde uyguladığında hem iç hem de dış tehditlere karşı daha dayanıklı hale gelir,

Genel Veri Koruma Yönetmeliği (GDPR), dünya genelinde en sıkı gizlilik ve veri güvenliği düzenlemelerinden biri olarak kabul edilmektedir. Avrupa Birliği (AB) tarafından hazırlanıp yürürlüğe konulmuş olmasına rağmen, AB'de yaşayan bireylerin verilerini toplayan veya işleyen tüm kuruluşlar için bağlayıcı hükümler içermektedir. 25 Mayıs 2018 tarihinde yürürlüğe giren bu yönetmelik, gizlilik ve güvenlik kurallarını ihlal edenlere milyonlarca euroya varan ağır para cezaları uygulanmasını öngörmektedir. Bu düzenleme ile Avrupa Birliği, giderek daha fazla insanın kişisel verilerini bulut tabanlı hizmetlere emanet ettiği ve veri ihlallerinin giderek yaygınlaştığı bir dönemde, veri gizliliği ve güvenliği konusundaki kararlılığını ortaya koymaktadır. (GDPR), bazı ayrıntılara fazla girmese de geniş bir kapsam sunmakta olup, özellikle küçük ve orta ölçekli işletmeler (Küçük ve Orta Büyüklükteki İşletmeler) için uyum sürecini oldukça zorlu bir hale getirmektedir. (wolford, 2024)

Amerika Birleşik Devletleri'ndeki 1974 tarihli Gizlilik Koruma Yasası, Bireylere özel verileri üzerinde kontrol hakkı tanıyan temel haklar sunar. Bu, federal

kayıtları yöneten 1974 tarihli Gizlilik Yasası'nda (5 USC 552'a ile değiştirildiği şekliyle) açıklanmıştır. Bu yasa, Gizlilik Yasası (SOR) kayıt sisteminde tutulan ve ad, Kişisel veriler, bireyleri tanımlamaya yarayan ve onlar hakkında bilgi sağlayan her türlü kaydı kapsar. Bu veriler arasında en yaygın olanları, resmi kimlik numaraları ve sosyal güvenlik kayıtları gibi benzersiz tanımlayıcılardır. Aynı zamanda, bireyleri doğrudan veya dolaylı olarak tanımlayabilen diğer kodlar ve referans numaraları da bu kapsama girer. Bir kişi, kayıtlarına erişme ve mümkünse bu kayıtların düzeltilmesini talep etme hakkına sahiptir. Yasak Gizlilik Yasası: Bu tür kayıtları, kayıtların ilgili olduğu kişilerin yazılı izni olmadan ifşa edilmesini yasaklamaktadır.

3.2. Gizlilik Tanımları ve Kavramları

Dijital gizlilik bir kişinin dijital ortamlarda yayınlanan ve dolaşan kişisel verilerinin korunmasının tanımı olarak tanımlanmaktadır. Kimlik bilgileri ve iletişim verileri (e-posta adresleri dahil) Özel fotoğraflar ve görsel içerikler Finansal bilgiler ve bankacılık verileri, iş ve ikamet bilgileri ile tüm bilgilerle temsil edilmektedir. Bilgisayar, cep telefonu veya internetteki Dijital iletişim platformları kullanımı sırasında etkileşimde kullanılan verileri temsil etmektedir. (Saad A. M., 2021, s. 12)

Etik olarak mahremiyet, insan onuru kavramıyla bağlantılıdır. Bir kişinin mahremiyetinin ihlali, kişinin özgürlük ve haysiyetine yönelik bir saldırıdır. Bu kavram, profesyonellerin müşterilerinin veya hastalarının bilgilerini izinsiz olarak ifşa etmelerinin yasak olduğu tıbbi gizlilik veya bankacılık gizliliği gibi mesleki etik kurallarda da kendini göstermektedir.

Gizlilik kavramı, bireylerin özel yaşam alanlarını belirleyen ve bu alanlarda özgürce karar verebilme hakkını ifade eder. Bu hak, kişilerin kendilerine ait bilgileri kontrol edebilme ve kimliklerini koruyarak sosyal ilişkilerini yönetebilme kapasitesini içerir. Gizlilik hakkının etkin şekilde kullanılması bireylerin, kendilerine ait egemen alan içinde mahremiyet olgusunu temsil etmektedir. Böylece verdiği kararlara saygı mahremiyet kavramı, kişilerin yaşam tarzlarıyla ilişkilendirilir ve dolayısıyla kalabalık topluluklar arasında ya da yalnız olarak yaşamanın tercih edilmesiyle ilgilidirMahremiyet hem bireylerin haklarını temsil eder hem de diğer topluluklarla ilişkilerini ortaya koyabilir.

Teknoloji dünyasında gizlilik kavramı son yıllarda önemli bir evrim geçirdi. Dijital çağın başlangıcını oluşturan internetin keşfi ve ardından sosyal medya

platformlarının küresel ölçekte yaygınlaşması, iletişim modellerinde köklü bir değişime yol açtı, bireyler mahremiyetlerinin ihlallerine karşı daha savunmasız hale geldi. Facebook ve Twitter gibi platformlar büyük miktarda kişisel veri toplayarak bu verilerin nasıl kullanıldığı konusunda ciddi endişelere yol açmakta. Örneğin, 2018 yılında, Facebook'taki milyonlarca kullanıcının verilerinin siyasi amaçlar için bilgileri olmadan istismar edildiği Cambridge Analytica Skandalı ile ortaya çıkmıştı.

3.3. Sosyal Medya Platformlarının Veri Güvenliği ve Veri Gizliliği Üzerindeki Etkisi

Facebook, Twitter (X) ve Instagram gibi sosyal medya platformları, dijital çağda veri güvenliği ve gizlilik risklerinin önde gelen itici güçler arasında yer almaktadır. Bu platformlar, kullanıcılarının verilerini sürekli olarak toplar ve bu verileri kullanıcı deneyimini iyileştirmek ve reklamları hedeflemek için kullanır. Ancak aynı zamanda bu süreç, bireylerin mahremiyetinin ciddi şekilde ihlal edilmesine de sebep olmaktadır.

Bilişim teknolojisinin kişisel verilerin gizliliği üzerindeki etkisi, bilişim alanındaki muazzam teknik gelişme çerçevesinde, devlet daireleri, kurumları ve ajansları ile özel şirketler tarafından toplanan büyük miktarda kişisel verinin alınması, depolanması ve analiz edilmesi mümkün olmuştur. Dahası, otomatik bir dosyada saklanan bilgiler, başka bir veri tabanındaki bilgilerle karşılaştırılabilir ve ülke genelinde saniyeler içinde ve kıyasla düşük maliyetlerle aktarılabilir, bu da gizlilik tehdidinin ne ölçüde olabileceğini açıkça ortaya koymaktadır. Kamera kontrol teknolojileri, kimlik kartları ve elektronik kimlik kişisel veri tabanları, postaları ele geçirme ve sansürleme araçları, çalışma ortamının izlenmesi, iletişim ve diğerleri gibi gizliliği tehdit eden artan kaynaklara ek olarak gösterilebilir. Bilişim alanındaki gelişme, bireylerin özel hayatlarına dair kişisel verilerin toplanması ve işlenmesi alanında, bireylerin ekonomik, bilimsel, sosyal ve diğer işlerinin devlet tarafından düzenlenmesi alanında olumlu bir etki meydana getirmişse de bu da veri bankaları olarak bilinen şeyin varlığının temel nedenidir. Veri bankaları, belirli bir konuya yarar sağlayan ve belirli bir amaca hizmet etmeyi amaçlayan bir veri tabanının oluşturulması ve elektronik bilgisayarlar tarafından işlenerek belirli amaçlar için farklı kullanıcılara yarar sağlayan bilgiler şeklinde üretilmesi ve teknik açıdan bilgisayarın veya bilgisayarın verilerin kaydedilmesi ve sınıflandırılmasından çeşitli işlemleri anlamına gelir.

Bu olumlu etkiyle birlikte, olumsuz etki, özel yaşam hakkının korunması ve toplumun kişisel verilerin toplanması, işlenmesi ve saklanması ihtiyaçları arasında mutlaka bir denge bulunması ve bu verilerin işleme tekniklerinin yasa dışı kullanımının risklerinden korunmasını sağlamak için uyulacak ilke ve kuralları bulmak için uluslararası, ulusal ve bölgesel çabaları harekete geçiren kişisel verilerin yasa dışı kullanımı ve bireylerin özel yaşam hakkına yönelik ihlal döngüsünün genişlemesi gibi gerçek vakalarda temsil edilmektedir. (Ahmed K. H., 2020, s. 66)

2018'deki Cambridge Analytica Skandalı'ndaki gibi örnekler, kişisel verilerin yasa dışı yollarla nasıl kullanılabileceğini göstermesi yönüyle önemli bir kriterdir. Etkinlikte şirket, Cambridge Analytica adlı veri analiz şirketi, kullanıcıların bilgisi ve onayı olmadan yaklaşık 87 milyon Facebook kullanıcısının kişisel verilerine erişim sağladı. Elde edilen bu veriler, özellikle ABD ve İngiltere'deki seçim süreçlerini etkilemek amacıyla kullanıldı.. Bu skandal, veri toplamanın daha sağlıklı bir şekilde düzenlenmesi ve kullanıcıların gizliliğinin korunması ihtiyacını vurguladı.

(The New York Times) ve (The Guardian'ın raporları), Cambridge Analytica'nın, İngiltere ve ABD'deki hedeflenen seçmenlere reklam vermek için Facebook aracılığıyla çok miktarda kişisel veri kullandığını gösterdi. Bu bilgiler bir araştırmacı tarafından Facebook'tan elde edildi ve daha sonra Cambridge Analytica'ya satıldı. Facebook, uygulamanın hizmet şartlarının ihlali olduğunu söylese de bu olay, veri toplama çağında veri korumayla ilgili önemli soruları gündeme getirdi. (Accessnow., 2018)

Ayrıca, bu platformlardan veri sızıntısı artık yaygınlaştı. 2019 yılında, yüz milyonlarca Facebook kullanıcısının verileri bir güvenlik açığı nedeniyle sızdırıldı ve hassas bilgiler riske atıldı. Bu tür bir olay, sosyal medya platformlarındaki güvenlik önlemlerinin zayıflığını gösterir ve bu platformların kullanıcılarının verilerini koruma yeteneği hakkında soruları gündeme getirir. Olumlu tarafı ise yapay zekânın veri güvenliğini artırmada önemli bir rol oynayabilir olmasıdır. Örneğin, makine öğrenimi teknikleri, siber saldırıları erken aşamalarında tespit etmek için kullanılabilir. Ancak öte yandan yapay zekâ, milyonlarca insanın görüntülerini içeren devasa veri tabanlarına dayanan yüz tanıma teknolojilerinde olduğu gibi gizliliği ihlal etmek için de kullanılabilir.

DÖRDÜNCÜ BÖLÜM

SOSYAL MEDYA PLATFORMLARI:TANIMLAR VE KAVRAMLAR

4.1. Sosyal Medya Platformlarının Tanımı ve Kavramları

Sosyal medya, bireylerin dijital bir ekosistem içerisinde birbirleriyle etkileşime girebildiği, paylaşım yapabildiği ve içerik yaratabildiği internet tabanlı uygulamalar bütünüdür. Sosyal medya araçları bireylerin günlük yaşamlarının ayrılmaz bir parçası haline gelmiş ve toplumsal iletişimin dinamiklerini kökten değiştirmiştir. Bu platformlar, kısa mesajlardan görsel ve video içeriklerine kadar geniş bir yelpazede iletişim olanakları sunarak kullanıcı deneyimini sürekli zenginleştiriyor.

Elektronik iletişim sistemlerinin tarihsel gelişimi 1970'lerin başında e-posta ve sohbet programlarının ortaya çıkışıyla başlamıştır. Ancak, 1979 yılında USENET tartışma ağının kurulmasına kadar sürekli ve organize çevrimiçi topluluklar oluşmamıştır. USENET sistemi, kullanıcıların belirli konu başlıkları altında (haber grupları) mesaj alışverişi yapabilmesine olanak tanıyarak dijital iletişimde önemli bir dönüm noktası oluşturmuştur. Bu dönemde, Bülten Tahta Sistemleri (BBS'ler) gibi diğer tartışma platformları da kullanıma sunulmuştur. Ancak bu sistemler, genellikle sınırlı erişime sahip ve birbirinden bağımsız çalışan yapılar olarak kalmıştır. 1993 yılında Mosaic web tarayıcısının piyasaya sürülmesi, internet kullanımında çığır açan bir gelişme olmuştur. Bu tarayıcı, kullanıcı dostu grafik arayüzü sayesinde internet deneyimini büyük ölçüde kolaylaştırmıştır. World Wide Web'in yapısı, kullanıcıların tek bir tıklamayla farklı siteler arasında kolayca gezinebilmesine imkân tanımıştır. Ayrıca, gelişen internet bağlantı hızları, metin ağırlıklı içeriklerin ötesine geçerek zengin multimedya içeriklerinin yaygınlaşmasını sağlamıştır. Bu gelişmeler, çevrimiçi iletişim ve bilgi paylaşımını temelden dönüştürerek günümüz internet ekosisteminin temellerini atmıştır.

Web teknolojisini temel alan sosyal medya ağlarını kuran ilk şirketler Classmates.com ve 1995 yılında kurulan SixDegrees.com. Classmates.com, web sörfçülerini sitesine çekmek için agresif bir pop-up reklam kampanyası kullandı. Sosyal ağını, lise ve üniversite mezuniyet sınıflarının üyeleri, silahlı hizmet şubeleri ve işyerleri arasındaki mevcut bağlantıya dayandırdı. SixDegrees.com ilk gerçek sosyal ağ sitesiydi. 1997 yılında, bu tür siteleri karakterize edecek özelliklerin çoğuyla

piyasaya sürüldü: üyeler kendileri için profiller oluşturabilir, arkadaş listelerini tutabilir ve sitenin özel mesajlaşma sistemi aracılığıyla birbirleriyle iletişim kurabilir. SixDegrees.com, 2000 yılına kadar üç milyondan fazla kullanıcıyı çektiğini iddia etti, ancak bu sayıları gelire dönüştüremedi ve balon o yıl e-ticaret şirketlerinin hisseleri için patladı.

Bununla birlikte, sosyal medya siteleri 21. yüzyılın ilk yıllarında dijital iletişim alanında önemli gelişmeler yaşanmıştır. Bu dönemde, insanların çevrimiçi ortamlarda sosyal bağlantılar kurmasını sağlayan platformlar ortaya çıkmıştır. Friendster ve MySpace gibi öncü sosyal ağlar, kullanıcıların kişisel ilişkilerini dijital ortama taşımalarına olanak tanımıştır. Zaman içinde bu platformların yerini, küresel ölçekte yaygınlaşan Facebook almıştır. Facebook'un kullanıcı sayısı hızla artarak milyarlara ulaşmış ve platform dünya çapında en çok tercih edilen sosyal medya araçlarından biri haline gelmiştir. Belirli içerik türlerinin paylaşılması için başka sosyal medya biçimleri ortaya çıktı. Video paylaşımı alanında YouTube ve TikTok gibi platformlar kullanıcıların görsel içerikler oluşturmasına ve paylaşmasına imkan sağlamıştır. Özellikle TikTok, kısa formatta video paylaşımı konusunda uzmanlaşmış bir platform olarak öne çıkmıştır. LinkedIn, kullanıcıların özgeçmişlere benzer yapıda sayfalar oluşturarak bir kullanıcının profesyonel bağlantılar kurmasını sağladı. (El Şair, 2015, s. 63)

4.2. Sosyal Medya Platformlarının Özellikleri

Sosyal media bireylerin içerik oluşturmasına, paylaşmasına etkileşimde bulunmasına ve iletişim kurmasına imkân tanıyan dijital hizmetlerdir. İşte sosyal medya platformlarının temel özellikleri:

- Kullanıcı Merkezli İçerik Üretimi: Sosyal medya platformları, kullanıcıların içerik üretmesine, paylaşmasına ve yorum yapmasına imkân tanır. Kullanıcılar aynı zamanda diğer kullanıcılarla etkileşimde bulunabilir.
- İki Yönlü İletişim: Geleneksel medya tek yönlü iletişim sağlarken, sosyal medya platformları iki yönlü iletişime imkân tanır. Kullanıcılar sadece içerik tüketicisi değil, aynı zamanda içerik üreticisidir.
- Etkileşim ve Topluluk Oluşturma: Sosyal medya platformları, kullanıcıların ilgi alanlarına göre topluluklar oluşturmasına imkân tanır. Bu topluluklar, ortak ilgi alanlarına sahip insanların bir araya gelmesine imkân tanır.

- Veri Toplama ve Analiz: Sosyal media bireylerin davranışları ve etkileşim kalıpları hakkında büyük miktarda veri topluyor ve bu bilgileri hassas bir şekilde analiz ederek kullanıcı deneyimini iyileştiriyor ve her bir bireye gösterilen içeriği ilgi alanlarına göre özelleştiriyor. (Aljazeera., 2024)

4.3. Sosyal Medya Türleri ve Örnekleri

Günümüz dijital dünyasında sosyal medya, bireylerin günlük iletişim aracı olmasının ötesinde, markalar için vazgeçilmez bir pazarlama ve etkileşim alanı hâline gelmiştir. Facebook, Instagram, Twitter (X), LinkedIn ve YouTube gibi platformlar, her biri farklı kitlelere hitap etse de, markaların dijital kimliğini oluşturma ve güçlendirme noktasında kritik bir rol üstlenmektedir. Bu nedenle, etkili bir sosyal medya yönetimi sadece çevrimiçi varlığı korumak değil, aynı zamanda doğru hedef kitleye ulaşarak uzun vadeli sadakat oluşturmaktır.

4.3.1. Facebook'un Sosyal Medya Stratejilerindeki Rolü

Facebook, bugün artık sadece bireysel kullanıcıların değil. küçük işletmelerden küresel markalara kadar her ölçekteki kurumun aktif olarak kullandığı stratejik bir platformdur. Geniş kullanıcı kitlesi, hedeflenebilir reklam olanakları ve detaylı analiz araçları sayesinde Facebook, dijital pazarlamanın merkezinde yer almaktadır. Ancak bu potansiyelden tam anlamıyla yararlanabilmek için platformun dinamiklerine hâkim, veri odaklı bir yönetim anlayışı gerekmektedir.

Başarılı bir Facebook yönetimi içerik planlamasından reklam kampanyalarına, kullanıcı etkileşiminden performans ölçümüne kadar birçok aşamayı kapsar. Burada amaç, yalnızca içerik üretmek değil hedef kitlenin ilgisini çekecek doğru mesajları, doğru zamanda ve doğru formatta sunmaktır. Bu süreçte, profesyonel sosyal medya yöneticileri, elde edilen verileri analiz ederek kampanyaları optimize eder ve markanın dijital alandaki etkisini artırır. İster yerel pazarda faaliyet gösteren bir işletme olun, ister küresel ölçekte hizmet veren bir marka. Facebook üzerindeki varlığınızı profesyonel bir şekilde yönetmek, dijital rekabette öne çıkmanız için kritik bir adımdır. Doğru stratejiyle yürütülen kampanyalar sayesinde, marka bilinirliği artar, kullanıcılarla daha sağlam bir bağ kurulur ve satış hedeflerine ulaşmak daha kolay hâle gelir.

4.3.2. Twitter'ın sosyal medya platformlarında bilgi aktarımı alanındaki stratejik konumu

Twitter, dijital iletişim ağları içinde özgün yapısıyla dikkat çekmektedir. Platformun temelini oluşturan 280 karakterlik sınırlama, kullanıcıların düşüncelerini özlü ve vurucu biçimlerde ifade etmelerine olanak tanırken, aynı zamanda bilgi akışının hızını ve yoğunluğunu artırmaktadır. Bu yapı sayesinde Twitter, yalnızca bireysel paylaşımlar için değil kurumların hedef kitleyle doğrudan temas kurmasında da etkili bir araca dönüşmüştür. Özellikle haberlerin yayılması, kamuoyunun yönlendirilmesi ve gündem oluşturmada gösterdiği yüksek etki, platformu hem bireysel hem de kurumsal iletişim stratejilerinin ayrılmaz bir parçası hâline getirmiştir. Bu bağlamda, Twitter üzerinden yapılan paylaşımlar, yalnızca içerik sunmakla kalmayıp, dikkat çekici bir dil ve görsel öğelerle desteklendiğinde hedef kitle üzerinde daha güçlü bir izlenim bırakmaktadır. Pazarlama alanında etkili bir sonuç elde edebilmek için kullanılan dilin sade ve etkileyici olması kadar, seçilen görsellerin mesajı desteklemesi de büyük önem taşır. Hashtag kullanımı ise içeriklerin görünürlüğünü artıran ve ilgili topluluklara erişimi kolaylaştıran stratejik bir unsurdur. Bu nedenle Twitter yönetimi yalnızca teknik bir süreç değil. aynı zamanda içerik, zamanlama, hedef kitle analizi ve etkileşim unsurlarının bir arada değerlendirildiği bütüncül bir strateji olarak ele alınmalıdır. Markaların sosyal medya platformları üzerinden yürüttüğü kampanyalarda, Twitter'ın sunduğu hız ve erişim potansiyeli, mesajların etkili biçimde yayılmasını sağlamaktadır. Karakter sınırlaması gibi görünürde bir kısıtlama dahi, yaratıcı içerik üretimi açısından bir avantaja dönüşebilmekte. bu da kullanıcıların dikkatini çeken, paylaşmaya değer mesajların öne çıkmasını beraberinde getirmektedir. (Gloddia, 2024)

4.3.4. Instagram'ın Sosyal Medya Yönetimindeki Rolü ve Etkileşim Gücü

Görsel odaklı yapısı ve kullanıcı dostu arayüzü sayesinde Instagram, özellikle genç kuşak ile markalar arasında doğrudan ve samimi bir iletişim alanı sunmaktadır. Platformun bu özelliği, kullanıcıların yalnızca içerik tüketicisi değil. aynı zamanda aktif birer katılımcı hâline gelmesine olanak tanır. Özellikle Y kuşağı bireylerinin, marka deneyimlerine önem vermesi ve görselliğe dayalı içeriklere daha yüksek düzeyde tepki göstermesi, Instagram'ı bu demografik kitleye ulaşmak isteyen kurumlar açısından değerli kılmaktadır. Aylık aktif kullanıcı sayısının bir milyarı aşması ve her gün milyonlarca görselin paylaşılıyor olması, platformun içerik üretimi ve yayılım

potansiyelini ortaya koymaktadır. Bu bağlamda, stratejik olarak planlanmış bir içerik yönetimi, markaların görünürlüğünü artırmakla kalmaz. aynı zamanda hedef kitleyle sürdürülebilir ve anlamlı bir bağ kurulmasını da mümkün kılar.

Instagram üzerinden gerçekleştirilen sosyal medya yönetiminde görsel anlatım kadar, etkileşim unsurlarının (yorumlar, beğeniler, hikâyeler) da dengeli bir şekilde değerlendirilmesi gerekmektedir. Hedef kitleye yönelik özgün ve dikkat çekici içerikler üreten profesyonel ekipler, yalnızca estetik açıdan güçlü paylaşımlar yapmakla yetinmez. aynı zamanda platformun algoritmalarını ve kullanıcı davranışlarını analiz ederek, erişimi en üst seviyeye çıkarmaya yönelik stratejiler geliştirir. İster dönüşüm oranlarını artırmayı hedefleyen bir reklam kampanyası, ister marka bilinirliğini genişletmeye yönelik organik bir içerik stratejisi olsun Instagram'ın sunduğu araçlar, görsel anlatımı merkeze alan etkili bir iletişim dili oluşturmak için uygun bir zemindir. Bu nedenle, başarılı bir Instagram yönetimi, teknik uzmanlıkla yaratıcı vizyonun birleşimini gerektirir. Bu yaklaşım, yalnızca takipçi sayısını artırmakla kalmaz, aynı zamanda marka sadakatinin güçlenmesine ve kullanıcı etkileşiminin kalıcı hâle gelmesine de katkı sunar.

Bir influencer'a ihtiyaç vardır ve bu da şirketlerin hedeflerine ulaşması için şirketlere sosyal medya yönetiminde rehberlik edebilir. Instagram ekibi, markaların Instagram sosyal medya yönetimi stratejilerini geliştirirken karşılaştığı birçok tuzağın farkında olmalıdır. Mobitek çatısı altında yer alan sosyal medya yönetimi hizmetleri, kullanıcı işletmelerin içerik üretimi ve reklamcılıkta büyük bir avantaj elde etmesini sağlar. (El Şair, 2015, s. 66)

4.3.5. YouTube'un Sosyal Medya Yönetimindeki Stratejik Kullanımı

YouTube. Dünya çapında kullanıcı sayısı bakımından Facebook'tan sonra ikinci büyük sosyal medya platformu ve en büyük çevrimiçi video platformudur. 2005 yılında kurulan kanalın ilk yüklenen videosu 18 saniye uzunluğundaydı. Aynı zamanda, Google'dan sonra en çok tercih edilen ikinci arama motoru özelliğini taşımaktadır. Bu platform, hem sosyal ağ hem de bilgi erişimi açısından küresel internet kullanıcılarının vazgeçilmez araçlarından biri haline gelmiştir. (Pasha, 2020, s. 28)

Ayrıca Profesyonel sosyal medya yönetimi kapsamında yürütülen YouTube çalışmaları, video prodüksiyonu, optimizasyonu, etkileşim analizi ve reklam yönetimi

gibi pek çok boyutu içermektedir. Böylece, şirketlerin YouTube kanalları, hem içerik pazarlamasının hem de hedef kitle ile olan bağın kuvvetlenmesinde etkili bir araç hâline gelir. Bu çok katmanlı yaklaşım sayesinde, platformun sunduğu olanaklar maksimum düzeyde değerlendirilebilir ve marka değerine uzun vadeli katkılar sağlanabilir.

4.3.6. TikTok'un Sosyal Medya Yönetimindeki Rolü

TikTok, özellikle genç ve enerjik bir kullanıcı kitlesine sahip bir platformdur. Bu platform, markaların genç tüketicilere doğrudan ulaşmalarını sağlarken, aynı zamanda bu kitleyle etkili bir şekilde etkileşimde bulunarak markaların gücünü artırmalarına olanak tanır. TikTok, içeriklerin hızlı bir şekilde yayıldığı ve kullanıcıların aktif olarak katıldığı bir alan sunarak, markaların hedef kitlesiyle güçlü bir bağ kurmalarını mümkün kılar.<CITATION mob24 \l 1033 (Mobitek., 2024)>

Uygulama, Tik Tok'un Amerikalılar hakkında Çin hükümetine teslim edilebilecek ve ABD vatandaşlarını gözetlemek için kullanabilecek bilgiler topladığına dair endişelerin ortaya çıkması üzerine Trump yönetiminin ve ABD hükümetinin diğer bölümlerinin dikkatini çekti. <CITATION Alh20 \l 1055 (Alhurra, 2020)>

Kanada, Avrupa Birliği ve Amerika Birleşik Devletleri'nden gelen benzer hamlelerin ardından Şubat 2023'te uygulamanın devlet tarafından verilen tüm telefonlara indirilmesini yasakladı ve Kanada hükümeti, kararının gizlilik ve güvenlik için kabul edilemez bir risk düzeyini temsil eden uygulamanın gözden geçirilmesinden kaynaklandığını söyledi. O sırada Başbakan Justin Trudeau, yasağı olası bir ilk adım olarak açıkladı, ancak aynı zamanda hükümetin atması gereken tek adım olabileceğini de söyledi. İngiltere, devlet bilgilerinin güvenliğinden endişe ederek geçen yıl hükümet bakanları ve memurları için Tik Tok Yasağı'nı tüm kamuoyuna duyurdu. İngiliz Parlamentosu, uygulamayı ağına bağlı cihazlarda ve elektronik cihazlarda hızla yasakladı. <CITATION Alh24 \l 1055 (Alhurra, 2024)>

4.4. Sosyal Medya Platformlarında Veri Gizliliği ve Güvenlik Sorunlarının Fırsatları ve Zorlukları

4.4.1. Yapay zekânın veri analitiğinde sunduğu fırsatlar

Günümüzün bilgi tabanlı toplumunda veri, hayatın her alanında önemli bir rol oynamaktadır. Özellikle dijital teknolojilerdeki gelişmeler, veri toplama, işleme ve

yorumlama süreçlerini kökten değiştirmiştir. Bu gelişmeler, Bilişim ve iletişim teknolojileri alanında sağlanan başarılar sayesinde gerçekleşmiştir.

Veri bilimi, geçmiş, mevcut ve gelecekteki verilerden anlamlı bilgiler elde etmeyi amaçlayan bir disiplindir ve bilgisayar bilimi, programlama, matematik ve istatistik gibi alanları bir araya getirir. Bu alanda yapılan çalışmalar, verileri düzenli hale getirmek ve doğru bir şekilde analiz etmek için yeni yöntemler geliştirmeye yöneliktir.

Yapay zekâ, veri bilimi alanından yararlanan önemli bir teknolojidir. Veri toplama ve analiz süreçlerini hızlandırarak, daha doğru sonuçlar elde edilmesine olanak tanır. İnsan gücünü minimum düzeye indirerek, dijital platformlardan elde edilen verilerin merkezi bir sistemde toplanmasını ve istenilen amaç doğrultusunda analiz edilmesini mümkün kılar. Bu özellik, yapay zekâyı işletmeler ve kamu kurumları için vazgeçilmez bir teknoloji haline getirmiştir. Veri madenciliği kavramı, verinin işlenerek değerli bilgiler haline getirilmesini ifade eder. Bugün birçok platform, kullanıcılarından topladığı veriler ile bu bilgileri kullanarak farklı stratejiler geliştirmektedir.

Facebook, yıllardır kullanıcı verilerini toplamakta ve bu veriler sayesinde kişilerin alışkanlıkları hakkında derinlemesine bilgiye ulaşmaktadır. Yapay zekâ teknolojileri, bu verilerin hızlı ve verimli bir şekilde analiz edilmesine olanak tanımaktadır. Yapay zekâ teknolojisinin veri analitiği alanındaki kullanımının artmasıyla birlikte, verilerin daha karmaşık yapıları da çok daha kısa sürede işlenebilecektir. Bu da veri analizinin daha etkili ve güvenilir sonuçlar vermesini sağlayacaktır. <CITATION map20 \l 1033 (Maptriks., 2024)>

4.4.2. Yapay zekânın güvenlik sorunlarında ve tehdit algılama sistemlerinde kullanımı

Sosyal medya platformları birçok güvenlik sorunuyla karşı karşıya gelebilmektedir. Veri ihlalleri, yanlış bilgi, kimlik hırsızlığı ve haberlerin yayılması gibi sorunlar özellikle dikkat çeker. Sosyal medya platformlarının güvenlik önlemlerinin yetersiz olduğu veri ihlalleri ortaya çıkabilir ve bu yetkisiz kişilerin kişisel verilere erişmesine neden olabilir. Sosyal medyanın yaygın bir sorunu olan kimlik hırsızlığı, kullanıcıların kişisel bilgilerinin çalınmasına ve Kötü niyetli insanlar tarafından kullanılmasına yol açabilir. Toplumsal olayları yanlış bir yöne kaydırarak, sosyal medyanın güvenilirliğini zedeleyebilecek olan, yayılmış olan yanlış bilgi ve

haberlerdir. Bütün bireyler özel veya kamu mülklerini hırsızlıktan, tahrifattan ve vandalizme karşı koruma konusunda isteklidir. İster kâğıt ister elektronik olsun, bireylerin doldurduğu çeşitli formlardaki bilgiler, kurumların kaydetmek ve korunması için büyük miktarlarda para harcanan varlıklar. Bu nedenle elektronik bilgi mülkiyettir ve bireyler onu korumak için elektronik sistemlerin (onu taşıyan bilgisayar sistemleri ve onu ileten elektronik ağlar) güvenliğini sağlamakla mükelleftir. (Sami, 2008, s. 7)

Sosyal medyada veri güvenliği ve gizlilik konuları oldukça önemlidir çünkü milyonlarca insan bu platformlarda Kişisel bilgilerin paylaşılması ve bu bilgilerin güvenliğinin sağlanması, Dijital teknolojilere giderek daha fazla bağımlı hale geldiğimiz bir dünyada, siber tehditlere karşı korunmak, bireylerin, işletmelerin ve hükümetlerin karşı karşıya olduğu en önemli zorluklardan biri haline gelmiştir. Siber saldırılar daha karmaşık ve sofistike hale geldikçe, geleneksel araçlar artık bunlara karşı koymada yeterli olmuyor ve uzmanları gelişmiş ve etkili bir çözüm olarak yapay zeka teknolojilerine yönelmeye yöneltiyor. Yapay zeka, devasa miktardaki verileri ışık hızında analiz etme yeteneğiyle siber güvenlik alanında bir paradigma değişimini temsil ediyor. Geleneksel sistemler tehditleri tespit etmek için önceden tanımlanmış kurallara güvenirken, yapay zeka geçmiş kalıplardan ders çıkarabilir, şüpheli davranışları belirleyebilir ve hatta saldırılar gerçekleşmeden önce bunları tahmin edebilir. Bu özellikler onu, insanların veya geleneksel yazılımların tespit etmesinin zor olduğu yeni ortaya çıkan tehditlere karşı hayati bir araç haline getirmektedir.

Aşağıda, tehditleri tespit etme ve bunlara yanıt vermede yapay zeka uygulamaları yer almaktadır:

- **Saldırı tespit sistemlerini geliştirmektir (Intrusion Detection Systems)**

Yapay zeka sistemleri, yalnızca bilinen tehdit listelerine güvenmek yerine ağ trafiğini izleyebilir, olağandışı davranışları analiz edebilir ve şüpheli etkinlik tespit edildiğinde anında uyarılar verebilir. Örneğin, sistem belirli bir cihazın olağandışı zamanlarda hassas dosyalara erişmeye çalıştığını veya büyük miktarda verinin harici bir sunucuya aktarıldığını fark ederse, bu cihazı izole etmek veya güvenlik görevlilerini bilgilendirmek için otomatik eylemler gerçekleştirebilir.

- **Kimlik avı (Phishing)**

Yapay zeka, kullanıcıları bilgilerini çalmaları için kandırmaya dayanan saldırılarla mücadelede önemli bir rol oynar. Doğal dil işleme (NLP) teknolojileri sayesinde, şüpheli e-postaların ve web sitelerinin içeriği, kimlik avı ifadelerini veya kötü amaçlı bağlantıları tespit etmek için analiz edilebilir. Bazı gelişmiş sistemler, kullanıcılar için daha net uyarı mesajları oluşturmak için insan yazımını taklit edebilir ve bu saldırıların kurbanı olma şanslarını azaltır.

- **Derin Öğrenme Teknikleri (Deep Learning)**

Yapay zekayı kullanarak kodu analiz edebilir ve kötü amaçlı yazılımlar arasındaki ortak özellikleri belirleyebilir ve benzer kalıplara dayalı yeni tehditleri tanımasına olanak tanır. Kötü amaçlı yazılımlara karşı mücadelede yapay zeka, daha önce hiç tespit edilmemiş olanlar da dahil olmak üzere virüsleri ve kötü amaçlı yazılımları tespit etmek için gelişmiş bir çözüm sunar.

- **Kimlik avı saldırıları (Adversarial Attacks)**

Yapay zekanın siber güvenlikte kullanımı zorluklar olmadan değildir. Bu zorlukların en öne çıkanlarından biri, bilgisayar korsanlarının yapay zeka sistemlerini kendilerine girilen verileri yanlış kararlar vermelerine neden olacak şekilde değiştirerek yanıltmaya çalışmalarıdır. Örneğin, bir görüntü veya yazılım dosyası, kötü amaçlı olmasına rağmen sistemin onu güvenli kabul etmesi için biraz değiştirilebilir. Bu tür saldırılar, daha esnek ve uyarlanabilir yapay zeka sistemlerinin geliştirilmesini gerektirir. Ayrıca gizlilik konusu, özellikle ağların izlenmesi ve kullanıcı davranışlarının analiz edilmesi söz konusu olduğunda büyük bir endişe kaynağı olmaya devam etmektedir. Bu tür bir gözetim, içeriden gelen tehditleri tespit etmek için gerekli olsa da, veri toplama ve kullanımının sınırları hakkında soru işaretleri doğurabilir. Burada, güvenliğin güçlendirilmesi, açık etik ve yasal kontrollerle bireylerin haklarının korunması ile dengelenmelidir. Şirketlerin altyapıya, teknolojilere ve nitelikli insan kaynaklarına önemli yatırımlara ihtiyaç duyması nedeniyle yüksek maliyet, yapay zeka çözümlerinin yaygın olarak kullanılmasının önündeki bir başka engeldir. Yapay zekaya önemli ölçüde güvenmek, insan unsurunun rolünü azaltabilirken, bağlamın dikkatli bir şekilde anlaşılmasını gerektiren karmaşık kararlar almak için insan uzmanlığı gereklidir. Bu zorluklara rağmen, yapay zekanın siber güvenlikteki geleceği umut verici görünüyor. Makine öğrenimi teknolojilerinin

ve veri işleme yeteneklerinin sürekli gelişmesiyle, dinamik tehditlere uyum sağlayabilen daha akıllı sistemler göreceğiz. Yapay zekanın diğer teknolojilerle entegrasyonu Sonuç olarak, yapay zeka teknolojisinin sağlam siber güvenlik sistemleri oluşturmada ve sosyal güvenliği korumada kilit bir dayanak haline geldiği söylenebilir, ancak başarısı geleneksel güvenlik mekanizmalarıyla nasıl bütünleştiğine ve modern teknolojiler ile insan uzmanlığı arasındaki işbirliğini nasıl geliştirdiğine bağlıdır. Otomasyon ve insan müdahalesi, güvenlik etkinliği ve gizliliğe saygı arasındaki denge, bu teknolojilerin giderek karmaşıklaşan dijital dünyamızı ne kadar etkili bir şekilde koruduğunu belirleyecektir.

4.4.3. Sosyal medya platformlarının veri güvenliği ve kişisel gizlilik düzenlemeleri

Milyonlarca insanın kişisel verilerini depolayan, işleyen ve paylaşan sosyal medya platformları bulunmaktadır. Ancak, bu bilgilerin nasıl korunduğu ve kullanıldığı önemli bir konudur. Son yıllarda sosyal medya platformlarının kullanıcılarının kişisel verilerini koruma konusundaki zayıflıklarını ortaya çıkaran bir dizi veri sızıntısı ve skandal meydana gelmiştir. Dijital platformlarda yaşanan mahremiyet ihlalleri ve veri güvenliği sorunları, kullanıcıların güvenini önemli ölçüde zedelemektedir. Özellikle siber zorbalık, dijital taciz ve kişisel alanın ihlali gibi olumsuz tutumlar, bu endişeleri daha da artırmaktadır. Günümüzde bireylerin haber alma ihtiyaçları ile başkalarının özel hayatına saygı gösterme arasındaki dengeyi korumak giderek zorlaşmaktadır. İlginç bir şekilde, bazı kullanıcılar kendi istekleriyle mahremiyet sınırlarını esneterek izlenmeyi ve takip edilmeyi tercih edebilmektedir. sanal dünyanın sınır tanımayan yapısı ile bireylerin onay görme arzusunun birleşiminden kaynaklanmaktadır. Sosyal medya platformlarının tasarımı, büyük ölçüde bu etkileşimleri teşvik edecek şekilde yapılandırılmıştır. yapılan araştırmalar, kullanıcıların günde ortalama 5-6 saatlerini bu platformlarda geçirdiğini göstermektedir. Ancak bu zaman diliminin verimli kullanıldığını söylemek pek mümkün görünmemektedir, ticari ve diğer birçok nedenden dolayı herkes için giderek daha işlevsel ve çekici hale gelmesi açısından İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde gizlilik doğrudan ve açıkça uluslararası insan hakları hukuku kapsamında şu şekilde korunmaktadır:

- Hiç kimsenin özel yaşamı, konutu, ailesi ya da yazışması hususunda keyfi karışmalara, şeref ve onuruna yönelik saldırılara maruz bırakılamaz. Herkesin bu tür müdahale ve saldırılara karşı kanun tarafından korunmaya hakkı vardır.
- Bu kişiye, hiç kimsenin mahremiyetine, konutuna, ailesine veya haberleşmesine keyfi veya hukuka aykırı müdahale veya saldırıda bulunulamayacağını belirten Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 17. maddesi uyarınca resmi yasal koruma sağlanmıştır. (Mendel, 2012, p. 52)

Sosyal medya platformları kullanıcıların kişisel gizlilikleri ve veri güvenliğini sağlamak için çeşitli düzenlemelere tabidir. Bu düzenlemeler platformlar aracılığıyla paylaşılan bilgilerin güvende tutulmasını ve kullanıcıların kişisel verilerini korumayı amaçlayan düzenlemelerdir. Ayrıca, sosyal medya platformlarının sorumluluklarını belirlemesi ve kullanıcıların güvenliklerini sağlamak için uygun önlemleri almalarını gerektiren düzenlemeler de beklenmektedir ve bu konuyla ilgili çalışmalar devam etmektedir.

4.4.3.1. Yerel ve uluslararası veri koruma yasaları

Sosyal medya platformlarının, ulusal ve uluslararası veri koruma mevzuatına uygun olarak veri güvenliği ve kişisel gizlilik sistemlerini sağlaması gerekmektedir. Her ülkenin kendi veri koruma yasaları bulunmakta ve sosyal medya platformları bu yasal düzenlemelere ayrı ayrı uymak zorundadır. Türkiye'de Kişisel Verilerin Korunması Kanunu, örneğin sosyal medya platformlarının kullanıcı verilerini koruması için belirli yasal yükümlülükler getirmektedir. Ayrıca sosyal medya platformlarının uluslararası düzeyde de veri koruma yasalarına uyum sağlaması beklenmektedir.

4.4.3.2. Sosyal medya platformlarının veri güvenliği ve kişisel gizlilik düzenlemelerine uyması

Sosyal medya platformlarının uyumu, veri güvenliği ve kişisel gizlilik düzenlemelerine uygun olması gerekir. Bu platformların, veri güvenliğini ve kişisel gizliliği korumak için etkili politikalar geliştirmesi ve önlemler alması gerekmektedir. Bu politikalar kullanıcı verilerinin toplandığı, saklandığı ve kimlerle paylaşıldığı gibi konuları kapsamalıdır. Kullanıcılar, sosyal medya platformlarının veri güvenliği ve kişisel

gizlilik düzenlemelerine uygun hareket etmesi için araştırma yapmalı ve bu platformları kullanırken güvenliklerini sağlayacak önlemleri almalıdır. İnternet Şartı, Gelişmiş İletişim Derneği (APC) tarafından Şubat 2001'de Prag'da düzenlenen Avrupa APC İnternet Hakları Çalıştayı'nda düzenlendi ve yasal hale getirildi. Bu anlaşma, Halkın İletişim Şartını temel alıyor ve aşağıdakileri gelişimi amaçlıyor: Yedi fikirden başlıcaları şunlardır: Herkes için internet erişimi, bilgiye erişim, örgütlenme özgürlüğü, ifade özgürlüğü, ücretsiz açık kaynaklı yazılım ve teknoloji geliştirme, ortak eğitim ve yazarlık, gizlilik, şifreleme ve gözetleme İnternet yönetişimi, farkındalığın korunması ve hakların gerçekleştirilmesi gerektiğini kamuoyu ile paylaştı. (Abrahİm, 2021, p. 16)

4.4. Veri Gizliliği ve Güvenliği Düzenlemeleri

Kişisel verileri korumak ve dijital ortamda güvenliği sağlamak için, verilerin nasıl toplandığına, kullanıldığına ve korunduğuna rehberlik eden yasa ve standartlar Bu, mutlaka ele alınması gereken önemli bir konudur.

4.4.1. Genel Veri Koruma Yönetmeliği (GDPR)

Kişisel verileri işlenen kişilerin haklarını, veri işleme faaliyetinde bulunanların yükümlülüklerini, kurallara uyum sağlama yöntemlerini ve kurallara uymayanlar hakkında uygulanacak yaptırımları öngören tüzük, giderek daha fazla kişisel verinin işlendiği günümüzde, veri gizliliği ve güvenliği konusunda uluslararası aktörleri ve üçüncü şahısları da etkileyen bir düzenlemedir.

Genel Bakış

Avrupa Birliği'nde 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü (GDPR), küresel bir veri koruma düzenlemesidir. için en kapsamlı çerçevelerden birini temsil etmektedir. Birincil amacı, kuruluşların bu verileri şeffaf, güvenli ve adil bir şekilde işlemesini sağlarken bireylere kişisel verileri koruması üzerinde daha fazla kontrol sağlamaktır. GDPR, kuruluşun konumundan bağımsız olarak AB içinde faaliyet gösteren tüm kuruluşlar ve AB vatandaşlarının verilerini işleyenler için geçerlidir. Yönetmelik, veri işlemeden önce açık rıza ihtiyacı, veri ihlali bildirimleri ve kişisel bilgilere erişme ve silme hakkı için katı gereklilikler dahil olmak üzere birkaç temel ilke getirmektedir. GDPR'nin geniş kapsamlı uygulamaları, Tüm dünyada şirketleri veri işleme uygulamalarını yeniden değerlendirmeye zorladı ve özellikle müşteri verilerine dayanan sektörlerde iş operasyonlarını önemli ölçüde etkiledi. Bu

uygulamalara uyumsuzluk ciddi cezalara neden olabilecek şekilde düzenlendiSonuç olarak GDPR uyumu, modern iş dünyasında yalnızca cezai yaptırımlardan kaçınma aracı değil, aynı zamanda sürdürülebilir iş modellerinin inşasında kritik rol oynayan stratejik bir unsur haline gelmiştir.

Temel İlkeler

Genel Veri Koruma Yönetmeliği'nin (GDPR) özü, kişisel verilerin nasıl işleneceğine rehberlik etmek üzere tasarlanmış çeşitli temel ilkelere dayanmaktadır:

- Meşruiyet, Adalet ve Şeffaflık: veri sahibiyle ilgili olarak şeffaf, adil ve yasal bir şekilde işlenmelidir.
- Amaç Sınırlaması: Veriler yalnızca önceden belirlenmiş, geçerli ve hukuka uygun amaçlar doğrultusunda toplanmalı, bu amaçlar dışında kullanılmamalıdır.
- Veri Minimizasyonu: Veriler, amaç için gerekli olan süreden daha uzun tutulmamalı, süre sonunda uygun şekilde imha edilmelidir.
- Doğruluk: Veri sorumlusu, işlediği kişisel verilerin doğruluğunu sağlamak ve gerektiğinde güncellemekle yükümlüdür.
- Depolama Sınırlaması: Veriler, işlendikleri amaçlar için gereğinden daha uzun süre saklanmamalıdır.
- Bütünlük ve Gizlilik: Toplanan veriler, yetkisiz erişim, kayıp veya zarara karşı uygun teknik ve idari önlemlerle korunmalıdır.
- Hesap Verebilirlik: Kuruluşlar, veri işleme faaliyetleri için sorumluluk almalı ve GDPR ilkelerine uyum göstermeli, istenildiğinde bu konularla ilgili hesap verebilmelidir.

Bu ilkeler, kişisel verilerin bireysel hak ve özgürlüklere en üst derecede saygı gösterilerek ele alınmasını sağlar. Kuruluşlar, bu ilkeleri veri işleme faaliyetlerine tanımlamalı, veri koruma etki değerlendirmeleri gibi önlemleri uygulamalı ve gerektiğinde Veri Koruma Görevlileri (DPO'lar) atamalıdır.

Cezalar

GDPR, uyumsuzluk için katı cezalar uygulayarak ilkelerine bağlı kalmanın önemini vurgulamaktadır. GDPR kapsamındaki para cezaları, ihlalin ciddiyetini yansıtacak şekilde kademelendirilir.

Düşük Kademe Para Cezaları:

Yıllık küresel cironun %2'si veya 10 milyon avroya kadar para cezası verilebilir. Bunlar, veri ihlallerinin bildirilmemesi veya işleme faaliyetlerinin kayıtlarının tutulmaması gibi daha az ciddi ihlaller için geçerlidir.

Daha Yüksek Kademe Para Cezaları:

20 milyon Euro'ya veya yıllık küresel gelirin %4'üne kadar para cezası uygulanabilir. Bunlar, veri işleme için uygun rızanın alınmaması veya veri sahiplerinin haklarının ihlal edilmesi gibi daha ciddi ihlaller için geçerlidir. Para cezasının belirlenmesine ilişkin kriterler arasında ihlalin süresi, ağırlığı, niteliği ve ihlalin ihmalkâr karakteri, kasıtlı veya zararı hafifletmek için alınan önlemler ve denetim makamlarıyla işbirliği derecesi yer alır. Ek olarak, GDPR, işleme faaliyetlerini uyumlu hale getirmek için uyarılar, kınamalar veya emirler dahil olmak üzere diğer düzenleyici önlemlere izin verir. Bu cezalar sadece caydırıcı olması için değil, aynı zamanda veri korumanın en üst yönetim seviyelerinde bir öncelik haline gelmesini sağlamak için tasarlanmıştır. Uyumsuzlukla ilişkili önemli finansal riskler, GDPR'yi uyumu, dünya çapındaki kuruluşlar için kritik bir endişe kaynağıdır. (Ab.gov, 2018, p. 86)

4.4.2. Kaliforniya Tüketici Gizliliğini Koruma Yasası (CCPA)

Sağlanan belgeye dayanarak, 1121 sayılı Senato Yasa Tasarısı, Bölüm 735, CCPA, Kaliforniya eyaletinde yaşayan tüketicilerin kişisel verileri üzerindeki haklarını düzenleyen önemli bir yasal düzenlemedir

Genel bakış

1121 sayılı Senato Yasa Tasarısı, Kaliforniyalı tüketicilere kişisel bilgileriyle ilgili belirli haklar veren CCPA'da bir değişiklik görevi görüyor. Tasarı, CCPA'nın hükümlerini 1 Ocak 2020'deki yürürlülük tarihinden önce iyileştirmek için yasalaştı. Mevzuat, tüketicilerin kişisel bilgilerine erişme, satışından vazgeçme ve bunları silme

hakları da dahil olmak üzere tüketici gizliliğinin çeşitli yönlerini ele almaktadır. Ayrıca, işletmelerin tüketici verilerini işleme konusundaki uyumluluğu ve sorumluluklarını sağlamak için mevcut uygulama mekanizmalarını da ortaya koymaktadır. CCPA, tüketicilere, işletmelerden kendileri hakkında toplanan kişisel bilgilerin kategorilerini ve belirli parçalarını ve bu verilerin toplanma veya satılma amacını açıklamalarını talep etme olanağı sağlar. İşletmelerin, doğrulanabilir tüketici taleplerine yanıt vermeleri ve bu istenen bilgileri tüketicilere ücretsiz olarak sağlamaları gerekmektedir. SB 1121 tarafından getirilen en önemli değişikliklerden biri de, işletmelerin tüketicinin kişisel bilgileri silme hakkını ifşa etme zorunluluğunun değiştirilmesidir. İşletmeler artık bu hakkı sadece web sitelerinde yayınlamak yerine, bilgilerin tüketiciler tarafından daha pratik ve anlaşılır bir şekilde erişilebilir olmasını sağlamalıdır.

Temel İlkeler

SB 1121 ile değiştirilen CCPA'nın temel ilkeleri, tüketici gizliliğinin korunması ve işletmelerin kişisel bilgileri nasıl ele aldığının düzenlenmesi etrafında dönmektedir. Kanun tüketicilere birkaç temel hak vermektedir:

- Bilme Hakkı:

Tüketiciler, verilerin kaynakları, bilgi kategorileri, verilerin toplanması veya satılması için iş amacı ve bilgilerin paylaşıldığı üçüncü şahısların kategorileri dahil olmak üzere kendileri hakkında hangi kişisel bilgilerin toplandığını bilme hakkına sahiptir.

- Silme Hakkı:

Tüketiciler, bir işletme tarafından tutulan kişisel bilgilerinin silinmesini talep edebilir. İşletmeler, veriler bir işlemi tamamlamak, güvenlik olaylarını tespit etmek veya yasal yükümlülüklere uymak gibi belirli amaçlar için gerekli olmadıkça bu tür taleplere uymak zorundadır.

- Vazgeçme Hakkı:

Tüketiciler, kişisel bilgilerinin satışından vazgeçme hakkına sahiptir. Bu, bir işletmenin verilerini satması bilgilendirilme hakkını ve işletmenin bunu yapmasını engelleme seçeneğini içerir.

- Ayrımcılık Yapmama:

İşletmelerin, CCPA haklarını kullanan tüketicilere karşı ayrımcılık yapması yasaktır. Bu, işletmelerin bir tüketicinin gizlilik haklarını kullanıp kullanmadığına bağlı olarak hizmetleri reddedemeyecekleri, farklı fiyatlar talep edemeyecekleri veya farklı bir hizmet düzeyi sağlayamayacakları anlamına gelir. SB 1121 ile getirilen değişiklikler, bu hakların uygulanmasını açıklığa kavuşturmakta ve işletmelerin operasyonel ihtiyaçları ile dengelenmesini sağlamaktadır.

Cezalar

SB 1121 ile değiştirilen CCPA uyarınca, tüketici gizliliği haklarının uygulanması öncelikle başsavcının sorumluluğundadır. Bununla birlikte, bir tüketicinin düzeltilmemiş veya şifrelenmemiş kişisel bilgilerinin Yetkisiz giriş, hırsızlığa, sızmaya veya ifşaya tabi olduğu özel bir dava hakkı hükmü vardır. Bu gibi tüketiciler, kişisel bilgilerini korumak için belirli güvenlik önlemlerini uygulamayan işletmelere dava açabilir. SB 1121, özel dava hakkının bu belirli senaryolarla sınırlı olduğunu açıklığa kavuşturur ve tüketicilerin dava açmadan önce başsavcıya bildirimde bulunma zorunluluğunu ortadan kaldırır. CCPA'yı ihlal eden işletmeler önemli cezalarla karşılaşabilmektedir. Başsavcı, her ihlal için 2,500 ABD Dolarına veya her kasıtlı ihlal için 7,500 ABD Dolarına kadar maddi para cezası uygulayabilir. Ek olarak, yasa tasarısı, daha fazla ihlali önlemek için ihtiyati tedbir kararı uygulanmasına da izin vermektedir.

SB 1121 ayrıca, tüm fonları Tüketici Gizlilik Fonu'na yönlendirerek para cezalarının ve uzlaşmaların tahsisini de revize eder. Bu fon, CCPA'nın uygulanmasında mahkemeler ve başsavcı tarafından yapılan masrafları karşılamayı amaçlamaktadır.

Özetle, 1121 sayılı Senato Yasa Tasarısı, hükümlerini iyileştirerek, işletmelerin yasalara nasıl uyacakları konusunda net yönergelere sahip olmalarını sağlayarak ve tüketicilerin haklarını açıklığa kavuşturarak CCPA'yı güçlendiriyor. Değişiklikler, kişisel bilgileri korumaya, ihlalleri caydırmak için sağlam yaptırım mekanizmaları sağlamaya ve tüketici haklarını daha erişilebilir hale getirmeye odaklanıyor. (Leginfo.legislature., 2018)

4.4.4. Bilgi güvenliği yönetimi için ISO/IEC 27001 standartları

ISO 27001 Bilgi Güvenliği Risk Yönetimi Prosedürü'nün genel bakış bölümü, bilgi güvenliği risklerinin yönetilmesine yönelik sistematik ve proaktif bir yaklaşımın temelini oluşturur. Kuruluşun varlıklarını anlamanın, paydaşları sürece dahil etmenin ve riskleri sürekli olarak izlemenin önemini vurgular.

Genel Bakış

Bir kuruluşun bilgi güvenliği risklerini yönetmesi için bir temel oluşturmaktadır. Bu prosedür, bilgi güvenliği ile ilgili meydana gelebilecek tüm tehditlerin tanımlanmasını, değerlendirilmesini ve etkin bir şekilde yönetilmesini sağlamayı amaçlar. Belge, risk yönetimi sürecinde yer alan amaçları, kapsamı ve sorumlulukları açıklar. Özellikle, bilgi varlıklarının bütünlüğünü, gizliliğini ve erişilebilirliğini korumayı amaçlar. böylece bu varlıklar izinsiz giriş, değişiklik, ifşa veya yok edilmelere karşı korunur. öncelikle kuruluşun sahip olduğu varlıkların ve bu varlıkları etkileyebilecek potansiyel tehditlerin belirlenmesiyle başlar. Yazılım sistemleri, donanım altyapısı, veri kaynakları ve insan kaynağı gibi kritik unsurların detaylı şekilde analiz edilmesi, risk değerlendirme çalışmalarının sağlıklı yürütülmesi açısından büyük önem taşımaktadır. Süreç içerisinde, kuruluşun faaliyet ortamında meydana gelen değişimlerin düzenli olarak takip edilmesi ve risk profillerinin buna göre güncellenmesi gerekmektedir. Bu dinamik yapı, risk yönetiminin sürekli gelişen tehdit ortamına uyum sağlamasını mümkün kılmaktadır. bilgi güvenliği uzmanları, üst düzey yöneticiler ve ilgili birim temsilcilerinden oluşan geniş bir paydaş grubunun katılımını zorunlu kılmaktadır. Çok disiplinli bu iş birliği sayesinde, potansiyel risklerin kapsamlı şekilde tanımlanması ve uygun tedbirlerin geliştirilmesi mümkün olmaktadır. Özellikle üst yönetim desteği, risk yönetimi faaliyetleri için gerekli kaynakların tahsis edilmesi ve kurumsal önceliklerin belirlenmesi açısından belirleyici rol oynamaktadır. Bu modeler. politika dokümanları, standart işleyiş prosedürleri ve uygulama kılavuzları gibi araçlarla desteklenmektedir. Esnek yapıda kurgulanan çerçeveler, kuruluşların kendi operasyonel ihtiyaçlarına, sektörel gerekliliklerine ve risk iştah düzeylerine göre özelleştirilebilmektedir. Bu uyarlanabilirlik özelliği, risk yönetimi sistemlerinin sürdürülebilirliğini ve etkinliğini artırmaktadır.

Temel İlkeler

Risk yönetim sürecini yönlendiren ana kavramlar ve metotlar üzerinde durur. Bu bölüm, kuruluşun bilgi varlıklarını tutarlı ve yapılandırılmış bir şekilde korumasını sağlamak için etkili risk yönetiminin temel ilkelerini özetler.

- **Gizlilik, bütünlük ve erişilebilirlik (CIA) ilkelerinin önemi üzerine;**

Bu üç sütun, bilgi güvenliği stratejisinin temelini oluşturur. bilginin izinsiz girişden korunmasını, yetkili kullanıcıların ihtiyaç duyduğunda erişebilir olmasını ve doğru ve eksiksiz kalmasını sağlar. Belge, tüm risk yönetim faaliyetlerinin bu ilkelerle uyumlu olmasını ve bilgi varlıklarının kapsamlı bir şekilde korunmasını sağlaması gerektiğini vurgular.

- **Risk değerlendirmesi;**

Risklerin tanımlanması, değerlendirilmesi ve analiz edilmesini içerir ve risklerin kuruluş üzerindeki potansiyel etkisini belirlemeye yardımcı olur. Risk değerlendirmesi, risk yönetimi sürecinin kritik bir bileşenidir, çünkü kuruluşun riskleri ciddiyetlerine ve gerçekleşme olasılıklarına göre sıralamasına imkân tanır. Belge, risk değerlendirmeleri yapmak için çeşitli yöntemler sunar. bunlar arasında nitel ve nicel yaklaşımlar yer alır ve kuruluşun belirli ihtiyaçları ve bağlamına göre uygun yöntemin seçilmesinin önemini vurgular.

- **Risk tedavisi;**

Risklerin hafifletilmesi, transfer edilmesi, kabul edilmesi veya tamamen önlenmesini içerir. Belge, kuruluşların riskleri yönetmek için kullanabileceği farklı yöntemleri, örneğin güvenlik kontrollerinin uygulanması, kuruluşun risk iştahı içinde olan risklerin kabul edilmesi, sigorta yoluyla risklerin transfer edilmesi veya risklerin tamamen önlenmesi gibi yolları özetler. Risk değerlendirme sonuçlarına dayalı olarak uygun risk tedavi yöntemlerinin seçilmesinin önemi vurgulanır bu, kuruluşun tanımlanan riskleri etkin bir şekilde ele almasını sağlar.

- **Sürekli iyileştirme risk yönetimi çerçevesi;**

Politikaları ve prosedürlerinin etkin ve geçerli kalmasını sağlamak için Düzenli inceleme ve güncelleme içerir. r. Bölüm, geçmiş olaylardan örnek almanın ve risk yönetimi yaklaşımını öğrenilen derslere dayalı olarak uyarlamanın önemini vurgular.

Bu proaktif yaklaşım, kuruluşun ortaya çıkan tehditlere ve değişen risk manzarasına Etkili yanıt verilmesine olanak sağlar.

Cezalar

Belirlenen risk yönetimi politikalarına ve prosedürlerine uyulmamasının sonuçlarını ele alır. Bu bölüm, kuruluşun bilgi güvenliği uygulamalarına uyulmasının önemini pekiştirdiği ve uyulmamanın olası sonuçlarını vurguladığı için kritik öneme sahiptir. Belge, risk yönetimi gereksinimlerine uyulmaması bireylere veya ilgili departmanlara uygulanabilecek çeşitli ceza türlerini özetler. Bu cezalar, ihlalin ciddiyetine ve niteliğine bağlı olarak küçük düzeltici eylemlerden daha ciddi disiplin önlemlerine kadar değişebilir. Bölüm, cezaların yalnızca cezalandırıcı olmadığını, aynı zamanda kuruluşun bilgi güvenliği politikalarına uyulmasının önemini pekiştirmek ve bir uyum kültürü teşvik etmek amacıyla uygulandığını vurgular. Bölüm ayrıca, bilgi güvenliği standartlarına uyulmamasının olası yasal ve mali sonuçlarını da tartışır. Örneğin, hassas bilgilerin korunmaması kuruluş aleyhine yaptırımlar, para cezaları ve diğer hukuki işlem türleri uygulanabilir. Belge, uyulmamanın aynı zamanda müşteri güveninin kaybı, itibar zedelenmesi ve mali kayıplar gibi sonuçlara da yol açabileceğini, dolayısıyla risk yönetimi prosedürlerine uyulmasının önemini daha da vurgular. Yasal ve mali cezalara ek olarak, belge uyumsuzluğun potansiyel operasyonel etkilerini de özetler. Örneğin, uygun güvenlik kontrollerinin uygulanmaması, sistem kesintilerine, veri ihlallerine ve kuruluşun operasyonlarını önemli ölçüde etkileyebilecek diğer aksamalara yol açabilir. Bölüm, bu operasyonel sonuçların yasal veya mali cezaların ne kadar zararlı olabileceğini ve tüm kuruluş üyeleri tarafından ciddiye alınması gerektiğini vurgular.

Ayrıca, Cezalar bölümü, yönetimin risk yönetimi prosedürlerine uyumu denetleme ve ihlaller olduğunda uygun eylemleri gerçekleştirme konusundaki rolünü vurgular. Yönetimin öncülük etmesi ve kuruluş içinde sorumluluk kültürü ve bir hesap verebilirlik teşvik etmesinin önemi belirtilir. (Adlbelge, 2024)

4.5. Yapay Zekânın Etik ve Yasal Boyutları

Yapay zekâ teknolojilerindeki hızlı ilerlemeler, toplumsal uyum sürecinde önemli etik ve hukuki sorunları beraberinde getirmektedir. Bu sorunların uygun şekilde ele alınması, yapay zekâ uygulamalarının sosyal güvenlik alanında güvenilir ve etkili bir şekilde kullanılabilmesi için kritik öneme sahiptir. Yapay zekâ etiği, bu

teknolojilerin geliştirilme ve kullanım süreçlerini yöneten temel ahlaki prensipleri ifade etmektedir. İnsan zekâsını taklit edebilen sistemlerin, insani karar alma mekanizmaları kadar etik kurallara ihtiyaç duyduğu açıktır. Uygun etik düzenlemeler olmadan, bu teknolojilerin kötüye kullanım riski belirgin şekilde artmaktadır. Günümüzde finans sektöründen sağlık hizmetlerine, ulaşımdan müşteri ilişkileri yönetimine kadar pek çok alanda yapay zekâ uygulamaları yaygın olarak kullanılmaktadır. Bu teknolojinin sağladığı avantajların giderek artması, küresel ölçekte etkili düzenlemelerin gerekliliğini ortaya koymaktadır. Bu nedenle, yapay zekâ teknolojilerinin etik çerçevesinin oluşturulması ve uygun şekilde denetlenmesi büyük önem taşımaktadır. Yapay zekânın kullanıldığı sektöre ve bu sektöre bağlı olarak farklı yönetim seviyeleri gerekir. Yapay zekâ kullanan bir robot süpürge, evin yerleşim planını çıkarırken herhangi bir etik değere uyması gerekmez. Ancak söz konusu olan yayaları tanıması gereken otonom araçlar ya da kredi onay mekanizmaları olduğu zaman kullanılan algoritmalar etik kurallara uygun hareket etmelidir. Yapay zekâ, insan yaşamını köklü bir şekilde değiştirme potansiyeline sahiptir. Bu nedenle, Yapay zekânın uygulanması ve geliştirilmesi sırasında etik ilkelerin gözetilmesi hayati önem taşır. (İnnova., 2022)

- **Yapay Zekâ Kullanımının Etik ve Hukuki Çerçevesi**

Yapay zekâ, günümüzde hızla gelişen ve pek çok alanda etkisini gösteren bir teknoloji olarak hayatımıza girmektedir. Bu teknoloji, birçok sektörde verimliliği artırırken, aynı zamanda bazı etik sorunları da gündeme getirmektedir. Bu bölümde, yapay zekânın kullanımına ilişkin etik tartışmaları inceleyecek ve bu alandaki mevcut yasal düzenlemeleri ele alacağız.

- **Yapay Zekânın Karar Alma Süreçlerine Etkisi ve İnsan Hakları**

Yapay zekâ teknolojilerinin karar alma mekanizmalarına entegre edilmesi, beraberinde bazı etik ve hukuki tartışmaları da getirmiştir. Bu sistemler, büyük veri kümeleriyle eğitildikleri için, verilerin içerdiği önyargıları doğrudan öğrenebilir ve karar süreçlerine bu önyargıları yansıtabilirler. Sonuç olarak, belirli sosyal gruplara yönelik ayrımcı, eksik ya da adaletsiz uygulamalar ortaya çıkabilmektedir.

Örneğin. Bir kişinin kredi başvurusunun değerlendirilmesi ya da bir bireyin suç işleme olasılığına dair yapılan tahminlerde, yapay zekâ sistemleri cinsiyet, etnik köken ya da ekonomik statü gibi kişisel özelliklere dayalı olarak sistematik yanlılıklar üretebilir. Bu tür hatalı kararlar, yalnızca bireylerin temel haklarını ihlal etmekle

kalmaz, aynı zamanda teknolojinin güvenilirliğini ve toplumsal kabulünü de sorgulanır hale getirir. Bu bağlamda, algoritmaların şeffaf ve denetlenebilir olması, insan hakları açısından kritik öneme sahiptir.

- **Gizlilik ve Kişisel Verilerin Korunması**

Yapay zekâ teknolojilerinin işlevsel hâle gelmesi ve etkin bir şekilde eğitilebilmesi için çok büyük miktarda veriye ihtiyaç duyulmaktadır. Bu verilerin büyük bir bölümü kişisel bilgilerden oluştuğunda, bireylerin özel yaşamlarına dair mahremiyetin korunması temel bir etik zorunluluk hâline gelir. Bu nedenle, verilerin toplanması, işlenmesi ve kullanılması süreçlerinde kişisel gizliliğe gösterilecek özen, yalnızca teknik bir gereklilik değil, aynı zamanda toplumsal güvenin inşasında da kritik bir rol oynamaktadır.

- **Otonom Sistemler ve Sorumluluk Meselesi**

Yapay zekâ teknolojilerinin günlük yaşama daha fazla entegre olmasıyla birlikte, bu sistemlerin yol açabileceği etik ve hukuki sorumluluklar da giderek daha fazla tartışma konusu haline gelmektedir. Özellikle karar alma süreçlerinde insan müdahalesi olmaksızın çalışan otonom sistemlerde, meydana gelebilecek hatalı ya da zararlı sonuçların sorumluluğunu kimin üstleneceği belirsizliğini korumaktadır. Bu durum, yalnızca teknik bir mesele olmanın ötesine geçerek, hukuk ve etik disiplinlerinin doğrudan ilgilendiği çok boyutlu bir problem hâline gelmiştir.

- **Yapay Zekâ ve İşgücü Üzerindeki Etkileri**

Yapay zekâ teknolojilerinin çalışma hayatına olan yansımaları, günümüzün en önemli etik ve toplumsal tartışma konularından biridir. Bu teknolojiler, bazı iş süreçlerini otomatik hâle getirerek çalışanların üzerindeki iş yükünü azaltma ve verimliliği artırma potansiyeline sahiptir. Bununla birlikte, özellikle rutin ve tekrarlayan işlerde insan gücüne duyulan ihtiyacın azalması, işsizlik riskini gündeme getirmekte ve bu durum toplumsal dengeyi olumsuz yönde etkileyebilmektedir. Bu nedenle, yapay zekânın iş dünyasına entegrasyon sürecinde yalnızca teknolojik değil, aynı zamanda sosyal boyutları da göz önünde bulunduran kapsamlı ve uzun vadeli stratejilerin geliştirilmesi büyük önem taşımaktadır. İnsan merkezli bir dönüşüm anlayışıyla, bu teknolojilerin hem üretkenliği artıran hem de toplumsal adaleti gözeten bir çerçevede kullanılması hedeflenmelidir.

- **Yapay Zekâ İçeriklerinde Şeffaflık ve Etik Kullanım**

Yapay zekâ ile üretilen içeriklerin ne şekilde ve hangi koşullarda kullanıldığı, günümüzde giderek daha fazla önem kazanmaktadır. Bir içeriğin insan eliyle mi yoksa bir yapay zekâ aracıyla mı üretildiğini kullanıcıların bilmesi, dijital ortamda güven duygusunun korunması açısından büyük bir gerekliliktir. Bu durum, özellikle bilgiye ulaşımın hızlı ve kolay olduğu sosyal medya platformlarında daha da belirgin hâle gelmektedir. yapay zekâ tarafından oluşturulan içeriklerin telif hakkı durumu ve özgünlük boyutu da tartışılması gereken önemli konular arasındadır. İçeriklerin yeniden üretilmesi ya da mevcut veri kümelerinden türetilmesi, özgünlük kavramını yeniden değerlendirmeyi gerektirmektedir. Bu nedenle, içerik üretim süreçlerinde şeffaflığın sağlanması, hem kullanıcıların bilgilendirilmesi hem de etik ilkelere uygunluk açısından dikkatle ele alınmalıdır. (Microdestek., 2024)

4.5.1. Sosyal medya platformlarında güvenlik politikalarının uygulanması

Yapay zekâ teknolojilerinin gelişimiyle birlikte, sosyal medya platformlarında güvenlik politikalarının uygulanması Daha önemli bir konu haline geldi. Sosyal medya, iletişim kurmak, etkileşimde bulunmak ve bilgi paylaşmak için geniş bir kullanıcı tabanına sahip olduğundan, bu platformlarda güvenlik politikalarının etkin bir şekilde uygulanması, kullanıcıların güvenliğini sağlamak ve sosyal güvenliği artırmak açısından kritik öneme sahiptir.

Sosyal medya platformlarında kullanıcıları tehdit eden beş temel siber güvenlik riski bulunmaktadır:

1. Sosyal Mühendislik Saldırıları: İnsan psikolojisindeki zaaflardan faydalanan bu saldırı türü, kullanıcıları güvenlik önlemlerini aşmaya veya hassas bilgileri paylaşmaya yönlendirir. Saldırganlar önce hedef hakkında detaylı araştırma yaparak, topladıkları kişisel verileri inandırıcı bir senaryo oluşturmak için kullanırlar. Sosyal medyanın doğası gereği sağladığı kişisel bilgi zenginliği, bu tür saldırıların etkinliğini artırmaktadır.
2. Kimlik Avı (Phishing) Girişimleri: Sahte iletişim kanallarıyla yürütülen bu saldırılar, kullanıcıları zararlı bağlantılara tıklamaya veya güvenli olmayan formlara bilgi girmeye ikna etmeyi hedefler. Sosyal medya üzerinden kurulan kişisel bağlar, saldırganların güven kazanma sürecini kolaylaştırarak aldatmaca başarısını yükseltir.

3. Zararlı Yazılım Tehditleri: Platformlar üzerinden yayılan virüs, truva atı, fidye yazılımı gibi çeşitli kötü amaçlı programlar, kullanıcı cihazlarının kontrolünü ele geçirmeyi veya veri sızdırmayı amaçlar. Bu yazılımlar genellikle masum görünen paylaşımların içine gizlenerek yayılır.
4. Marka Taklidi Dolandırıcılıkları: Siber suçlular, tanınmış markaların kimliklerini taklit ederek kullanıcıları kandırmayı hedefler. Sahte hesaplar veya destek sayfaları üzerinden yürütülen bu taktikler, kurbanların finansal bilgilerini veya sistem erişim kimlik bilgilerini ele geçirmeye yöneliktir.
5. Kişisel Veri İhlalleri: Platformlardaki gizlilik ayarlarının yetersizliği veya kullanıcıların bilinçsiz paylaşımları, kişisel verilerin yetkisiz kişilerin eline geçme riskini artırmaktadır. Bu veriler kimlik hırsızlığından hedefli reklamcılığa kadar çeşitli amaçlarla kötüye kullanılabilir Catfishing, bir kişinin sahte bir kimlik oluşturmak için başka bir kişiden görüntü ve bilgi alması ve ardından bu sahte kimliği bir sosyal medya platformunda o kişiyi mağdur etmek için kullanmasıdır. Amaç, bu mağdurdan bir şey çalmak, onu küçük düşürmek veya genellikle her ikisini birden yapmaktır. (Globaltechmagazine, 2022)

4.6. Sosyal Medya Güvenliği İçin En İyi Uygulamalar

Sosyal medya hesaplarının güvenliğini sağlamak için çeşitli önlemler alınmalıdır. Olası siber tehditleri en aza indirmek için şu yöntemler uygulanabilir:

1. **Çok Faktörlü Kimlik Doğrulamayı (MFA) Etkinleştirme:** Çok faktörlü kimlik doğrulama, hesap güvenliğini artıran önemli bir adımdır. Kullanıcıların giriş yaparken ek doğrulama adımlarını tamamlamasını gerektirerek, çalınan veya ele geçirilen kimlik bilgilerine rağmen hesapların korunmasını sağlar. Bu yöntem, gelişmiş siber saldırılara karşı ek güvenlik katmanları sunar.
2. **Aynı Şifreyi Birden Fazla Hesapta Kullanımdan Kaçınma:** Her hesap için farklı ve güçlü bir şifre kullanmak, siber saldırganların bir hesabın şifresini ele geçirdiğinde diğer hesaplara kolayca erişmesini engeller. Güçlü ve karmaşık şifreler oluşturmak ve yönetmek için bir şifre yöneticisi kullanılması önerilir.
3. **Güvenlik Ayarlarını Düzenli Olarak Gözden Geçirme:** Sosyal medya platformlarının güvenlik ve gizlilik ayarları belirli aralıklarla kontrol edilmelidir. Mevcut güvenlik seçeneklerinin en yüksek düzeye ayarlandığından emin olunmalı ve yeni güvenlik güncellemeleri takip edilerek gerekli düzenlemeler yapılmalıdır.

4. **Bilinmeyen tehditleri azaltmak için bağlantılar azaltılmalıdır:** Sosyal medya platformlarında bağlantı kurulan kişi ve kurum türleri konusunda ayrımcı olunmalı. Her bağlantı dikkatle incelenmeli ve şüpheli görünen hesaplarla bağlantı kurulmamalıdır.
5. **Sosyal medyadan güvenlik riskleri takip edilmeli:** Belirli sosyal medya platformlarındaki tehdit haberleri takip edilmeli ve buna göre adımlar atılmalıdır. Güvenlik açıkları veya bilgisayar korsanlığı olayları öğrenilerek, bireysel hesaplar kontrol edilebilir ve Siber saldırganların izinsiz girişlerine yol açabilecek sorunlar düşünülebilir.
6. **Kimlik avı saldırısının nasıl yapıldığı öğrenilmeli:** Bu konuda aktif olunarak çevrede gerçekleşen yeni kimlik avı saldırıları öğrenilip, bu konuda şahsi eğitim sağlanabilir. Bilinmeyen bir şahıs yada şirket Sosyal medya veya e-posta yoluyla davetsiz bir şekilde sizinle iletişime geçen kişilere karşı her zaman şüpheci olun.
7. **Hesap sahtekârlıklarına ve marka kimliğine bürünme girişimlerine dikkat edilmeli:** İhlaller sosyal medya platformu yöneticilerine bildirilmeli ve takipçiler de Konuyla ilgili bilgilendirilmeli. (Hurriyet, 2022)

Sosyal medya platformlarında güvenlik politikalarının uygulanması, kullanıcıların güvenliğini sağlamak ve sosyal güvenliği artırmak için kritik öneme sahiptir. Veri gizliliği ve koruması, kullanıcı bilinçlendirme, içerik denetimi ve güvenlik protokolleri gibi yaklaşımlar, platformların güvenli bir ortam sunmasını sağlar. Yapay zekâ teknolojilerinin etkin kullanımı ve sürekli gelişen güvenlik stratejileri, sosyal medya platformlarının güvenlik politikalarını daha da etkili hale getirir. Bu, kullanıcıların platformlara olan güvenini artırır ve sosyal medyanın topluma sağladığı yararları en üst seviyeye taşır.

BEŞİNCİ BÖLÜM

YAPAY ZEKÂ ALANINDA HÜKÜMET STRATEJİLERİ VE POLİTİKALAR

5.1. Hükümetin Dokümanlarının Analizi

5.1.1. ABD'de Yapay zeka alanında araştırma ve geliştirmeye yönelik ulusal stratejik plan (2023)

ABD'nin 2023 yılında yayınladığı plan, yapay zekanın etik ve güvenli bir şekilde geliştirilmesini sağlamaktadır. Plan, yapay zekânın toplumsal yararlarını en üst seviyeye getirmek ve olası risklerini azaltmak için yedi öncelikli konu belirlemiştir:

1. Yapay zeka alanında temel ve uygulamalı araştırmaları desteklemek.
2. Etik ve sorumlu yapay zekâ kullanımına yönelik rehberlerin oluşturulması.
3. Teknolojik altyapının güçlendirilmesi.
4. Toplumun yapay zekâ teknolojileri konusunda bilinçlendirilmesi.
5. Ulusal güvenlik uygulamalarında yapay zekâ kullanımının geliştirilmesi.
6. Veri paylaşımı ve erişim mekanizmalarının iyileştirilmesi.
7. Uluslararası işbirliklerinin teşviki.

Bu strateji, hem bireylerin hem de toplulukların sosyal güvenliğini sağlamaya yönelik politikaları da içerir. Özellikle etik ilkeler ve veri gizliliği konusunda yoğun vurgu yapılmış, önlemlerin yasal çerçevede uygulanması için çağrıda bulunulmuştur.

Özet

Yapay zekâ, zamanımızın en güçlü teknolojilerinden biridir. Yapay zekânın sağladığı fırsatlardan yararlanmak için devletin öncelikle risklerini yönetmek için çalışması gerekir. Federal hükümet, sorumlu bilişimi teşvik eden ve diğer sektörlerin kendi başlarına baş edemeyeceği zorluklara çözümler geliştiren araştırma ve geliştirmeye yapılan akıllı yatırımlar da dahil olmak üzere bu çabada kritik bir rol oynamaktadır. Bu, büyük toplumsal zorlukları çözüme kavuşturmak ve yapay zekâ risklerini azaltmak için yeni yaklaşımlar geliştirmek için yapay zekâdan yararlanmak

adına araştırma ve geliştirmeyi içerir. Federal hükümet, kamu yararına hizmet eden, insanların haklarını ve güvenliğini koruyan ve demokratik değerleri ilerleten sorumlu araştırma ve geliştirmeye yatırım yaparak insanları ve toplulukları merkeze yerleştirmelidir. Bu güncelleme Yapay Zeka Alanında Araştırma ve Geliştirmeye Yönelik Ulusal Stratejik Plan'a yöneliktir, bu hedefe doğru yol almayı sağlamak için bir yol haritasıdır. Bu plan, federal araştırma ve geliştirme yatırımlarını organize etmek ve odaklamak için yapay zekâdaki başlıca araştırma zorluklarını tanımlamaktadır. Güvenilir Yapay Zekâ sistemlerinin kullanımı ve geliştirilmesinde ve ABD liderliğinin devam etmesini sağlayacak, mevcut ve gelecekteki ABD işgücünü Yapay Zekâ sistemlerinin tüm sektörlere kullanımı için hazırlayacak ve tüm federal kurumlarda devam eden Yapay Zekâ faaliyetlerini organize edecektir. Bu plan 2016 ve 2019 yıllarında yayınlanan planların devamı niteliğindedir. Yapay Zekâ araştırmalarında uluslararası işbirliğine yönelik ilkeli ve organize bir yaklaşımın önemini belirtmek için sekiz stratejiyi yeniden teyit ediyor ve dokuzuncu stratejiyi ekliyor:

Strateji 1:

Kamu yararına hizmet eden ve ABD'nin yapay zeka alanında küresel lider olmaya devam etmesini sağlayan sorumlu bilişimi teşvik etmek için yeni nesil yapay zekaya uzun vadeli yatırımlara öncelik verin.. Bu, algı, öğrenme, akıl yürütme ve temsil gibi temel yapay zekâ yeteneklerinin geliştirilmesinin yanı sıra yapay zekânın kullanımını Gerçekçi ve daha güvenilir şeyler oluşturmak ve üretken yapay zekâ ile ilişkili riskleri ölçmek ve yönetmek için odaklanmış çabaları içerir.

Strateji 2:

Yapay zekâ-insan işbirliği için etkili yöntemler geliştirin. İnsan yeteneklerini etkili bir şekilde tamamlayan ve artıran yapay zekâ sistemlerinin nasıl meydana getirileceğine dair anlayışı artırın. Açık araştırma alanları, başarılı yapay zekâ-insan ekiplerinin özelliklerini ve gereksinimlerini yapay zekâ ekip oluşturma uygulamalarının etkinliğini, verimliliğini ve performansını ölçme yöntemleri ve zararlı sonuçlara yol açan yapay zekâ özellikli uygulamaların insan tarafından kötüye kullanılması riskini azaltılmalı.

Strateji 3:

Yapay zekânın toplumsal, yasal ve etik etkileri anlaşılmalı ve ele alınmalı. Yapay zekâ sistemlerinin milletin değerlerini yansıtmasını ve eşitliği teşvik etmesini sağlamak için yapay zekânın oluşturduğu sosyal, yasal ve etik riskleri anlamak ve azaltmak için yaklaşımlar geliştirilmeli. Bu, teknik süreçler ve tasarım yoluyla değerleri korumak ve desteklemenin yanı sıra yapay zekâ gizliliği ve açıklanabilirliğini koruyan tasarım ve analiz gibi alanları ilerletmek için disiplinler arası araştırmalar içerir. Adalet, gizlilik, doğrulanabilir hesap verebilirlik ve önyargı için metrikler ve çerçeveler geliştirme çabaları da önemlidir.

Strateji 4:

Güvenli yapay zekâ sistemlerinin nasıl tasarlanacağı konusunda ileri düzeyde bilgi gerektirir. Bu, yapay zekâ sistemlerinin işlevselliğini ve doğruluğunu test etme, doğrulama ve doğrulama yeteneğini geliştirmeye ve yapay zekâ sistemlerini veri güvenlik ve siber güvenlik açıklarından korumaya yönelik araştırmaları içerir.

Strateji 5:

Yüksek kaliteli veri kümeleri ve ortamların yanı sıra eğitim ve test kaynakları geliştirilmeli ve bunlara erişim sağlanmalı. Yapay zekâ araştırması yürütmek için en iyi veri ve araçlarla çalışan daha geniş, daha çeşitli bir topluluk, daha adil ve yenilikçi sonuçlar elde etme potansiyelini artırır.

Strateji 6:

Yapay zekâ sistemlerini standartlar ve kıyaslamalar aracılığıyla ölçülmeli ve değerlendirilmeli. İdarenin Yapay Zekâ Haklar Bildirgesi Planı ve Yapay Zekâ Risk Yönetimi Çerçevesi (RMF) tarafından bilgilendirilen teknik standartlar ve Standartlar dahil yapay zeka için geniş bir değerlendirme teknikleri yelpazesi geliştirilmeli.

Strateji 7:

Amerika'da yapay zeka geliştiricilerini teşvik etmek için Ar-Ge işgücü geliştirme fırsatları iyileştirilmelidir.. Bu, yapay zekâ ve yapay zekâ ile ilgili çalışmaların sınırlarının ve imkânlarının anlaşılmasını geliştirmek için araştırma ve geliştirmeyi ve yapay zekâ sistemleriyle etkili bir şekilde etkileşim kurmak için gereken eğitim ve akıcılığı içerir.

Strateji 8:

Uluslararası ortaklar, endüstri, akademi ve diğer federal olmayan kuruluşlarla işbirliği içinde sorumlu Yapay Zekâ araştırma ve geliştirmesine sürekli yatırım yapma ve ilerlemeleri pratik yeteneklere dönüştürme fırsatları teşvik edilmeli.

Strateji 9:

Yapay zekâ araştırmalarında uluslararası işbirliğine yönelik ilkeli ve organize bir yaklaşım oluşturulmalı. Çevresel sürdürülebilirlik, üretim ve sağlık hizmetleri gibi Uluslararası zorlukların çözümek için yapay zekâ araştırma ve geliştirmesinde uluslararası işbirliklerine öncelik verilmeli. Stratejik uluslararası ortaklıklar, yapay zekâ araştırma ve geliştirmesinde sorumlu ilerlemeyi ve yapay zekâ için uluslararası kılavuzların ve standartların geliştirilmesini ve uygulanmasını desteklemeye yardımcı olacaktır. (State-gov, 2024, p. 6)

5.1.2. Avrupa Birliği ve Üye Devletler

2021 yılında yapay zekâya yönelik Yapay Zekâ Yasası taslağını hazırlamış ve bunun üzerine stratejik politikalar geliştirmeye devam edilmiştir. Avrupa Birliği'nin bu çalışmalarının temel amacı, yapay zekâ uygulamalarının güvenli şeffaf ve etik olmasını sağlamaktır. Öne çıkan hedefler şunlardır:

- **Yüksek risk içeren yapay zekâ uygulamalarının düzenlenmesi.**
- **Veri koruma ve mahremiyet haklarına riayet edilmesi.**
- **Avrupa'nın rekabet gücünü arttıracak teknolojik yeniliklerin desteklenmesi.**

Ayrıca Üye Devletler, kendi ulusal stratejilerini geliştirerek Avrupa Birliği ile koordine etmeye çalışmaktadır. Fransa'nın etik ve insan odaklı politikaları, Almanya'nın endüstriyel yapay zekâ uygulamaları bu stratejilere örnek olarak verilebilir.

Yeni yasa, AB'nin tek pazarında Hem kamu hem de özel kuruluşlarca güvenli ve güvenilir yapay zekâ sistemlerinin benimsenmesini ve geliştirilmesini teşvik etmeyi amaçlamaktadır. Aynı zamanda, AB vatandaşlarının temel haklarına saygı gösterilmesini sağlamayı ve Avrupa'da yapay zekâya yenilik ve yatırımı teşvik etmeyi

amaçlamaktadır. Yapay zekâ yasası yalnızca AB hukuku kapsamındaki alanlar için geçerlidir ve yalnızca askeri ve savunma için kullanılan sistemler ile araştırma amaçlı muafiyetler sağlar. toplumlarımız ve ekonomilerimiz için de fırsatlar meydana getiren küresel bir teknolojik zorluğu ele almaktadır. Yapay Zekâ Yasası ile Avrupa, yeni teknolojilerle uğraşırken hesap verebilirlik, şeffaflık ve güvenin önemine vurgu yaparken, aynı zamanda bu hızla değişen teknolojinin gelişebilmesini ve Avrupa bilişmini artırabilmesini sağlıyor.

5.2. Yapay Zekâ Sistemlerinin Yüksek Riskli ve Yasaklanmış Yapay Zekâ Uygulamaları Olarak Sınıflandırılması

Yeni yasa, farklı yapay zekâ türlerini içerdiği risklere göre sınıflandırıyor. Yalnızca sınırlı risk sunan yapay zekâ sistemleri çok hafif şeffaflık yükümlülüklerine tabi olurken, yüksek riskli yapay zekâ sistemlerine izin verilecek. Örneğin, bilişsel davranışsal manipülasyon ve sosyal puanlama gibi yapay zekâ sistemleri, gündeme gelebilecek riskleri kabul edilemez olduğu için AB'den yasaklanacak. Yasa ayrıca, insanları din, inanç, cinsiyet veya ırk gibi belirli kategorilere göre kategorize etmek için biyometrik verileri kullanan profil oluşturma ve sistemlere dayalı tahmine dayalı polislik için yapay zekânın kullanılmasını da yasaklıyor.

5.2.1. Genel amaçlı yapay zekâ modelleri

Yapay Zekâ Yasası ayrıca genel amaçlı yapay zekâ (GPAI) modellerinin kullanımını da kapsamı için alır. Sistemsel riskler oluşturmayan GPAI modelleri, örneğin şeffaflık ile ilgili olarak bazı sınırlı gerekliliklere tabi olacaktır, ancak sistemsel riskleri olanların daha katı kurallara uyması gerekecektir.

Yeni bir idare mimarisi

Uygun uygulamayı sağlamak için birkaç yönetim organı kurulmuştur:

- AB genelinde ortak kuralları uygulamak için Komisyon içinde bir Yapay Zekâ Ofisi
- Yaptırım faaliyetlerini desteklemek için bağımsız uzmanlardan meydana gelen bilimsel bir panel

- Yapay Zekâ Konseyi, kanunun etkinliğini ve tutarlılığını sağlar. Tüm Üye Devletlerin temsilcilerinden oluşur ve Komisyona ve Üye Devletlere bu tavsiyelerin uygun şekilde uygulanması konusunda tavsiyelerde bulunur ve yardımcı olur.

Ceza

Yapay Zekâ Yasası'na yönelik ihlaller için para cezaları, hangisi daha yüksekse, kusurlu şirketin bir önceki mali yıldaki küresel yıllık cirosunun bir yüzdesi veya önceden belirlenmiş bir miktar olarak belirlenir. KOBİ'ler ve start-up'lar orantılı idari para cezalarına tabidir.

Şeffaflık ve temel hakların korunması

Kamu sektöründeki yüksek riskli akıllı sistemler, vatandaşların temel haklarını korumaya odaklanan önemli düzenleyici gelişmelere tanık oluyor. Yeni düzenlemeler, tüm yüksek riskli akıllı sistemlerin birleşik bir Avrupa sicilinin oluşturulmasını öngörüyor ve hükümet kurumlarının bu kategoriye giren tüm teknoloji çözümlerini kaydetmesini zorunlu kılıyor. Kurallar ayrıca, duygusal tanıma sistemleri kullanan kuruluşların, bireyler bu teknolojilerle etkileşime girdiğinde onları açık ve net bir şekilde bilgilendirmelerini ve böylece bilgilendirilmiş onay ilkesini güçlendirmelerini gerektiriyor.

Bilişimi destekleyen önlemler

Yapay zekâ yasası, bilişim dostu bir yasal çerçeve sağlar ve kanıta dayalı düzenleyici öğrenmeyi teşvik etmeyi amaçlar. Yeni yasa, yenilikçi yapay zekâ sistemlerinin test edilmesi, doğrulanması ve geliştirilmesi için kontrollü bir ortam sağlayan yapay zekâ düzenleyici sanal alanların, yenilikçi yapay zekâ sistemlerinin gerçek dünya koşullarında test edilmesine de izin vermesi gerektiğini öngörüyor. (Consilium.europa, 2024) (Data.consilium.europa, 2024, p. 24)

5.3. Çin'in Yapay Zekâ Stratejik Öncelikleri

Çin, yapay zekâ alanında dünya lideri olma hedefiyle 2017 yılında Yeni Nesil Yapay Zekâ Geliştirme Planını açıklamıştır. Bu plan çerçevesinde Çin, yapay zekâ teknolojilerinin ticarileştirilmesi ve toplumsal yaşamın her alanına entegre edilmesine yönelik adımlar atmıştır. Başlıca öncelikleri:

- Endüstri liderliği için yenilikçi teknolojilerin geliştirilmesi.
- Kamu hizmetlerinde yapay zekâ uygulamalarının artırılması.
- Ulusal güvenlik ve savunmada yapay zekânın etkin kullanımı.
- Veri mahremiyeti ve sosyal risklerin kontrol edilmesine yönelik politika geliştirilmesi.

Yeni Nesil Yapay Zekâ Geliştirme Planı, Çin'in göreceli yetenekleri, potansiyel riskleri ve fırsatları da dahil olmak üzere yapay zekâ konusundaki stratejik konumuna ilişkin özel bir bakış açısı sunmaktadır. Plan, yapay zekânın Çin'e önemli stratejik kazanımlar sağlayabileceği üç alanı vurgulamaktadır. Askeri teknoloji geliştirme, ekonomik kalkınma ve sosyal yönetişim bu alanların en önemlilerindendir.

Askeri Teknolojinin Geliştirilmesi

Yapay zekanın da aralarında bulunduğu çeşitli ileri teknolojiler alanlarından istifade ederek ABD liderliğindeki Batı ordularına karşı üstünlük sağlama hedefini içeren yeni nesil silahlarına göre yürütülüyor. Bunu, Başkan Xi Jinping'in talimatları ve askeri rekabetin sadece yenilikçi kazanır kavramı takip ediyor. Çin, dünyanın büyük askeri güçleri arasında askeri yapay zekâ teknolojisi geliştirmeye tartışmasız en hızlı odaklanan ülkedir. 22 Nisan 2015 Tarihi'nde ise Çin'de kurulan ve uzay, siber, ve psikolojik savaş yeteneklerinden sorumlu olan Stratejik Destek Gücü'nü lağvedeceği açıklanmıştı. Bunun yerine ise modern bir Bilgi Destek Gücü oluşturuldu. Bununla birlikte, aynı zamanda Çin, AI silahlarının risklerini azaltmak için uluslararası işbirliğini güçlendirmenin en aktif savunucularından biridir. Çin'in endişeleri üç ana risk etrafında toplanıyor: yapay zekâ silahlarının insan kontrolünden çıkması, ülkeler tarafından yapay zekâ silahlarının kullanımına ilişkin politikaları ve kuralları tanımlayan standartların olmaması ve yapay zekâ silah kazalarından kaynaklanan yanlış hesaplamalar nedeniyle askeri çatışma veya savaş riski . Çin'in bu endişeleri, ölümcül AI silahlarının yasaklanması için kamuoyunu bilgilendirirken ortaya çıktı. Ancak araştırmacılara göre Çin'in yasaklama çağrısının, Çin'in caydırıcılık politikasının bir parçası olarak üretimi ve geliştirmeyi yasaklamakla değil, kullanımı yasaklamakla sınırlı olduğuna inanıyor. Bu, Çin'in nükleer silahların ilk kullanımı yok politikasına benzer. Nükleer silah politikasında olduğu gibi, yasağa odaklanmak,

çalışmalarını yöneten etik kontrollerin olmaması nedeniyle yapay zekâ silahlarının çok popüler olmadığı demokratik ülkelerin orduları üzerinde baskı kurmayı amaçlıyor gibi görünmektedir. Kaldı ki Çin'in otonom silah tanımı dar ve sadece tam otonomiye sahip silahları içerirken, Batılı ülkeler daha geniş tanımlar benimsemektedir. Bu nedenle, Pekin'in yapay zekâ vizyonu, askeri alanlarda Batı ile askeri rekabeti kazanmasını sağlayabilecek stratejik bir fırsat olarak açıktır.

Ekonomik Kalkınma

2017 Gündemi, ekonomik kalkınmayı ikinci en büyük stratejik odak noktası olarak tanımladı. Esas olarak imalat, finans, lojistik ve tarım sektörlerinin güçlendirilmesine odaklandı. Yapay zekânın önemli rolü, halihazırda önemli bir ilerleme sağladığı bu alanlarda anlaşılabilir. Araştırmalar, erken dönemlerden itibaren Çin'in ekonomik kalkınmasının yapay zekânın büyümesinden kaynaklanan potansiyel yararlarını gösterdi. Örneğin Çin, bunu yaparak 2030 yılına kadar %26'lık bir ekonomik büyüme yakalayacağını ve aynı yıl içinde işgücü sayısında %12'den fazla bir çıkış yapacağını bildirdi. Bu beklentiler, Çin'de, özellikle lojistik ve imalat sektöründe otomasyonu teşvik etti ve genişletti. Ancak bu eğilimi benimsemenin bazı zorluklar da var, bunlardan bazıları ulusal işgücü üzerindeki uzun vadeli etkiler ve bir yanda yüksek işler ile diğer yanda orta ve düşük işler arasında bir dengesizlik meydana getirmesidir.

Bu, Pekin'in şu anda 2010'dan başlayarak ulusal düzeyde benimsediği hızlı ve büyük eğitim reformu hareketini açıklayabilir ve bu hareket, yalnızca yapay zekâdaki (derin bir küresel sorun) uzmanlaşmış yetkinliklerdeki açığı doldurmayı değil , böylece mezunlar yapay zekânın hızlı entegrasyonu nedeniyle işgücü piyasasındaki derin ve hızlı değişikliklere ayak uydurabilirler. Yapay zekânın benimsenmesine doğru kayma, ekonomik yeniden yapılanma sürecinin ana dallarından biri olarak kabul edilebilir. Major şu anda devam etmekte olup, eski büyüme motorlarını yüksek teknoloji ile ilişkili olanlarla değiştirmeyi amaçlamaktadır.

Sosyal Gelişim

Çin, başta kapsamlı bir sosyal refah sistemi, tüm vatandaşları içeren bir sağlık sistemi ve bundan kaynaklanan kirliliği ve çevresel ve iklim olaylarını azaltan bir ekosistem inşa edememe olmak üzere, kontrol altına alınmasında zorlanan çeşitli sosyal krizlerden dolayı muzdariptir. Çin'de yapay zekâ teknolojisi, bu sektörlerde

performansı artırmak için kullanılabilecek yöntemlerden biri olarak görülüyor. Örneğin, yapay zekâ, bir emeklilik ve sosyal yardım sisteminin sağlanmasına katkıda bulunan bir veri tabanı oluşturmaya yardımcı olabilir. Marjinal gruplar ve uzak bölgelerde yaşayan vatandaşları için hastalık teşhis sistemleri ve tedavi yöntemleri geliştirmenin yanı sıra bir yerdeki yüksek kirlilik seviyelerini uyarmak veya çevresel felaketleri tahmin etmek için bir erken uyarı sistemi de geliştirebilir. Ayrıca yapay zekâ, hükümetin toplumu kontrol etme yeteneğini güçlendirmesine imkân tanır. Örneğin, 2021'de Öneri Algoritmalarını Yönetmeye İlişkin Hükümler, sosyal düzeni bozma veya iyi alışkanlıklara ve kamu düzenine aykırı uygulamaları teşvik etme yeteneklerini baltalamaya odaklanmaktadır. 2023'te yayınlanan Üretken Yapay Zekâ Hizmetlerinin Yönetimi için Geçici Önlemler, ister resim ister metin olsun, yapay zekâ tarafından oluşturulan içeriğin şu düşüncelere uyumlu olmasını zorunlu kıldı: Sosyalizmin temel değerleri devlet iktidarını sarsmamalı, ulusal birliğe zarar vermemeli veya yanlış bilgi yaymamalıdır. Pekin, modernleşme ile siyasi ve sosyal istikrar arasında bir denge kurmaya dayalı bir yaklaşım benimsiyor. Bu, Beş Yıllık Plan'da (2021-2025), Çin'in teknolojik kalkınma politikalarının tanımlayıcı bir felsefesi haline gelen istikrar çerçevesinde ilerlemeyi sürdürme ihtiyacına atıfta bulunulmaktadır. Başka bir deyişle Çin, sosyal kontrolde avantajlar aramak ve küresel jeopolitik nüfuzu genişletmek amacıyla hızlı bilişimin neden olduğu kabul edilebilir bir kaos seviyesine izin vermeye çalışıyor. Bununla birlikte, Çin'in 2030 yılına kadar dünyanın en büyük yapay zekâ gücü olma planı göz önüne alındığında, ChatGPT'ye benzer Çin yapay zekâ programlarının Amerika Birleşik Devletleri'ndeki benzerleriyle rekabet edememesine neden olan büyük zorluklar var. Bu zorluklardan ilki, Çinli şirketlerin Batı modeli gibi kaynakları araştırma ve geliştirmeye yönlendirmek (daha uzun süren) yerine hızlı uygulamalara yatırım yapmak istemeleridir. Ayrıca, Çin'de dil modeli eğitimi dilin karmaşık ve aynı zamanda zengin doğası nedeniyle İngilizce'ye kıyasla daha zordur. Ancak Çin yapay zekâ sektörünün Amerikalı benzerlerini atlamasını engelleyen en önemli zorluk, siyasi hassasiyetler ve Çin'in ağır bir şekilde sansürlenen ve kontrol edilen internet ortamıdır ve bu, yapay zekâ programları geliştirirken sosyalizme ve topluluk değerlerine bağlılık konusundaki resmi belgelerin odağına yansımaktadır. (Epc.ae, 2024, pp. 4-9)

5.4. Türkiye'nin 2021-2025 Ulusal Yapay Zekâ Stratejisi

Türkiye'nin Ulusal Yapay Zeka Stratejisi (2021-2025), ülkenin yapay zeka yeteneklerini geliştirmeyi ve böylece ekonomik, sosyal ve teknolojik kalkınmaya katkıda bulunmayı amaçlamaktadır. Strateji, altyapı geliştirme, araştırma ve geliştirmeyi teşvik etme, insan kadrolarını eğitme ve girişimcilik ve yenilikçiliği teşvik etme konularına odaklanarak Türkiye'nin bu alandaki vizyonunu özetlemektedir. Ayrıca, kamu, özel sektör ve akademi arasındaki işbirliğini güçlendirerek Türkiye'yi uluslararası düzeyde rekabetçi bir konumda konumlandırmayı amaçlamaktadır.

Türkiye'de Yapay Zeka Ulusal Stratejisinin temel hedefleri 2021-2025:

1. Verimliliği ve üretkenliği artırmak, yapay zeka teknolojilerinin farklı ekonomik sektörlerde yaygınlaşmasını sağlamak.
2. Ar-Ge çalışmalarını desteklemek, üniversiteler ve araştırma kurumlarının yapay zeka alanındaki çalışmalarını teşvik etmek.
3. Güçlü bir dijital altyapı oluşturmak, büyük veri ve bulut bilişim gibi teknolojilere yatırım yapmak.
4. Girişimciliği teşvik etmek, yapay zeka alanında faaliyet gösteren start-up şirketlerini desteklemek.
5. Dijital becerileri geliştirmek, genç yeteneklerin yapay zeka odaklı iş gücüne hazırlanmasını sağlamak.
6. Etik ve güvenli yapay zeka kullanımını sağlamak, yasal ve düzenleyici çerçeveler oluşturmak.

Stratejiler

Strateji 1: Yapay zekâ alanında insan kapasitesini artırmak için eğitim müfredatına yapay zekâ derslerini dahil etmek.

Strateji 2: Ar-Ge ve inovasyonu desteklemek amacıyla yapay zeka projelerine yatırımları artırmak ve üniversite-sanayi iş birliğini teşvik etmek.

Strateji 3: Yapay zeka inovasyonunu ve gelişimini desteklemek için güçlü bir veri ekosistemi ve teknolojik altyapı oluşturmak.

Strateji 4: Yapay zekanın etik ve sorumlu kullanımını sağlamak için düzenleyici ve etik mekanizmalar geliştirmek.

Strateji 5: Yapay zekâ alanında faaliyet gösteren girişimlerin sayısını artırmak için finansal teşvikler ve destekler sağlamak.

Strateji 6: Yapay zekâ konusunda toplumsal farkındalığı artırmak ve toplumun yapay zekâ gelişimine katılımını sağlamak. (Cbddo.gov, 2021, s. 6)

5.6. Yapay zekâ alanında Katar Ulusal Stratejisi

2019 yılında yayınlanan strateji ile Katar, yapay zeka teknolojilerinin ülke için çok çeşitli kamu hizmetlerinde kullanılmasını hedeflemektedir. Stratejinin kilit noktaları şunlardır

- Veri analitiği ve makine öğrenimi kullanımıyla karar verme mekanizmalarını iyileştirmek.
- Yapay zekâya dayalı yenilikçi çözümlerle ulusal ekonomiyi güçlendirmek.
- Veri güvenliği ve mahremiyeti konusunda uluslararası standartlarla uyumlu politikalar oluşturmak.

Katar Ulusal Yapay Zekâ Stratejisi altı temel sütuna dayanmaktadır: eğitim, istihdam, veri erişimi, araştırma, iş ve etik. Katar'ın iki rol oynayacağı öngörülüyor: Birincisi, Katar'ın yerelleştirilmiş alanlarda müşteri tarzı yapay zekâ uygulamaları üretebilmesi ve yapay zekânın bilişiminin itici gücü olarak kullanılmasına izin veren bir iş ortamına sahip olması gerekiyor. Katar, etik kurallara, sağlam bir eğitime ve sağlam yasalara sahip ikinci bir vatandaşla etkili bir yapay zekâ tüketicisi haline gelmelidir.

Yapay zekâ alanındaki Katar stratejisinin temel direkleri

Sütun 1: Yapay zekâ çağında yetenek için rekabet etmek

Sütun 2: Verilere erişim kritik öneme sahiptir

Sütun 3: Değişen İstihdam Ortamı

Sütun: 4 Yeni İş ve Ekonomik Fırsat

Sütun 5: Katar – Yapay zekânın benimsenmesi için odak alanları (uluslararası işbirliği)

Sütun 6: Etik ve kamu politikaları. (Qcai-blog.qcri., 2020, pp. 4-10)

5.7. Suudi Arabistan'da Yapay Zekâ Stratejileri

Suudi Arabistan Krallığı, Ulusal Veri ve Yapay Zekâ Stratejisi (NSDI) aracılığıyla, sürdürülebilir kalkınmayı teşvik etmek ve 2030 Vizyonuna ulaşmak için modern teknolojinin kullanım şeklini kökten dönüştürmeyi hedefliyor. Bu strateji, yapay zekayı sosyal güvenlik gelişiminin temel bir kolaylaştırıcısı ve uluslararası ve yerel ticaretin itici gücü olarak görüyor ve Krallığı bu alanda lider bir ülke konumuna getirmektedir. Strateji, yapay zekâ ve büyük veri uygulamalarıyla başa çıkma verimliliğini artıran güçlü ve gelişmiş bir dijital altyapı oluşturmayı amaçlıyor.

Krallığın çeşitli strateji uygulamalarını desteklemek için yenilikçi teknoloji platformlarının ve modern veri merkezlerinin kurulduğu veri işleme alanındaki yeteneklerinin geliştirilmesini içeriyor. Odak noktası ayrıca, bu alandaki projelere ve girişimlere liderlik edebilecek yeni nesil yetkinlikler hazırlamak amacıyla Yapay Zekâ Akademisi tarafından sunulanlar gibi özel eğitim ve öğretim programları sağlayarak insan yetkinliklerinin geliştirilmesidir.

Etik ve yasal çerçeveler açısından bakıldığında Krallık, gizliliği korumak ve yapay zekânın etik ve sorumlu kullanımını sağlamak için uluslararası standartları uygulamaya kararlıdır. Bu çabalar, Krallığın etik değerlere saygı duyarken sürdürülebilir kalkınmaya ulaşma taahhüdünü yansıtarak, Bilişim, teknoloji ve insan haklarının korunması arasındaki dengeyi sağlamayı amaçlamaktadır.

Suudi Veri ve Yapay Zekâ Kurumu (SDAIA), ulaşım, sağlık ve eğitim gibi çeşitli sektörlerde yapay zekâ kullanımını teşvik etmeyi amaçlayan politikalar geliştirmek ve girişim faaliyetlerini düzenlemek için çalıştıkları. Bu açıdan bakıldığında en öne çıkan projelerden biri, kaynakları verimli bir şekilde yönetmek ve sakinlerin yaşam kalitesini iyileştirmek için yapay zekâ teknolojilerine dayanan akıllı bir şehir modeli olan NEOM projesidir.

Bu alandaki önemli ilerlemeye rağmen, Krallık yerel uzmanlık eksikliği, bilgi ve ileri teknoloji transferi için uluslararası işbirliğini güçlendirme ihtiyacı ile ilgili zorluklarla karşı karşıyadır. Ancak Krallık, 2030 yılına kadar yapay zekâ için küresel bir merkez

haline gelmek için dijital altyapısını güçlendirmek ve insan yeteneklerini geliştirmek için çalışmaya devam ediyor.

5.8. Yapay Zekâ Stratejisinin Temel Boyutları

Başarılı bir yapay zekâ stratejisi beş esas boyut üzerinden tanımlanır:

- **Veri**

Verilerin toplanması, işlenmesi, depolanması, korunması, gizliliğinin sağlanması, kalite doğrulaması ve yönetimi ile ulusal ve uluslararası düzenlemelere ve politikalara uygunluğuna yönelik kontrollere ek olarak, Veri, yapay zeka çözümlerinin sağlanmasının temelini oluşturur.

- **İnsan Kaynakları**

Yapay zekâ kullanımının değişimi organizasyon düzeyinde yönetmenin ve çalışan Etkisini analiz etmenin yanı sıra, yetkinlikleri ve insan kaynaklarını yapay zekâ stratejisinin gerekliliklerine uygun bir şekilde planlamak ve çeşitli seviyelerdeki ilgili tüm çalışanların Değişimi başarıyla uygulamak için farkındalık ve eğitim aldığını dikkate almak.

- **Yönetmelikler ve Politikalar**

Yapay zekânın yönetiminde kuruluşun iç ve dış organizasyon politikaları, değer ve kuralları, sistemlerine erişimin yönetilmesi, sonuçlarının izlenmesi ve belgelenmesinin yanı sıra, yapay zekâ modelleri geliştirirken ve kullanırken etik yönergeler ve bunlara ulaşma hedefi belirleme.

- **Yordam**

Yapay zekâ modellerinin geliştirilmesi ve üretim hatlarına başarılı bir şekilde aktarılması için gerekli prosedürlerin Aynı zamanda planlama ve organizasyon hassasiyetlerin belirlenmesi, bütçelerin yönetilmesi, tesis için uygulama, değerlendirme, işletme ve destek verilmesi ve bu süreçlerin tesisin temel prosedürleri ile uyumluluğunun doğrulanması süreçleridir.

- **Teknoloji**

Bulut bilişim gibi yapay zekâ sistemlerini, veri yönetimi ve işleme için uygun platformları oluşturmak, işletmek, korumak ve dağıtmak için gereken altyapı ve teknik araçlar,<CITATION Yap24 \p 12 \l 1055 (Sdaia.gov, 2024, s. 12)>

5.9. Yapay Zekânın Sosyal Güvenliği Hükümet Belgelerinin Analizinin Bulgularının Özeti ve Tartışılması

Yapay zeka, sosyal güvenlik mekanizmalarından ekonomik süreçlere kadar insan hayatının her alanını yeniden şekillendiren teknolojik bir devrimi temsil ediyor. Bu bölümde, ulusal yapay zeka stratejileri geliştirmeye çalışan çeşitli ülkelerin stratejileri analiz edilmekte ve vurgulanmakta, yapay zekanın potansiyeli vurgulanmakta, farklılıklar ve ortak zorluklar ortaya konulmaktadır.

5.10. Yapay Zekâ Stratejilerinin Analizi

5.10.1. Amerika Birleşik Devletleri

Strateji: Yapay Zekâda Araştırma ve Geliştirme için Ulusal Stratejik Plan (2023).

Amerika Birleşik Devletleri, araştırma ve geliştirmeyi destekleyerek ve yeniliği teşvik ederek yapay zekâda küresel liderliğini güçlendirmeye odaklanmıştır. Ana hedefler şunlardır:

- **Teknik yenilik:** Kamu ve özel hizmetleri iyileştirmek için makine öğrenimi ve robotik teknikler gibi gelişmekte olan teknolojilere yatırım yapmak.
- **Ortaklıklar:** Kalkınmayı hızlandırmak için kamu ve özel sektör arasındaki işbirliğinin teşvik edilmesi.
- **Siber güvenlik:** Koruma sistemlerini iyileştirmek ve dijital tehditlerle mücadele gücünü artırmak için yapay zekâ kullanmak.

Zorluklar: Bilişime odaklanılmasına rağmen, veri koruma için geniş kapsamlı bir yasal çerçeve eksikliği tespit edilmiştir ve bu da kişisel bilgi sızıntısı riskini artırmaktadır.

5.10.2. Avrupa Birliği

Strateji: Avrupa Birliği Üye Devletlerinin ulusal stratejileri.

Avrupa Birliği, yapay zekânın kullanımını düzenlemede küresel bir model olarak kabul edilir ve aşağıdakilere odaklanmasıyla kendisini belli eder:

- **Etik:** Yapay zekânın insan haklarına ve etik standartlara saygılı bir şekilde kullanıldığından emin olunmalı.

- **Gizlilik:** Bireylerin gizliliğini sağlamak için Genel Veri Koruma Düzenlemelerini (GDPR) uygulanmalı.
- **Şeffaflık:** Yorumlanabilir algoritmalar geliştirilerek önyargılar azaltılmalı.

Zorluklar: Üye Devletlerin ulusal politikalarının çok çeşitli olması, birlik düzeyinde birleşik bir stratejinin uygulanmasını zorlaştırmaktadır.

5.10.3. Çin

Strateji: Yapay Zekâ için Ulusal Stratejik Öncelikler.

Yapay zekanın ekonomiyi ve ulusal güvenliği artıracak bir araç olarak kullanılmasına odaklanarak başarmayı hedefliyor. Amaçlar şunlardır:

- **Global Liderlik:** 2030 yılına kadar yapay zeka teknolojileri alanında dünyanın lider ülkesi olmak.
- **Güvenlik gözetimi:** Gözetim sistemlerini geliştirmek ve kamu güvenliğini sağlamak için yapay zekâ tekniklerinin kullanılması.
- **Endüstriyel Kalkınma:** Üretken sektörlerin verimliliğini artırmak için yapay zekânın kullanılması.

Zorluklar:

Ulusal güvenliğe odaklanma, gizlilik ihlalleriyle ilgili uluslararası eleştiriler almaktadır.

5.10.4. Türkye

Strateji (2021-2025) dayanıklı ve sürdürülebilir bir ekosistem inşa ederek Türkiye'yi yapay zekâ alanında küresel bir oyuncu haline getirmeyi amaçlamaktadır.

Etik:

- İnsan haklarına, demokrasiye ve hukukun üstünlüğüne saygı

Mahremiyet:

- Genel veri alanı yaratarak güvenli veri yönetimini teşvik edin.
- Standardizasyonun sağlanması amacıyla Ulusal Veri Sözlüğü oluşturulması.

- Veri yönetimi ve gizliliği için ulusal bir çalışma grubu oluşturulması.

Şeffaflık:

- Yapay zeka sistemlerinin açıklanabilir olması gerekliliğinin vurgulanması.
- Yapay zekanın işgücü piyasası ve ekonomi üzerindeki etkilerine ilişkin periyodik raporlar yayınlamak.

Zorluklar:

- Yapay zeka alanında kalifiye eleman eksikliği.
- Teknolojik gelişmelere ayak uydurabilmek için yasal çerçevenin güncellenmesi ihtiyacı.
- Yapay zeka teknolojilerine olan kamu güveninin artırılması.
- Çin ve ABD gibi ülkelerle küresel rekabet.

5.10.5. Katar

Strateji: Katar Ulusal Yapay Zekâ Stratejisi (2019).

Katar, ekonomisini desteklemek için yapay zekâ yeteneklerini geliştirmeyi hedefliyor ve Katar Ulusal Vizyonu 2030 aracılığıyla, özellikle Dünya Kupası'na hazırlanırken toplumun, ekonominin ve sporun gelişiminin önemli bir parçası olarak bilişim ve teknolojiyi içeren iddialı bir vizyon benimsedi. Hedefleri şunları içerir:

- **Grafiksel analiz:** Büyük verilerle karar verme sürecinin iyileştirilmesi.
- **Eğitim ve Araştırma:** Bilgiyi geliştirmek için eğitim ve araştırma geliştirmeye yatırım yapmak.
- **Etik:** Uluslararası gizlilik standartlarına uygun politikalar benimsemek.

Zorluklar:

Eğitimli bireylerin sayısını artırarak yerel yetenekler oluşturmak ve yeniliği teşvik etmek, bu stratejinin uygulanmasında karşılaşılan en büyük zorluklardan ikisidir.

5.10.6. Suudi Arabistan Krallığı

Strateji: Ulusal Veri ve Yapay Zeka Stratejisi (NSDI).

Suudi Arabistan yerel insan kaynaklarının ve sağlam altyapının geliştirilmesine güvenerek yapay zekâ alanında liderliğe ulaşmaya odaklanmıştır. Ulusal stratejinin hedefleri şunları içerir:

- **Bölgesel ve küresel liderlik:** Suudi Arabistan, 2030 yılına kadar yapay zekâ alanında küresel bir merkez haline gelecek,
- **Altyapı ve teknolojiler:** Büyük veri analizi ve yapay zekâ uygulamalarının geliştirilmesi için gelişmiş platformlar oluşturulacak,
- **Eğitim ve mesleki gelişim:** Suudi Yapay Zekâ Akademisi gibi eğitim programları ve girişimler aracılığıyla gelecek nesilleri teknolojiyi benimsemeye hazırlamak,
- **Etik çerçeveler:** Uluslararası yasalara uygun olarak gizlilik ve veri koruma standartlarına uygunluk sağlanacak.

Zorluklar:

Yüksek hırslara rağmen, Krallık yerel uzmanlığı artırma ve uluslararası ortaklardan bilgi aktarma ihtiyacı gibi zorluklarla karşı karşıyadır.

5.11. Ülkelerin Kapsamlı Karşılaştırması

Yapay zeka alanındaki küresel rekabet, ülkeleri stratejik hedefleriyle uyumlu politikalar geliştirmeye yöneltiyor. Bu bağlamda ABD, Avrupa Birliği, Çin, Türkiye, Katar ve Suudi Arabistan'ın yapay zeka stratejilerinin karşılaştırmalı analizi kısaltmalar aşağıdaki tabloda verilmektedir.

Tablo 1. Ülkelerin kapsamlı karşılaştırması

Devlet	Ana hedefler	Etik ve Gizlilik	Zorluklar
ABD	Yenilik, Ortaklıklar, Siber Güvenlik	Gizliliğe orta düzeyde odaklanma	Kapsamlı bir yasal çerçevenin olmaması
AB	Politik standardizasyonu, şeffaflık, bireysel haklar	Katı Yasalar (GDPR)	Üyeler arasında politika çeşitliliği

Çin	Küresel Liderlik, İç Güvenlik	Gizliliğe az odaklanma	Gözetim eleştirisi
Türkye	Yapay zekanın GSYH'ye katkısını %5'e çıkarmak, 2025 yılına kadar 50.000 uzman yetiştirmek ve uluslararası iş birliğini artırmak.	Adalete, çeşitliliğe ve veri korumasına odaklanın. Ve deneysel alanlar için yasal bir çerçeve oluşturulmalı.	Uzman eksikliği ve ileri teknik altyapıya ihtiyaç duyulması.
Katar	Yenilikçi Ekonomi, Eğitim, Etik	Uluslararası gizlilik standartlarına bağlılık	Yerel kadro sıkıntısı
Suudi Arabistan	Bölgesel Liderlik, Yetkinlik Geliştirme, İnovasyon	Küresel gizlilik standartlarına bağlılık	Yerel uzmanlık eksikliği

5.11.1. Etik ve yasal yönler

Etik ve yasal yönler, ulusal önceliklerine göre ülkeler arasında farklılık gösterir:

- **ABD:** Bilişime odaklanmış ancak sert veri koruma yasalarından yoksun.
- **AB:** GDPR gibi etik standartların ve yasaların belirlenmesinde öncü.
- **Çin:** Gözetim için yapay zekâ kullanımı konusunda uluslararası tartışmalara neden oldu.
- **Türkye:** Bireysel verilerin yerel ve uluslararası kanunlara uygun olarak korunmasına daha fazla öncelik verir.
- **Katar:** Bilişimi gizliliğe saygı ile dengelemeye çalışmakta ve bu da onu gelişmekte olan ülkeler için bir model haline getirmektedir.
- **Suudi Arabistan:** Gizlilik ve veri koruma standartlarına saygı gösterirken yeniliği teşvik etmeyi amaçlayan dengeli bir model göstermektedir. Krallık,

açık etik politikalar uygulamaya kararlıdır ve bu da onu küresel sahnede güçlü bir rakip haline getirir.

5.11.2. Ortak fırsatlar ve zorluklar

Paylaşılan Fırsatlar:

- **Hizmetlerin iyileştirilmesi:** Devlet hizmetleri, sağlık ve eğitimde verimliliği artırmak için yapay zekâyı kullanmak.
- **Ekonomiyi canlandırmak:** Bilişim yoluyla yeni ekonomik fırsatlar meydana getirmek.
- **Uluslararası işbirliği:** Küresel yararı teşvik etmek için birleşik politikalar geliştirme imkânı.

Yaygın Zorluklar:

- **Gizlilik koruması:** Verilerin kötüye kullanılmadığından emin olunmalı.
- **Önyargıyı azaltın:** Adil ve kapsamlı algoritmalar geliştirilmeli.
- **Dönüşümleri yönetmek:** Otomasyonun toplumsal, uluslararası ve yerel etkilerinin ele alınması.

5.11.3. Sosyal güvenlik boyutları çerçevesinde stratejik yaklaşımlar

1994 Raporu, güvenliği bölgelerden çok insanlarla, Sosyal güvenliği silahlara değil, kalkınmaya bağlayan yeni bir sosyal güvenlik kavramı öneriyor. Sosyal güvenliğinin hem ulusal hem de küresel endişelerini inceler. Rapor, bu endişeleri yeni bir sürdürülebilir insani gelişme düşüncesi, potansiyel barış getirilerini yakalamak, yeni bir kalkınma işbirliği biçimi ve yapılandırılmış bir uluslararası kuruluşlar sistemi aracılığıyla ele almayı amaçlamaktadır.

Dünya Sosyal Kalkınma Zirvesi'nin bir dünya sosyal sözleşmesini onaylamasını, sürdürülebilir bir insani kalkınma düşüncesini onaylamasını, gelecekteki barış düşüncelerini dikkate alarak küresel bir insan güvenliği fonu oluşturmasını, insan önceliği endişeleri için 2020 sözleşmesini onaylamasını, kaynak seferberliği için küresel vergiler teklifini ve bir Ekonomik Güvenlik Konseyi Oluşturulmasını önerir. (Hdr.undp, 1994)

1994 BM İnsan Güvenliği Raporu temel boyutları şu şekilde belirledi;

- Silaha değil, insani gelişmeye yatırım yapmak.
- Ortaya çıkan barış düşüncelerini dikkate almak için politika yapıcıları dahil etmek.
- Birleşmiş Milletlere kalkınmayı güçlendirmek ve sürdürmek için açık bir yetki vermek.
- Kalkınma işbirliği kavramının sadece yardımı değil, tüm akışları kapsayacak şekilde genişletilmesi.
- Ulusal bütçelerin yüzde 20'sinin ve dış yardımların yüzde 20'sinin insani gelişme için kullanılması konusunda anlaşarak.
- Ekonomik Güvenlik Konseyi'nin kurulması.

5.12. Yapay Zekânın Sosyal Güvenlik Bağlamındaki Etkileri Hakkında Örnek Analizi

Yapay zekâ dünyası, İnsan Güvenliğine yönelik risklerle doludur. Bunlar şu şekilde birkaç farklı kategoriye ayrılır . sistemik veya akut, etik/ahlaki, kısa veya uzun vadeli, ekonomik ve hatta varoluşsal olabilirler. Avantajlar da şu şekilde sıralanabilir çevreden ulaşım ve savaşa, iş dünyası ve sağlık gibi dünyamızın hemen hemen her sektöründe görülmek. Bunların olumlu ve olumsuz yönlerinin değişkenleri 1994 BM İnsan Güvenliği ışığında incelenebilecek kategoriler ise Ekonomik, Kişisel, Gıda, Çevresel, Topluluk, Sağlık ve Siyasi Güvenlik. (Elizabeth, 2019, p. 65)

Yapay zekâ teknolojisinin hızla gelişmesi, insanlar arasındaki etkileşimi de değiştirmektedir. Yapay zekânın insanlarla ilişkisi üzerine odaklanarak, etik ve güvenlik konuları üzerinde durulabilir. Ayrıca, gelecekteki yapay zekâ etkileşimlerine yönelik tahminler, yapay zekânın iş dünyası, eğitim, sağlık ve diğer sektörlerde nasıl kullanıldığı, insanların yapay zekâ ile duygusal bağ kurması ve yapay zekânın sosyal alanda insan üzerindeki etkileri.

- Yapay Zekâ ve İnsan Ahlakı: Yapay zekanın insanlarla etkileşiminde doğan etik ikilemler.
- Yapay Zekâ Güvenliği: Yapay Zekâ sistemlerinin siber tehditlere karşı korunması.
- Yapay Zekâ ve Sağlık: Tıp alanında yapay zekâ uygulamalarının insan sağlığına etkileri.

- Eğitimde Yapay Zekâ: Öğrenme süreçlerinde yapay zekâ kullanımı ve akademik başarıya katkısı.
- Yapay Zekâ ve İş Yaşamı: Otomasyon ve yapay zekanın çalışma hayatına yansımaları.
- Yapay Zekâ Destekli Asistanlar: Günlük yaşamda dijital asistanların rolü ve kullanıcı deneyimi.
- Yapay Zekâ ve Sanat: Yaratıcı süreçlerde yapay zekanın kullanımı ve estetik etkileri.
- Yapay Zekâ ve Sosyal Adaletsizlik: Teknolojinin toplumsal eşitsizlikler üzerindeki etkisi.
- Yapay Zekâ ve Psikoloji: İnsanların yapay zekâ ile kurduğu duygusal bağlar.
- Yapay Zekâ ve Sosyal Ağlar: Sosyal medyada içerik öneri sistemlerinin işleyişi.
- Yapay Zekâ ve Otonom Araçlar: Kendi kendine giden araçlarda yapay Zekâ teknolojisi.
- Yapay Zekâ ve İletişim Teknolojileri: Dil işleme ve çeviri sistemlerindeki gelişmeler.
- İnsan-Makine İş Birliği: Gelecekte yapay zekâ ile ortak çalışma modelleri.
- Yapay Zekâ ve Hukuk: Yapay zekanın yasal düzenlemelerde yol açtığı değişimler.
- Yapay Zekâ ve Veri Gizliliği: Kişisel verilerin korunmasında yapay zekâ uygulamaları.
- Tıp Etiği ve Yapay Zekâ: Sağlık sektöründe yapay zekâ kullanımının etik boyutları.
- Eğitim Etiği ve Yapay Zekâ: Öğrencilerin verilerinin kullanımındaki etik sorunlar.
- Yapay Zekâ ile Duygu Tanıma: İnsan duygularını analiz eden akıllı sistemler.
- Yapay Zekâ ve Eğlence Dünyası: Film, müzik ve oyun sektöründe yapay Zekâ etkisi.

- Yapay Zekâ ve Geleceğimiz: İnsanlığın geleceğinde yapay zekanın oynayacağı rol. (Aldex., 2024)

Yapay zekâ teknolojisinin hızlı gelişimi, insanların hem birbirleriyle hem de makinelerle etkileşimlerini tamamen değiştirmektedir. Bu değişim, özellikle etik ve güvenlik konularında büyük endişelere neden olmaktadır. Etik olarak değerlendirildiğinde, yapay zekâya artan bağımlılık sağlık ve işe alım gibi alanlarda önyargıya dayalı kararlar verilmesine sebep olabilir. Yapay zekâ algoritmalarının şeffaf ve adil kararlar vermesi istenir, fakat pratikte bu algoritmalardaki ayrımcılık sosyal sınıf, cinsiyet veya ırk gibi faktörleri artırabilir. Bu sebeple, adalet ve hakkaniyetin sağlanabilmesi için sıkı bir etik kurallar bütünü oluşturmak gereklidir. Sosyal güvenlik bakımından, yapay zekâ iki farklı yönde etkili olabilir. Hem siber güvenliği artırmak için potansiyele sahip olabilir, hem de saldırıların hedefi olma ihtimali olabilir. Gelişmiş güvenlik önlemlerine ihtiyaç duyulan alanlar, yapay zekâ tabanlı sistemlerin yanı sıra güvenlik ve istihbarat sistemleri, otonom araçlar veya sosyal medya platformları gibi kritik sektörlerdir. Bu sistemlerdeki bir güvenlik açığı, insanların ve toplumun hayatını tehlikeye atabileceği gibi aynı zamanda gizlilik ihlallerine ve hassas verilerin sızmasına yol açabilir. Bu sebeple, yapay zekâ sistemlerinin güvenliği için sağlam ve güvenilir güvenlik protokolleri geliştirilmesi büyük bir öneme sahiptir.

Sağlık sektörü, aynı zamanda yapay zekâ tarafından getirilen büyük değişimlerin etkisini de hissediyor. Yapay zekâ, büyük bir potansiyele sahip olup hastalıkların erken teşhis edilmesi ve kişiye özgü tedavi yaklaşımları sunma konusunda önemli bir rol oynamaktadır. Buna ek olarak, bu kullanım etik sorunları da beraberinde getirebilir örneğin algoritmik önyargılar ve hasta verilerinin gizliliği gibi. Benzer bir şekilde, yapay zekâ eğitim alanında da kullanılarak öğrencilere kişiselleştirilmiş öğrenme deneyimleri sunarak eğitim süreçlerini geliştirmektedir. Ancak, bu gelişme dijital uçurumu derinleştirme tehdidini de oluşturarak teknolojiye erişimi olanlarla olmayanlar arasındaki farkın artmasına neden olabilir. Yapay zekâ, iş dünyasında yeniden şekillenmeye ve otomasyon aracılığıyla verimliliği arttırarak maliyetleri azaltmaya yardımcı oluyor. Aynı zamanda, bu değişim iş gücü dinamiklerini tamamen değiştirmektedir. Şöyle ki. bazı geleneksel mesleklerin yok olmasına, bununla beraber yeni beceri taleplerinin ortaya çıkmasına yol açmaktadır.

AI'nın önemi hala birçok alanda devam etmektedir, ancak sürdürülebilir gelişim için etik ve güvenlik konularına yeteri kadar özen gösterilmelidir.

Yapay zekânın kötüye kullanılması, keyfi gözetimi kolaylaştırarak, bilgi dünyasının kontrolünü ve sansürlenmesini sağlayarak veya ayrımcılık ve önyargıyı sağlamlaştırarak insan haklarını ihlaline neden olabilir. Yapay zekâ, haklara saygılı olacak şekilde tasarlanmış ve geliştirilmiş olsa bile, en son kullanıcı tarafından kötüye kullanılması, sistemin insan haklarını ihlal etmek için kullanılmasına neden olabilir. <CITATION ohc23 \l 1033 (Ohchr.org, 2023)>

5.13. Yapay Zekânın Sosyal Güvenlik Stratejisi Bulgularının Özeti ve Tartışılması

Yapay zekânın sosyal güvenlik stratejileri ödünleşimleri keşfetmede ve iyi düşünülmüş metodolojiyi uygulamada deneme yanılma yönlerinden yararlı olacaktır. Gelecekteki bazı bireysel güvenlik çalışmaları veya NHDR'ler için yararlı olabilir. Analiz ve eyleme daha farklı bir yaklaşımda, özellikle de 1994 HDR'de tanımlanan yedi güvensizlik alanının her birine daha az dikkat eden bir yaklaşımda değerli olacaktır. Bunun yerine, kamuoyu araştırmalarında ve ülkelerdeki insanların deneyimlerine ilişkin diğer analizlerde güvensizliğin hangi boyutlarının tespit edildiğine dikkat edilmelidir. Özellikle toplumsal cinsiyet güvensizliklerine dikkat neredeyse kesinlikle bir endişe alanı olmalıdır, ancak diğerlerine ayrıntılı odaklanma, duruma ve daha önceki NHDR'lerin ve diğer ulusal düzeydeki değerlendirmelerin daha genel bir insani gelişme analizinin bir parçası olarak diğer güvensizlik nedenlerini ne ölçüde ele aldığına bağlı olarak değiştirilmelidir. (Hdr.undp., 2006, p. 30)

Yapay zekâ teknolojilerinin hızlı gelişimi, sosyal güvenlik boyutlarını derinlemesine etkileyerek, bu alanda yeni stratejilerin oluşturulmasını zorunlu hale getirmiştir. Yapay zekâ, sağlık hizmetlerinden ekonomik kalkınmaya, çevresel güvenlikten kişisel güvenliğe kadar birçok alanda hem fırsatlar hem de tehditler sunmaktadır. Bu nedenle, Yapay zekânın sosyal güvenlik üzerindeki etkileri, geniş kapsamlı bir stratejik yaklaşımı gerektirmektedir.

Bulguların Özeti

- Yapay zekânın kişisel güvenlik, siber güvenlik ve veri güvenliğindeki rolü Yapay zekâ, veri ve siber güvenlik ve kişisel güvenlik konularında hem fırsatlar hem de tehditler sunmaktadır. Sosyal medya platformlarında, siber saldırılara karşı koruma

sağlamak için geliştirilen ileri düzeydeki güvenlik önlemlerine rağmen, yapay zekâ temelli saldırılar bu korumayı riske atabilir, yapay zekânın insanın sosyal güvenliği alanında desteklenmesi için güvenilir sistemlere ve protokollere ihtiyaç duyulduğunu göstermektedir.

• Yapay zekâ ve sosyal eşitsizlikler: Yapay zekâ, sosyal adaletsizlikleri ve dengesizlikleri artırma potansiyeline sahiptir. Dijital uçurum, özellikle teknolojiye ulaşma imkânı bulunmayan bireyler için büyümeye devam ediyor. Dolayısıyla, yapay zekânın adil bir şekilde uygulanabilmesi için en kısa zamanda çeşitli politikalar hayata geçirilmelidir.

• Yapay Zekânın Ekonomik Güvenlik Üzerindeki Etkileri: Yapay zekânın ekonomik güvenliği desteklemesi ve verimliliği artırması amacıyla iş dünyasında otomasyon sağlayabileceği ancak aynı zamanda sosyal dengesizlikleri artırarak iş kaybına sebep olabileceği sonucuna varılmıştır. Bu sebeple, yapay zekânın ekonomik etkilerini hafifletmek için işgücünün eğitimine ve yeniden beceri geliştirme programlarına yatırım yönelinmesinin büyük bir önemi vardır.

• Yapay Zekânın Sağlık Sektöründeki Etkileri: Yapay zekâ sağlık hizmetlerinde devrim niteliğinde yenilikleri beraberinde getirirken, ortaya çıkan etik sorunlar da dikkate alınmalıdır. Sağlık hizmetlerinde yapay zekâ uygulanırken, algoritmik önyargılar (dil, din, ırk v.s.) ve hasta veri gizliliği gibi kritik unsurları önemsemek önemlidir.

Tartışma

Yapay zekânın yararları, kişisel güvenlikten sosyal güvenliğe kadar bir dizi alanda stratejik planlama ve uygulama ile yönetilmelidir. Ancak, bu teknolojinin sağladığı yararların yanında dikkate alınması gereken tehditler de göz ardı edilmemelidir. Yapay zekâ, veri güvenliği ve gizliliğini olumsuz yönde etkilemeden ve sosyal yapıyı istikrarsızlaştırmadan uygulama alanlarına entegre edilmelidir.

Yapay zekânın veri gizliliği konuları ve etik sorunları, sosyal güvenlik stratejilerinin öncelikleri arasında yer almalıdır. Toplulukların güvenliği ve refahı için, sağlam rehberlik ve yönetimin yapay zekâ tarafından tesis edilmesi çok önemlidir. Bu önem sosyal medya platformlarında yapay zekânın sosyal güvenlik üzerindeki etkilerini izlemeye başlamak ve bu etkilerin dengesini sağlayabilmek için gerekli önlemleri almak sürdürülebilir bir toplumsal yapı oluşturmak açısındandır.

5.14. Yapay Zekâ Çağında Sosyal Güvenliğin Sağlanması İçin Öneriler

Yapay zekâ çağında, veri gizliliği ve sosyal güvenlik konuları giderek daha fazla önem kazanmıştır. Sosyal medya platformları, kullanıcılarının büyük miktarlarda kişisel verilerini toplar ve işlerken, bu verilerin güvenliği ve gizliliği konusunda ciddi endişeler ortaya çıkmaktadır. Bu açıdan bakıldığında, güvenlik açıklarının minimize edilmesi, veri gizliliğinin korunması ve kullanıcı haklarının korunması için stratejik adımların atılması gerekmektedir.

Kuruluşlar, insan hakları risk yönetimi çerçevesine dayalı olarak insan hakları risklerinin ele alınmasına yardımcı olmak için önerilen eylemler, insan hakları risklerini belirlemeye, azaltmaya, önlemeye ve ele almaya yardımcı olan bu eylemleri teşvik etmek için etkilerini ve kaynaklarını kullanmalıdır. Yukarıdaki yaşam döngüsü aşamalarında tanımlanan riskleri yönetmek için yönetim, planlama ve ölçüm olmak üzere üç kurumsal işlevi tanımlayan Yapay Zekâ Risk Yönetimi çerçevesinden türetilen öneriler sunar. (State.gov، 2024)

Kapalı güvenlikli platformlar üzerinden yeniden kayıt yapılarak sosyal medyanın düzenlenmesi Sosyal medya platformlarının kayıt ve abonelik süreçleri, yetkili güvenlik otoritelerinin denetiminde bulunan kapalı güvenlik ağlarına aktarılmalıdır. Bu önlem, yaymayı amaçlayan terör ve korkuya neden olabilecek kişilerin tespit edilmesini veya verilerin yönetme yeteneğini geliştirmeyi ve dezenformasyonu hacklemeyi hedeflemektedir. Bu düzenleme ile gözetim ve denetim güçlendirilebilir ve toplumu siber ve bilgi tehditlerinden koruyan bu platformlarda dolaşan içerik güvenli ve emniyetli hale getirilebilir.

1. Yapay Zekâ Tabanlı Güvenlik Sistemlerinin Geliştirilmesi : Yapay zekâ, sosyal medya platformlarında ortaya çıkan güvenlik tehditlerini tespit etme ve engelleme amacıyla kullanılabilir. Bir örnek olarak, geliştirilebilen yapay zekâ algoritmaları şüpheli paylaşımları gerçek zamanlı izleyebilir ve analiz edebilir. Kullanıcıların verilerini koruma altına alabilen bu sistemler, siber saldırıları erken aşamalarda tespit edebilir.
2. Veri Minimizasyonu İlkesinin Benimsenmesi: Sosyal medya platformları, yalnızca zorunlu verileri toplamak ve bu verilerin kullanımını sınırlamakla kalmamalı. Aynı zamanda fazla veri toplama, veri sızıntılarına ve gizlilik ihlallerine sebep olabilir.

Bu yüzden, veri gizliliğini korumak için kritik bir strateji olan veri minimizasyonu ilkesine önem verilmektedir.

3. Kullanıcıların Bilgilendirilmesi ve Onaylarının Alınması: Kullanıcılara, verilerinin nasıl toplandığı, saklandığı ve kullanıldığı hakkında net bir şekilde bilgilendirme yapılmalıdır. Bunun yanı sıra, verilerin işlenmesi için kullanıcıların net bir şekilde onayları alınmalıdır. Bu şekilde veri gizliliği ihlallerini önlemenin önemli bir adımı gerçekleştirilmiş olur.

4. Düzenli Güvenlik Denetimlerinin Yapılması: Sosyal medya platformları, veri güvenliğini korumak amacıyla periyodik olarak güvenlik denetimlerine tabi tutulmalıdır. Denetimler potansiyel güvenlik açıklarını tespit eder ve düzeltici önlemlerin alınmasına yol açar.

5. Veri gizliliği ve sosyal güvenliğe ilişkin yasal düzenlemelerin oluşturulması: Hükümetler, sosyal medya platformlarında veri gizliliğini ve güvenliğini düzenlemek ve izlemek için daha sıkı çalışmalıdır. Bu, platformların sorumluluklarını artırarak kullanıcı verilerinin güvenliğini sağlayacaktır.

SONUÇLAR VE ÖNERİLER

Modern teknoloji, özellikle yapay zekâ teknikleri, hukuki, sosyal ve ekonomik ve yaşamın çeşitli yönlerini temelden etkileyen en önemli gelişmelerden biridir. Yapay zekâ: İnsan gibi hareket edebilen düşünebilen ve geçmiş verileri anlayarak öğrenme yeteneğine sahip robotik programlar ve teknolojilerdir. Yaşam standartlarının ve bireysel bürokrasinin korunması için yapay zekâ teknolojilerinin düzenlenmesi ve sosyal medyada gizlilik ihlali ile ilgili tehlikelerin göz önünde bulundurulması gerekmektedir.

Yapay zekâ çağında toplum ve insan güvenliği, verilerinin korunması ve ülkelerin internet, sosyal medya platformları ve medya ile ilgili krizleri yönetme ve suçları önleme faaliyetlerinde yapay zekâ tekniklerinin kullanılması ile ilgili daha önce yapılan çalışmalarda, sosyal güvenlik konusunda yetkili makamların temel görevlerinden biri olan teknolojik gelişmelerin birey ve toplum yararına olması gerektiğinin doğrulanması ile ilgilidir. Amerika Birleşik Devletleri, Avrupa Birliği, Çin, Katar ve Suudi Arabistan'daki örnekleriyle konu ele alındığında yapay zekâyı kurumlarında, eğitimlerinde, teknolojilerinde ve altyapılarında mesleki gelişimlerinde geliştirmek isteyen bu ülkelerin, uluslararası yasalara uygun olarak gizlilik ve veri koruma standartlarına uyumu sağlarken gelecek nesilleri teknolojiyi benimsemeye hazırlamak için stratejileri araştırıldı. Bu rapordaki farklı bölümlerin kapsamlı bir analizine dayanarak, teknik ilerlemeyle ilgili fırsatları ve zorlukları anlamak için bir temel olarak kabul edilebilecek birkaç önemli nokta ortaya çıkmaktadır. Bu sonuçların analizi aşağıdakileri içermektedir:

Yapay zekâ ve kişisel verilerin korunması

Yapay zeka çağında kişisel verilerin korunması oldukça önemli bir konu haline gelmiştir. Veri madenciliği, makine öğrenmesi ve benzeri teknolojiler, uygulamaları verimli ve doğru hale getirmek için büyük miktarda kişisel bilgiye ihtiyaç duyar. Ancak verilere olan bu artan bağımlılık aynı zamanda artan gizlilik risklerine de yol açıyor. Örneğin, birçok ülkede popüler bir araç haline gelen ve gizlilik ihlalleri konusunda endişelere yol açan yüz tanıma gibi veriler ve teknolojiler, kullanıcıların bilgisi veya izni olmaksızın kitlesel gözetleme için kullanılabiliyor ve bu da onların haklarını ihlal ediyor. Mevcut veri koruma mevzuatı çağdaş ihtiyaçları karşılamada hala yetersiz kalmaktadır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve

Kaliforniya Tüketici Gizliliği Yasası (CCPA) gibi çığır açan mevzuatlara rağmen, uygulamada önemli zorluklar devam etmektedir.

Sosyal Güvenlik ve İnsan Hakları

Modern sosyal güvenlik sistemleri, bireyselleştirilmiş hizmetler sağlamak ve etkinliği yükseltmek için yapay zekâ teknolojileri üzerinde giderek daha fazla çalışıyor. Örneğin, kaynakları daha etkin bir şekilde dağıtmak için nüfus verilerini analiz etmek için kullanılan algoritmalar insan haklarını etkileyen potansiyel riskler taşıyabilmektedir. Algoritmik önyargıların bir sonucu olarak istem dışı ayrımcılığa yol açarak eşitliğe zarar verebilirler. Örneğin, yapılan araştırmalar, bazı işe alım algoritmalarının, eğitildikleri veri kalıpları nedeniyle azınlıkları veya kadınları dışlayabileceğini göstermiştir. Ayrıca, sosyal medyada sahte haberlerin yayılması, toplumların istikrar ve düzenini etkileyen en önemli zorluklardan biridir. Bu olgu medya kaynaklarına olan güveni zayıflatmakta ve aynı zamanda sosyal güvenliği tehdit edebilmektedir. Araştırmalar, Yanlış bilgi, doğru haberden daha çabuk yayılır. ve siyasi ve sosyal kararlar üzerinde olumsuz etkilere yol açtığını gösteriyor. Farklı toplumlar arasındaki dijital uçurum, teknolojiye erişimde önemli eşitsizliklere yol açarak sosyal zorlukları artırmaktadır.

Yasal ve etik sorunlar

Yapay zekâ uygulamalarının karşılaştığı en büyük sorunlardan biri yasal ve şeffaflık hesap verebilirlik eksikliğidir. Çoğu zaman , kararların algoritmalar tarafından nasıl alındığı net değildir ve bu da adaletle ilgili endişeleri artırmaktadır. Yüz tanıma gibi teknolojiler, bireylerin yasa dışı gözetimine yol açacak şekilde kullanılabilecekleri için bu sorunu vurgulamaktadır. Örneğin, raporlar, sosyal medya platformlarında bazı yüz tanıma sistemlerinin olduğunu göstermiştir. Bu sistemler gösterileri veya belirli gruplara karşı ayrımcılığı izlemek için kullanılmaktadır. Ayrıca, birçok uygulama algoritmik önyargılardan muzdariptir ve bu da farklı insan kategorileri arasında eşit olmayan sonuçlara yol açar. Bu sistemler özellikle istihdam veya ceza adaleti gibi hassas alanlarda kullanıldığında, adalet ve eşitlikle ilgili derin etik sorunları gündeme getirmektedir. Ayrıca bu konular, algoritmaların gözden geçirilmesi, etik ve yasal standartlara bağlılıklarının sağlanması için bağımsız komisyonların kurulmasını gerektirmektedir.

Sosyal medya platformları ve ilgili zorluklar

Sosyal medya Sosyal medya ağları, günlük hayatın önemli bir parçasıdır ve bireylerin içerik oluşturup paylaşmasına ve topluluklar oluşturmasına imkân tanır. Ancak bu platformlar, kullanıcılar hakkında büyük miktarda veri toplamak için de kullanılır. Verilerin bu denli büyük miktarda toplanması ve kullanımı, onu kimlik hırsızlığı ve siber saldırılar gibi birçok tehdide karşı savunmasız hale getirir.

Genel Veri Koruma Yönetmeliği (GDPR) gibi yasalar olsa da, özellikle uluslararası sınırların ötesinde faaliyet gösteren platformlar söz konusu olduğunda, bunların uygulanmasında bazen engellerle karşılaşmaktadır. Örneğin, teknoloji şirketleri ülkeler arasındaki farklı yasalarla başa çıkmak ve bu da yasal uyumluluğu daha da karmaşık hale getirmektedir. Etik zorluklar ayrıca, verilerin davranışlarını analiz etmek için kullanılması ve kullanıcıların bilgileri olmadan hedefli reklamlarla hedeflenmesi gibi yasa dışı yollarla da kullanılmasını içerir. Bu uygulamalar, gizlilik ve güven konusunda önemli endişelere yol açmaktadır.

Ulusal ve uluslararası stratejiler

Ülkeler, bilişim ve güvenlik arasındaki dengeye odaklanarak yapay zekâya yönelik farklı stratejiler ve politikalar benimsiyor. Amerika Birleşik Devletleri ve Avrupa'da, veri koruma ve etik bilişime büyük önem verilirken, Çin gibi ülkeler büyük yatırımlar yaparak bu alanda küresel liderlik elde etmeye çalışıyor. Bununla birlikte, kapsamlı yasaların olmaması, algoritmik önyargılar ve otomasyondan kaynaklanan sosyal dönüşümlerin yönetilmesi gibi herkesin karşı karşıya olduğu ortak zorluklar vardır. Ülkeler arasındaki organize çabalar, teknolojinin etik ve sorumlu kullanımını sağlamak için küresel standartların geliştirilmesine katkıda bulunabileceğinden, Bu zorlukların aşılması için küresel iş birliği gereklidir.

Öneriler

Yasal ve düzenleyici çerçevelerin güçlendirilmesi

Yapay zekâ alanındaki hızlı teknolojik gelişmelerle orantılı olarak yeni ve daha ayrıntılı uluslararası mevzuat geliştirilmelidir. Bu mevzuat, sosyal güvenliği ve özel bilgilerin güvence altına alınmasını temin etmek. için açık, anlaşılabilir, net standartlar ile birlikte özel hayatın gizliliğinin ihlallerini önlemek için katı cezalar içermesi gerekmektedir.

Her ne kadar birçok ülke, dijital çağa yakalayabilmek için mevzuatlarını değiştirmeye istekli olsa da, kapsamlı veri izleme, mahremiyet hakkının anayasal ve yasal korumasının çok ötesindedir. Bu uluslararası sözleşmeler, dijital mahremiyet hakkına uluslararası meşruiyet kazandırıyor ve gözetleme, casusluk ve kimlik avını izlemek için uluslararası bir etik çerçeve sağlıyorsa da, uluslararası insan hakları hukukunun harekete geçirilmemesi ve uluslararası insan hakları örgütlerinin şeffaflık raporlarının ve davalarının dev internet ve telekomünikasyon şirketleri tarafından görmezden gelinmesi gerçek ve etkili bir uluslararası koruma sağlamaz. (Saad A. M., 2021, pp. 20-21)

Toplum bilincini artırmak

Bireylerin kişisel verilerini korumasının önemi konusunda dikkatlerini yoğunlaştırmak ve Teknoloji güvenle nasıl kullanacaklarını anlamaları için geniş çaplı bilinçlendirme kampanyaları düzenlenmelidir. Örneğin, bireylere kendilerini siber tehditlerden nasıl koruyacaklarını ve yanlış haberleri nasıl tanıyacaklarını öğretmek için eğitimler düzenlenebilir.

Dijital eğitim, hem öğrenmede bağımsızlığı ve esnekliği artırma hem de etkileşimli teknoloji ile etkileşimi artırma açısından farkındalık ve öğrenme yeteneklerini derinden etkilemiştir. Sosyal iletişim ve dikkat dağınıklığı üzerindeki etki gibi bazı zorluklar ortaya çıkabilse de, dijital eğitim, kendi kendine öğrenmeyi teşvik etmek ve sonucunda bilişi genişletmek için muazzam fırsatlar sunar. Dijital eğitim, dünyayı kavrama ve onunla iletişimde bulunma şeklimizi yeniden şekillendirerek bireysel ve kolektif farkındalığın gelişimi için yeni bir ufuk açabilir. (El-Bayati, 2024, p. 85)

Bağımsız yapay zekâ izleme komiteleri kurulmalı

Yapay zekânın kullanımlarını gözden geçirmek, etik ve güvenlik standartlara uyduklarından emin olmak için, sosyal güvenlik, hukuk ve teknoloji uzmanlarından oluşan bağımsız organlar oluşturulmalıdır. Bu komiteler ayrıca anlaşmazlıkların, kişisel veri ihlallerinin ve siber tehditlerin çözülmesine de yardımcı olabilir.

IŞİD terör örgütünün 2014 yılından itibaren farklı yaşlardaki gençleri organizasyona dahil etmek maksadıyla hedeflenen kişilerin sempatisini kazanmak için bir medya stratejisiyle gençleri cezbetmesinde olduğu gibi, internetin yüksek hızının terör operasyonlarını finanse etmek, üyelerinin hareketini ve bazı bankalarla İnternet

üzerinden kara para aklama operasyonlarını finanse etmek, silah ve teçhizat satın almak amacıyla finansal bağışları artırmak için büyük olanakların açılmasını sağladığından, terörizmin tüm bilgi ve uygulamalara ilişkin istihbarattan yararlanmakla sınırlı olmadığı, finansman elde etmek amacıyla kullanıldığı açık görünüyor. (Airot, 2024, p. 24)

Uluslararası işbirliğinin güçlendirilmesi

Yapay zekâdaki ilerlemeler, düzenleyici çerçeveler ve birleşik standartların geliştirilmesi için küresel iş birliğinin güçlendirilmesi, devletlerin bilgi alışverişini artırmalarını ve deneyimlerini paylaşarak, siber suçlar ve etik ihlaller gibi ortak zorlukları birlikte ele almalarını gerektirir.

Yapay ve dijital zekâ ve gelişmekte olan teknolojiler, sürdürülebilir kalkınma ve dünyada önemli bir değişiklik yapmak için katalizör bir rol oynayarak büyük bir etki yaratmaktadır. İnsanın ve gezegenin çıkarlarının anında ve alıcı bir şekilde gerçekleştirildiği muazzam bir ilerleme potansiyeli sunar. Uluslararası alanda ve paydaşlarla iş birliğini güçlendirerek, sorumluluk ve sürdürülebilirlik ruhunun hakim olduğu kapsayıcı bir dijital gelecek için çalışarak bu potansiyeli gerçekleştirmeye ve riski yönetme ve bu konuda bu sözleşmeye küresel bir dijital sözleşme eklenmiştir. (Undocs.org, 2024, s. 25)

Teknolojiyi eğitime entegre etmek

Gelecek nesillerin teknolojiyi sorumlu bir şekilde anlamaları ve kullanmalarını sağlamak için yapay zekâ ve veri koruma kavramları okullardaki müfredat programlarına entegre edilmelidir. Yeni ve yenilikçi çözümler için bu alandaki akademik araştırmalar da teşvik edilmelidir.

Dijital eğitim, her öğrenci için kendi seviyesine ve ihtiyaçlarına göre özelleştirilmiş öğrenim yollarının oluşturulmasına imkân tanır. dijital sistemler öğrencinin ilerlemesini takip edebilir ve yeteneklerine uygun ders içerikleri önerebilir. Bu şekilde. öğrencinin, ilerlemesini somut olarak görebileceği ve anında geri bildirim alabileceği kişisel motivasyonu teşvik eder, bu da eğitimsel gelişim düzeyine ilişkin öz farkındalığını artırır. (El-Bayati, 2024, p. 83)

Etik bilişimi desteklemek

Yaşam standardını yükseltmek ve Toplumsal adaleti desteklemek etmeyi amaçlayan yapay zekâ uygulamalarının geliştirilmesi desteklenmelidir. Etik yenilik, biyometrik özelliklere (Biyometrik Parmak Taraması Veya Yüz Biyometrisi gibi) dayalı karmaşık doğrulama sistemleri oluşturmak için kriptografik tekniklerin geliştirilmesi ve sistemlerin güvenliğini değerlendirmek ve güvenlik açıklarını sürekli olarak analiz etmek için yapay zekânın geliştirilmesi gibi sorunlara çözümler geliştirmeyi içerebilir.

Teknolojinin doğası gereği ne olumlu ne de olumsuz olduğunu, esasen kullanım şeklinin belirleyici olduğunu unutmamalıyız. Onları kullanma şeklimiz çok önemlidir. Süper zekâyı insan yaşam kalitesini iyileştirmek, karmaşık küresel sorunları çözmek, bilgi ve anlayışın sınırlarını genişletmek için bir araç olarak kullanabilirsek, bu teknolojiyi doğru kullandığımızı söyleyebiliriz. (Milad, 2024, s. 26).

KAYNAKÇA

Ab.gov. (2018, 05 25). *www.ab.gov.tr*. Retrieved from Genel Veri Koruma Yönetmeliği (GDPR).: https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf

Abrahim, M. S. (2021). *Veri Devrimi ve Yasal ve Uluslararası Müdahale Modelleri Bağlamında Dijital Gizlilik Hakkı - Sayı 15*. Mısır: Medya Araştırmaları ve Çalışmaları Dergisi.

Abudureyimu, Y. (2021, 09 30). *Yapay zeka uygulamalarının kişisel verilerin korunmasına ilişkin yaratabileceği sorunlar ve önerilen çözümler.* Retrieved from dergipark.org.tr: https://dergipark.org.tr/en/pub/iticusbe/issue/65071/863505

Accessnow. (2018, 04 10). *www:accessnow.org*. Retrieved from Cambridge Analytica: 87 milyon kişinin kişisel verilerini elde etmenin yasa dışı bir yolu: https://tinyurl.com/2s4dsx98

Adlbelge. (2024, 08 20). *www.adlbelge.com.* Retrieved from ADL Uluslararası Belgelendirme ve Eğitim Hizmetleri Limited Şirketi: https://www.adlbelge.com/iso-27001-bilgi-guvenligi-risk-yonetim-proseduru

Ahmed, H. H. (2020). *Yasal koruma ve teknik zorluklar arasında kişisel verilerin mahremiyeti hakkı: karşılaştırmalı bir çalışma* . Mısır: Arapça Kitaplar ve Araştırmalar Evi.

Ahmed, K. H. (2020). *Yasal koruma ve teknik zorluklar arasında kişisel verilerin mahremiyeti hakkı: karşılaştırmalı bir çalışma* . Mısır: Kitaplar ve Arap Araştırmaları Evi.

Airot, A. (2024). *Yapay Zekanın Geleceği: Yasal ve Etik Zorluklar*. Almanya.: Ahmat Bohker.

Aldex. (2024, 8 21). *www.aldex.com.* Retrieved from Yapay Zeka ve İnsan İlişkisi: Etik, Güvenlik ve Gelecekteki Etkileşimler: https://www.aldex.com.tr/Blogdetay/60-Yapay-Zeka-ve-Insan-Iliskisi-Etik-Guvenlik-ve-Gelecekteki-Etkilesimler

Al-Hashemi, R. (2018). *Electronic Terrorism* . Amman: Dar Amjad for Publishing and Distribution.

Alhurra. (2020, 08 01). *www.alhurra.com*. Retrieved from Amerika neden TikTok uygulamasını yasaklamak istiyor?: https://tinyurl.com/2w7ztfjk

Alhurra. (2024, 03 15). *www.alhurra.com*. Retrieved from Amerika neden TikTok uygulamasını yasaklamak istiyor?: https://tinyurl.com/2w7ztfjk

Aljazeera. (2024, 08 21). *www.aljazeera.net.* Retrieved from Sosyal Medyanın Artıları ve Eksileri: https://tinyurl.com/ms2pn5hm

Arastirma.disk. (2015, 11 10). *arastirma.disk.org.tr*. Retrieved from Uluslararası Sosyal İnsan Hakları Sempozyumu: https://arastirma.disk.org.tr/wp-content/uploads/2020/08/2015sosyalhaklar.pdf

Babos , T. T. (2021, 10 05). *press.mater.uni-mate.hu.* Retrieved from Siber Uzayda Dijital Güvenlik Politikası Macaristan Tarım ve Yaşam Bilimleri Üniversitesi Gödöllu,: https://press.mater.uni-mate.hu/151/8/kibereng-final-digit_j%C3%B3%20ISBN-nel.pdf

Babos, T. T. (2021, 10 05). *press.mater.uni-mate.hu.* Retrieved from Siber Uzayda Dijital Güvenlik Politikası - Macaristan Tarım ve Yaşam Bilimleri Üniversitesi Gödöllu: https://press.mater.uni-mate.hu/151/8/kibereng-final-digit_j%C3%B3%20ISBN-nel.pdf

Ber, A. S. (2022, 07 19). *Yapay Zekânın Hukuki Statüsü Ve Kişilik Hakkı Kapsamında Değerlendirilmesi.* Retrieved from dergipark.org.tr: https://dergipark.org.tr/en/pub/duamydad/issue/76833/1284619

Bilal, A. A. (2019). *Yapay zeka modern teknolojilerde bir devrimdir.* Mısır, Kahire: Arap Eğitim ve Yayıncılık Grubu.

Birleşmiş Milletler. (1994, 01 01). *Human Development Report 1994 Birleşmiş Milletler.* Retrieved from https://hdr.undp.org: https://hdr.undp.org/content/human-development-report-1994

Cbddo.gov. (2021, 08). *https://tinyurl.com/mryejw29*. Retrieved from Türkiye'nin Ulusal Yapay Zeka Stratejisi – 2021-2025: https://tinyurl.com/mryejw29

Consilium.europa. (2024, 5 21). *www.consilium.europa.eu.* Retrieved from Yapay zeka yasası: Konsey, YZ ile ilgili ilk dünya çapındaki kurallara nihai yeşil ışığı yaktı: https://tinyurl.com/5kpzmjvs

Data.consilium.europa. (2024, 5 14). *https://data.consilium.europa.eu.* Retrieved from Regulation laying down harmonised rules on artificial intelligence (artificial intelligence act: https://tinyurl.com/atys7e5r

El Şair, A. A. (2015, 08 20). *Sosyal medya ve sosyal davranış.* Ürdün, Amman: Dar Al Safa Yayıncılık ve Dağıtım. Retrieved from social media.

El-Bayati, F. (2024). *Dijital Çağda Bilinç: Teknolojik Dönüşümlerde Neden-Sonuç İlişkilerinin Felsefi Analizi.* Londra: Faris El-Bayati.

Elizabeth, W. (2019, 07 25). *https://dspace.cuni.cz.* Retrieved from Yapay Zeka ve İnsan Güvenliği: Yapay Zeka Strateji Analizi: https://dspace.cuni.cz/bitstream/handle/20.500.11956/177198/120348672.pdf?sequence=1

Ellen Glover. (2024, 04 2). *https://builtin.com/artificial-intelligence.* Retrieved from Yapay zeka (YZ) nedir?: https://builtin.com/artificial-intelligence

Ensari, H. (2023, 12). *Yapay Zeka Çağında Kişisel Veri Mahremiyeti.* Retrieved from dergipark.org.tr: https://dergipark.org.tr/en/pub/umay/issue/81365/1357617

Epc.ae. (2024, 5 6). *www.epc.ae.* Retrieved from Yapay Zeka Stratejisi: Çin'in Kendi Kendine Yeterlilik Yoluyla Rekabet Avantajı: file:///C:/Users/DELL/Downloads/estiratijiat-aldhaka-alaistinaei-alsiynia%20(2).pdf

Gençoğlu, M. T. (2023, 12). *www.researchgate.net.* Retrieved from İstihbarat Alanında Kuantum Teknolojilerinin: https://www.researchgate.net/profile/Mtuncay-Gencoglu/publication/377085142_Istihbarat_Alaninda_Kuantum_Teknolojilerinin_Kullanimi_Muharrem_Tuncay_GENCOGLU/links/65950baa0bb2c7472b2c7a60/Istihbarat-Alaninda-Kuantum-Teknolojilerinin-Kullanimi-Muharrem-Tunc

Globaltechmagazine. (2022, 04 05). *www.globaltechmagazine.com.* Retrieved from Sosyal medya güvenliği ve gizliliği için 7 tavsiye: https://www.globaltechmagazine.com/2022/04/05/sosyal-medya-guvenligi-ve-gizliligi-icin-7-tavsiye/

Gloddia. (2024, 01 5). *www.gloddia.com*. Retrieved from x-yonetimi: https://www.gloddia.com/x-yonetimi/

Hdr.undp. (1994, 01 01). *https://hdr.undp.org.* Retrieved from İnsan Gelişimi Raporu 1994: https://tinyurl.com/bdfmyv3x

Hdr.undp. (2006, 01 1). *hdr.undp.org.* Retrieved from Tematik Rehberlik Notu: https://hdr.undp.org/system/files/documents/human-security.pdf

Hurriyet. (2022, 4 5). *www.hurriyet.com.* Retrieved from Sosyal medya güvenliği ve gizliliği için 7 tavsiye: https://www.hurriyet.com.tr/teknoloji/sosyal-medya-guvenligi-ve-gizliligi-icin-7-tavsiye-42037319

İbrahim, M. S. (2021). *Veri devrimi ve yasal ve uluslararası müdahale kalıpları çerçevesinde dijital gizlilik hakkı,.*

İnnova. (2022, 09 8). *https://www.innova.com.tr/blog/yapay-zeka-etigi-nedir*. Retrieved from yapay-zeka-etigi-nedir: https://www.innova.com.tr/blog/yapay-zeka-etigi-nedir

İnnova. (2022, 09 8). *www.innova.com.tr*. Retrieved from Yapay zeka etiği nedir?: https://www.innova.com.tr/blog/yapay-zeka-etigi-nedir

Jack, W. (2011, 01 04). *www.nber.org*. Retrieved from Mobil Para: M-Pesa'nin Ekonomisi: https://www.nber.org/system/files/working_papers/w16721/w16721.pdf

Karjian, R. (2024, 10 24). *www.techtarget.com*. Retrieved from The history of artificial intelligence: Complete AI timeline: https://www.techtarget.com/searchenterpriseai/tip/The-history-of-artificial-intelligence-Complete-AI-timeline

Kaya, M. B. (2021, 01 09). *Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi.* Retrieved from dergipark.org.tr: https://dergipark.org.tr/en/pub/ihm/article/879251

Köse, U. (2022). *Yapay Zeka Felsefesi - 1 Temmuz 2022.* İstanbul, Zeytinburnu : T.C. Kültür ve Turizm Bakanlığı, Ofset Yayıncılık.

Kotil, Z. Ö. (2022, 05). *Yapay Zekâ Teknolojilerinin Kişisel Verilerin Korunmasına Etkileri, Mevcut Problemler Ve Çözüm Önerileri.* Retrieved from tez.yok.gov.tr: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Küçükkavruk, K. (2023, 03 16). *Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk.* Retrieved from tez.yok.gov.tr: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Kurtuluş, Ö. (2023, 08). *www.stgm.org.tr*. Retrieved from Yapay Zeka ve Sivil Toplum: İyi Amaçlar için Yapay Zeka Ankara: https://www.stgm.org.tr/sites/default/files/2023-09/yapay-zeka-ve-sivil-toplum.pdf

Leginfo.legislature. (2018, 09 23). *https://leginfo.legislature.ca.gov.* Retrieved from Kaliforniya Tüketici Gizliliği Yasası -2018: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

Maptriks. (2024, 08 21). *https://maptriks.com.* Retrieved from Gelecekte Yapay Zeka ve Veri Analitiği Üzerine Etkisi: https://maptriks.com/gelecekte-yapay-zeka-ve-veri-analitigi-uzerine-etkisi/

Mendel, T. (2012). *Küresel Anket- Çevrimiçi Gizlilik ve İfade Özgürlüğü Hakkında.* Fransa: Birleşmiş Milletler Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü UNESCO Yayınları.

Microdestek. (2024, 07 5). *https://microdestek.com.* Retrieved from Yapay Zekâ Kullanımının Etik Boyutları ve Mevcut Düzenlemeler: https://microdestek.com.tr/yapay-zeka-kullaniminin-etik-boyutlari-ve-mevcut-duzenlemeler.html

Milad, W. (2024). *Yapay Zeka ve İnsanlık: Makine Hakimiyeti Çağında Etik Zorluklar.* İRAN: Dr. Alaa Taaima.

Mobitek. (2024, 8 19). *https://mobitek.com.* Retrieved from Sosyal Medya Yönetiminin Önemi: https://mobitek.com/sosyal-medya-yonetimi/?gad_source=1&gclid=CjwKCAjw_ZC2BhAQEiwAXSgClnKcrKdyvHd2Xml6ttfigrh5QzNQ2Rlb1mfMn1nVjMqca19aZze8axoCUZsQAvD_BwE

mpdv. (2024, 09 09). *www.mpdv.com.* Retrieved from Yapay zeka (YZ) nedir?: https://www.mpdv.com/en/innovation-knowledge/kuenstliche-intelligenz-in-der-produktion/ki-definition-und-geschichte

Nour, A. A. (2005). *Endüstriyel zeka dünyasına giriş* . Suudi Arabistan, Kral Abdülaziz, Bilim ve Teknoloji Şehri: Lotus Elektronik Kütüphanesi,.

Ohchr.org. (2023, 07 12). *https://www.ohchr.org.* Retrieved from Yüksek Komiser: İnsan hakları yapay zekanın merkezine yerleştirilmelidir: https://www.ohchr.org/ar/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner

Parliament, U. (2024, 01 05). *www.parliament*. Retrieved from Social Insurance and Allied Services (Beveridge Report): https://www.parliament.uk/about/living-heritage/transformingsociety/livinglearning/coll-9-health1/coll-9-health/

Pasha, H. s. (2020). *Sosyal Medya Derinliklere Yolculuk.* Suriye: Dar Şam Kalem.

Privacy, N. (2024, 08 20). *https://usaidmomentum.org/ar/privacy/.* Retrieved from https://usaidmomentum.org/ar/privacy/

Qcai-blog.qcri. (2020). *https://qcai-blog.qcri.org.* Retrieved from Yapay zeka alanında Katar Ulusal Stratejisi: https://qcai-blog.qcri.org/wp-content/uploads/2020/04/QCRI-Artificial-Intelligence-Strategy-2019-AR.pdf

S S Corporation. (2024, 01 02). *www.ssc.gov.jo*. Retrieved from Sosyal Güvenlik Kanunu 1978: https://www.ssc.gov.jo/en/for-the-year-1978/

Saad, A. M. (2021). *Veri devrimi ve yasal ve uluslararası müdahale kalıpları bağlamında dijital gizlilik hakkı Medya Araştırmaları ve Çalışmaları Dergisi - Sayı 15.* Mısır: Shorouk Uluslararası Medya Yüksek Enstitüsü.

Saad, A. M. (2021). *Veri Devrimi ve Yasal ve Uluslararası Müdahale Modelleri Bağlamında Dijital Gizlilik Hakkı Medya Araştırmaları ve Çalışmaları Dergisi - Sayı 15.* Mısır: Shorouk Uluslararası Medya Yüksek Enstitüsü.

Sami, Ş. (2008). *Ag güvenliği.* msir: Fayoum Üniversitesi.

Sdaia.gov. (2024, 04). *https://sdaia.gov*. Retrieved from Suudi Arabistan'ın Yapay Zeka Stratejisi: https://sdaia.gov.sa/ar/MediaCenter/KnowledgeCenter/ResearchLibrary/SDAIAPublications13.pdf

Ssa.gov. (2024, 01 02). *ssa.gov/history/ottob.html*. Retrieved from Sosyal Güvenlik Tarihi -Bismarck'ın sanatı Alman Shankler 1862-1890: https://www.ssa.gov/history/ottob.html

Ssa.gov. (2024, 01 03). *www.ssa.gov/history*. Retrieved from Sosyal Güvenlik Tarihi -Bismarck'ın sanatı Alman Shankler 1862-1890: https://www.ssa.gov/history/35act.html#TITLE%20VII

State.gov. (2024, 07 26). *www.state.gov*. Retrieved from Yapay Zeka ve İnsan Hakları için Risk Yönetimi Profili: https://www.state.gov/risk-management-profile-for-ai-and-human-rights/

State-gov. (2024, 12 24). *https://www-state-gov*. Retrieved from ABD Yapay Zeka Politikası Kaynakları ve Bağlantıları -ABD'de Yapay Zeka Araştırma ve Geliştirme Ulusal Stratejik Planı: https://www-state-gov.translate.goog/artificial-intelligence/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=en-US&_x_tr_pto=sc

Suncem Koçer, E. S. (2024, 02). *dergi.bilgi.edu.tr*. Retrieved from Makale Çağrısı: Yapay Zeka'nın Sosyal Hayata Etkileri: https://dergi.bilgi.edu.tr/index.php/reflektif/announcement/view/25

Uidai.gov. (2024, 01 04). *uidai.gov.in*. Retrieved from My-Aadhaar: https://uidai.gov.in/ur/my-aadhaar-ur/about-your-aadhaar-ur.html

Undocs.org. (2024, 09 20). *https://undocs.org*. Retrieved from Gelecek Paktı: https://undocs.org/Home/Mobile?FinalSymbol=A%2F79%2FL.2&Language=E&DeviceType=Desktop&LangRequested=False

Undp.org. (2006, 09 20). *www.undp.org*. Retrieved from İnsani Güvenlik Çerçevesi Ve Ulusal İnsani Gelişme Raporları Tematik Rehberlik Not 2006: https://www.undp.org/tr/turkiye/publications/2006-kuresel-insani-gelisme-raporu

Undp.org. (2006, 09 21). *www.undp.org*. Retrieved from İnsani Güvenlik Çerçevesi Ve Ulusal İnsani Gelişme Raporları Tematik Rehberlik Notu: https://www.undp.org/tr/turkiye/publications/2006-kuresel-insani-gelisme-raporu

Varol, D. S. (2023, 09). *Sosyal Medyada Kişisel Verilerin Korunması Sorunu*. Retrieved from tez.yok.gov.tr: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Wolford, B. w. (2024, 08 20). *https://gdpr.eu/what-is-gdpr*. Retrieved from AB'nin yeni veri koruma yasası GDPR nedir?: https://gdpr.eu/what-is-gdpr/