Yapay Zekâ Çağında Kişisel Veri Mahremiyeti

Hüseyin Ensari Eryılmaz

https://orcid.org/0009-0007-0744-7496 | h-ensari@outlook.com

Doktora Öğrencisi, Dokuz Eylül Üniversitesi, İzmir, Türkiye

Öz

Yapay Zekâ (YZ), 1950'li yıllarda Alan Turing'in "Makineler Düşünebilir mi?" sorusu ile gündemimize girmiş, son dönemde yapılan insansı makine tasarımlarında ciddi başarılara ulaşılmıştır. YZ'nın gelişimi büyük veri ile büyük veri de daha fazla kişisel verinin toplanması ile yakından ilişkilidir. Bu durum özellikle felsefi alanda özgürlük tartışmalarının arttığı, bireye vurgunun ön plana çıktığı günümüzde bireyler açısından oldukça önemli olan kişisel veri mahremiyeti ile ilgili birçok problemi de beraberinde getirmektedir. Veri mahremiyeti ile ilgili ulusal ve uluslararası birçok yasal düzenlemeye sahip olsak da ilgili teknolojilerin geliştirilme süreçlerini denetleyen bir düzenleme bulunmamaktadır. YZ sahip olduğu teknik yeterlilikler açısından genellikle "Dar Yapay Zekâ", "Genel Yapay Zekâ" ve "Süper Zekâ" olarak sınıflandırılmaktadır. Felsefede büyük ilgi gören YZ, mantıktan estetiğe, hukuktan etiğe ve hatta tıptan sanata disiplinlerarası birçok yeni araştırma alanını da beraberinde getirmektedir. Yeni gelişen teknolojiler karşısında, felsefenin yeni bir araştırma dizisi doğurması da kaçınılmaz gözükmektedir. Bildirimizde YZ'ya dair bu üç kavramı, bu kavramın mahremiyet kavramı ile olan ilişkisini, kişisel mahremiyet alanlarımıza dair oluşan ve oluşabilecek riskleri ve bu riskleri azaltmak için yapılması gerekenleri inceledik. Çalışmamızda literatür taraması yaparak nitel veri analizi yöntemini kullandık. Yaptığımız araştırmalarda, mahremiyet kavramının, genellikle teknolojik gelişmelerle ilgili kişisel verilerin güvenliğinin sağlanması ve bireylerdeki mahremiyet algısının değişimiyle ilgili olduğunu tespit ettik. Ancak bu çalışmaların mevcut gelişmeleri kapsamadığını gördük. Bildirimizde şu sorulara cevap vermeye çalıştık: "YZ, Dar YZ, Genel YZ, Süper Zekâ ve Kişisel Veri Mahremiyeti" kavramları ile ne kastedilmektedir? YZ kavramları ve kişisel veri mahremiyeti ilişkisiyle ilgili çalışmalar yapılmış mıdır? Kişisel veri mahremiyeti ile ilgili riskler nelerdir? Bu riskler nasıl azaltılabilir? Bildirimizin amacı, bu alanda çalışan bilim insanlarının son dönemde daha yüksek sesle ifade etmeye başladıkları YZ geliştirme süreçlerindeki riskleri belirtmek; kişisel mahremiyet içeren verilerin, bulut teknolojisinde bizden habersiz veya farkında olmadan verdiğimiz izinlerle toplanması ve depolanması; bu verilerin YZ'nın eğitiminde kullanılması durumunda ortaya çıkacak problemleri ve bu sorunları azaltmak için gerçekleştirilebilecek çözüm önerilerini tartışmaktır. Bu kapsamdaki son gelişmelere sosyal bilimcilerin dikkatini çekmek, bu alanla ilgili gelişmelerden haberdar etmek büyük önem arz etmektedir. Yaptığımız incelemeler ve analizler sonucunda yeni yeterlilikler kazanan YZ'nın, etkilediği alanlarla ilgili çalışmaların interdisipliner bir bakış açısıyla ele alınması gerektiği, bu alandaki çalışmaların sadece mühendislere bırakılmasının yakın gelecekte pek çok problemi beraberinde getireceği tespit edilmiştir. Hayatımızın her anını kapsayan akıllı makinelere karşı mahremiyet alanlarımızın muhafazasının oldukça zor olduğu, yaşanabilecek problemleri azaltmak için bireysel bilinçlenmenin önemi, YZ

geliştirme süreçleri ile ilgili yasal düzenlemelerin gerçekleştirilmesi gerektiği, problemi çıkaran YZ teknolojilerinin aynı zamanda çözümün de bir parçası kılınabileceği sonucuna ulaşılmıştır.

Anahtar Kelimeler

Felsefe, Teknoloji, Mahremiyet, Kişisel Veri, Yapay Zekâ, Süper Zekâ.

Etik Beyan	Bu çalışma, Türkiye Sosyal Bilimler Sempozyumu'nda sunulan "Yapay Zekâ Çağında Kişisel Veri Mahremiyeti" adlı tebliğin özetidir.
Türü	Bildiri Özeti
Geliş Tarihi	26.07.2023
Kabul Tarihi	07.08.2023
Yayım Tarihi	09.08.2023
Kategori	Sanat ve Beşeri Bilimler, Felsefe, Mantık
Araştırma Alanı	Felsefe, Mantık
Sempozyum	:
Adı	3. Türkiye Sosyal Bilimler Sempzyumu
Web	https://sempozyum.okuokut.org/index.php/tsbs/article/view/539
Yer ve Tarih	Çevrim İçi - 26-31 Ağustos 2023
Sponsor	Ankara Yıldırım Beyazıt Üniversitesi; Oku Okut Derneği
Bildiri Oturum Bilgisi	1. Oturum - 26 Ağustos 2023 Cumartesi 14:00 - 15:00
Telif Hakkı	© 2023 Hüseyin Ensari Eryılmaz. Yazar telif hakkını elinde tutarak yayımcıya uygun lisans ile yayım izni vermiştir.
Lisans	
Yayımcı	Oku Okut Yayınları
Kaynak Gösterimi	Eryılmaz, Hüseyin Ensari. "Yapay Zekâ Çağında Kişisel Veri Mahremiyeti". *3. Türkiye Sosyal Bilimler Sempozyumu Bildiri Özetleri Kitabı*. ed. Abdullah Demir. 17-20. Ankara: Oku Okut Yayınları, 2023. https://doi.org/10.55709/okuokutpress.54

Personal Data Privacy in the Age of Artificial Intelligence

Hüseyin Ensari Eryılmaz

https://orcid.org/0009-0007-0744-7496 | h-ensari@outlook.com
Ph.D. Student, Dokuz Eylül University, İzmir, Türkiye

Abstract

The article discusses the relationship between Artificial Intelligence (AI) and personal data privacy. Artificial Intelligence which emerged in the 1950s with Alan Turing's question "Can Machines Think?" has achieved significant successes in recent years, particularly in the development of human-like machine designs. The advancement of AI is closely related to the collection of big data, which in turn involves gathering more personal data. In today's context, marked by increased philosophical discussions about freedom and heightened emphasis on the individual, the issue of personal data privacy has become considerably important, accompanied by numerous challenges. Despite the existence of many national and international legal regulations regarding data privacy, there lacks a regulation overseeing the development processes of related technologies. Artificial Intelligence is often classified into categories based on its technical capabilities, namely "Narrow AI," "General AI," and "Superintelligence." AI has attracted significant attention in philosophy and has brought about interdisciplinary research in fields ranging from logic and aesthetics to law, ethics, medicine, and even art. In the face of emerging technologies, it seems inevitable that philosophy will initiate new research trajectories. The paper examines these three concepts related to AI, their connection with the concept of privacy, the issues arising and potentially arising in the realm of personal privacy, and the measures to mitigate these risks. The methodology employed includes a literature review and qualitative data analysis. The research reveals that the notion of privacy is mainly linked to ensuring the security of personal data related to technological advancements and the changing perception of privacy in individuals. However, it's observed that these studies often do not encompass current developments. The paper endeavors to answer questions such as: What do the terms "AI, Narrow AI, General AI, Superintelligence, and Personal Data Privacy" refer to? Have studies been conducted on the relationship between AI concepts and personal data privacy? What are the risks associated with personal data privacy, and how can these risks be mitigated? The study aims to highlight the risks in the development processes of AI as increasingly vocalized by scientists working in this field. It delves into issues such as the collection and storage of personal data, often unbeknownst to individuals, through cloud technologies and the potential problems arising from the use of this data in AI training. The article also discusses potential solutions to these issues. Drawing attention to recent developments in this scope is of paramount importance for social scientists, and disseminating information about these advancements is crucial. Based on the examinations and analyses conducted, it's determined that AI, now possessing new competencies, requires an interdisciplinary approach to address the areas it influences. It's found that leaving this field solely to engineers would result in numerous problems in the near future. Safeguarding privacy in the face of intelligent machines that

encompass every aspect of our lives is a formidable challenge. Reducing potential problems necessitates individual awareness, legal regulations concerning AI development processes, and recognizing that AI technologies causing issues can also be part of the solution.

Keywords

Philosophy, Technology, Privacy, Personal Data, Artificial Intelligence, Superintelligence.

Ethical Statement	This paper is a summary of the study titled "Personal Data Privacy in the Age of Artificial Intelligence" presented at the 3rd Turkish Symposium of Social Science.
Type	Conference Proceeding
Received	2023-07-26
Accepted	2023-08-07
Published	2023-08-09
Category	Art & Humanities, Philosophy, Logic
Research Area	Philosophy, Logic
Conference	:
Title	The 3rd Turkish Symposium of Social Sciences
Web	https://sempozyum.okuokut.org/index.php/tsbs/article/view/539
Location & Date	Online - August 26-31, 2023
Sponsor	Ankara Yıldırım Beyazıt University; Oku Okut Association
Proceeding Session	Session 1 - August 26, 2023, Saturday 14:00 - 15:00
Copyright	© 2023 Hüseyin Ensari Eryılmaz. The author retains the copyright and provides the publisher with a proper license to publish.
License	
Publisher	Oku Okut Press
Citation	Eryılmaz, Hüseyin Ensari. "Personal Data Privacy in the Age of Artificial Intelligence". *The 3rd Turkish Symposium of Social Sciences: The Book of Abstracts*. ed. Abdullah Demir. 17-20. Ankara: Oku Okut Press, 2023. https://doi.org/10.55709/okuokutpress.54