Chapter 3

Privacy and Artificial Intelligence

Engin Yavuz[1]

Abstract

The areas of use of artificial intelligence are constantly increasing. It has started to play a major role especially for brands to increase sales by influencing consumers. In an increasingly competitive environment, it is vital to reach more consumers and increase sales rates. Consumers prefer the option they find closer to themselves among brands due to easy access to products and services and the abundance of options. Therefore, the demand for personalized products and services is increasing day by day. Brands also need more information to offer personalized products to consumers. It is very difficult to access consumers' personal data and make meaningful inferences from them, especially with large amounts of data. Artificial intelligence makes the work of brands much easier at this point. Consumer data, most of which is collected on the internet, can be analyzed with artificial intelligence and meaningful information can be obtained. Recently, however, there have been some concerns about the collection and use of consumer data. Personal data may be improperly shared with third parties and may lead to legal problems. Artificial intelligence developers should ensure that personal data is collected and used in line with principles such as transparency, fairness, accountability, privacy and security. The establishment of an effective control system and the sanctions to be taken against violations should be clearly stated. Providing the necessary support from governments and ensuring global cooperation can contribute to the reduction of personal data breaches. In this section, within the scope of privacy and artificial intelligence, the definition of artificial intelligence, the privacy of consumers and artificial intelligence, the views of the European Data Protection Board on the use of personal data, the views of the OECD on the use of personal data, the Council of Europe's ethical principles on artificial intelligence are examined under the headings.

1 Dr. Amasya Üniversitesi, engin84yavuz@gmail.com, https://orcid.org/0000-0002-9644-4946

https://doi.org/10.58830/ozgur.pub710.c3020

Privacy and Artificial Intelligence

1. Introduction

In recent years, the number of consumer concerns about ethical issues in online shopping has continued to grow. Privacy and security are considered by consumers and researchers to be the most important ethical violations (Román and Cuestas 2008). The possibility of artificial intelligence violating privacy is increasing day by day. Although privacy is considered a fundamental right, it should be taken into account that artificial intelligence may lead to violations of privacy protection (Akyol and Özkan, 2023: 122).

Digital technology environments are being used more and more in daily life. However, it has become possible to talk about the privacy of private life with the data collected, archived, analyzed and interpreted as a result of artificial intelligence consisting of platforms, software, codes and algorithms (Wilson, 2016). With these developments, it can be considered that artificial intelligence prepares the ground for revealing personal freedoms and privacy (Gül, 2018: 20).

Technological developments bring about changes in daily life. Artificial intelligence, which is one of them, has risks affecting human rights as well as areas where it is beneficial. Especially in areas such as trade, communication and cybercrimes, malicious use is also possible. This situation prompts politicians, states and artificial intelligence developers to develop new strategies (Dost, 2023: 1275).

Having data, which is the basis of artificial intelligence, also brings power. In today's increasingly competitive environment, it is critical for both private sector organizations and governments to gain power. Therefore, governments and private organizations may want to access personal data as soon as possible and use it for their own interests. By capturing the personal data of the target audience, they can use it to market products and services in accordance with the wishes of consumers and to increase their sales. When this data is not used properly, it may mean a violation of consumers' privacy (Varkonyi, 2018: 3).

Artificial intelligence technologies can easily obtain sensitive personal data by processing data that is not considered sensitive. In other words, artificial intelligence technologies can cause violation of private life by converting non-sensitive data into sensitive data. Personal data can be extracted through social media platforms such as Facebook, Instagram, etc. and consumers' virtual identities can be captured. With this data, consumers' interests,

tendencies and expectations can be learned and used in commercial activities (Abudureyimu and Oğurlu, 2021: 771).

In this section, within the scope of privacy and artificial intelligence, the definition of artificial intelligence, the privacy of consumers and artificial intelligence, the views of the European Data Protection Board on the use of personal data, the views of the OECD on the use of personal data, the Council of Europe's ethical principles on artificial intelligence are examined under the headings.

2. Artificial Intelligence

There is not yet an agreed definition of artificial intelligence. However, according to the definition by the European Commission of Human Rights, artificial intelligence is "used as an umbrella term to refer to a set of sciences, theories and techniques dedicated to improving the ability of machines to do things that require intelligence. An artificial intelligence system is a machine-based system that produces recommendations, predictions or decisions for a given set of goals (European Commission of Human Rights, 2019)".

The concept of artificial intelligence should be characterized as an algorithm-supported artificial machine that can learn in a complex and variable field, make decisions, influence those around it, and transfer the information and decisions it obtains to users, that is, an entity with the ability to think (Gezici, 2023: 112).

If we define artificial intelligence briefly, it is a technology-based system that analyzes simultaneous product and service simulations using data obtained from both digital and physical channels and makes personalized recommendations to solve consumers' complex problems and answer their questions, enabling them to decide between options (Xu et al., 2020).

3. Consumer Privacy and Artificial Intelligence

Artificial intelligence uses algorithms to calculate the probabilities that are likely to occur using the data they obtain and tries to gain useful information as a result. For example, artificial intelligence algorithms are used extensively in areas such as tourism, logistics, retail and e-commerce to monitor competitors' prices and determine price policies accordingly, to determine consumer preferences and to analyze the data obtained (Öz, 2020: 40).

Artificial intelligence also makes extensive use of consumers' personalized data in shopping and entertainment. Amazon's purchase recommendations,

Netflix's efforts to direct the audience, prioritizing consumers in terms of content and making consumer-specific recommendations. At this point, consumers evaluate what to buy or not to buy, which product or service will be beneficial for them through artificial intelligence rather than individual thoughts (Eltimur, 2022: 578).

Artificial intelligence in marketing is frequently used in areas such as analyzing consumer behavior, consumer experience, providing personalized products and services, and managing consumer relationships quickly and effectively before, during and after sales. In consumer research, abilities such as understanding, speech and cognitive abilities are performed by the algorithms of artificial intelligence (Huang & Rust, 2022: 210).

With the increasing use of social media, people share their daily lives and experiences on these platforms. These shares are increasing day by day. Large amounts of data can reach many people simultaneously with the internet. Consumers' personal information, what they like and dislike, and their thoughts are very important for marketing practitioners. It becomes difficult to process large amounts of data into meaningful information. Artificial intelligence is one of the most effective ways to turn difficult into easy (Binbir, 2021: 315).

However, in addition to these benefits, artificial intelligence may use personal data improperly to increase consumer satisfaction. The information obtained through digital traces while browsing the internet and the advertisements developed through this information are just one of the many violations in the field of artificial intelligence. The large amount of data collected from consumers also raises issues related to their private lives. These problems are not only related to data management. In addition, directing consumer preferences and encouraging them to buy the products and services they want is one of the steps that restrict consumers' freedom. For example, with the consumer data obtained, artificial intelligence algorithms can identify certain consumers and manage their perceptions (Gonçalves et al., 2023: 315).

Aleksandr Kogan, a researcher at the University of Cambridge, collected users' personal data on Facebook without their consent and transmitted it to Cambridge Analytica. The personal data obtained targeted consumers through advertising. After the personal data breach was revealed, the company was shut down. In order to prevent this vulnerability, Facebook blocked Cambridge Analytica's access and launched an investigation into applications that similarly had access to personal data. It also restricted third-party developers from accessing personal profiles (The Guardian, 2018).

4. Various Organizations' Views on Privacy and Artificial Intelligence

Although obtaining personal data provides great advantages to brands, the use and sharing of data without taking the necessary privacy and security measures can harm consumers as well as brands (Danışman, 2023: 161). In this section, the views of the European Data Protection Board, the OECD and the Council of Europe on the use of personal data are given.

4.1. Opinions of the European Data Protection Board on the Use of Personal Data

On December 18, 2024, the European Data Protection Board (EDPB) issued an opinion on the use of personal data in the use of artificial intelligence. According to this opinion (European Data Protection Board, 2025):

1) When and how AI models will be considered anonymous:

Whether an AI model is anonymous or not depends on the decision of countries' data protection authorities and may need to be assessed on a case-by-case basis. For an AI model to be considered anonymous;

a) Direct or indirect identification of the persons whose data are used in the creation of the artificial intelligence model.

b) It is necessary to prevent personal data from being obtained from the artificial intelligence model through querying.

2) Procedures required to develop or use artificial intelligence models:

A representative should be provided by AI developers so that users can communicate when necessary and necessary measures should be taken to increase cyber security. These measures can be beneficial for users and provide legal protection, but only if the processing of personal data is truly necessary and personal rights are respected.

3) Unlawful development of artificial intelligence:

Unless artificial intelligence models are duly anonymized, the use of personal data may be unlawful.

4.2. OECD's Views on the Use of Personal Data

According to the report published by the OECD, there is a need for global coordination to solve the problems related to the data used by artificial intelligence. In this report, six issues are highlighted in order to harmonize the developments in the field of artificial intelligence with privacy principles (Maxwell, et. al., 2024). These are (Maxwell, et. al., 2024):

1) Privacy in the use of artificial intelligence

Complaints about privacy violations in the use of artificial intelligence are increasing and the measures to be taken to address this issue are important. Particular attention needs to be paid to privacy in the conceptualization, development and deployment phases of artificial intelligence actions. It is important to comply with privacy rules from the early stages of AI development and design, and to make proactive efforts to close gaps in implementation. Building bridges between societies, making privacy a permanent policy in AI development and supporting privacy-oriented innovation are among the critical issues (Shrestha and Joshi, 2025; Mooradian et. al, 2025; Maxwell, et. al., 2024).

2) Cooperation between communities

Terminological and conceptual misunderstandings in AI privacy and policies can lead to ambiguities. Therefore, it is important to build sustainable interactions between AI communities. In this way, terminological and conceptual harmonization between AI communities on privacy-related issues can be achieved and contribute to the development of AI (Welsh et al., 2024; Maxwell, et. al., 2024).

3) Justice

It is very important for AI models to process personal data fairly and reach conclusions in terms of privacy principles of AI. Principles such as limitation of data collection, purposefulness, openness and quality of data collected are critical to ensure fairness (Verma et al., 2024; Maxwell, et. al., 2024).

4) Transparency and accountability

Obtaining consent when processing individuals' data and informing them about how it is used is one of the most important issues in artificial intelligence development. As transparency increases, so does trust, making it easier for users to make informed decisions. Practical solutions such as model cards can be produced to ensure that the information provided by AI is understandable and meaningful (Cheong, 2024; Maxwell, et. al., 2024).

5) Accountability

It is also important to be able to integrate privacy and risk management principles into AI applications at the design stage and, as a result, to be accountable and comply with the laws of countries. Deep privacy detection programs to detect privacy can also help prevent breaches (Moch, 2024; Maxwell, et. al., 2024).

6) Global cooperation

Global synchronization, guidance and collaboration are needed to help AI mitigate privacy concerns. While there have been improvements in global collaboration, increased efforts can help prevent privacy violations. In addition, Privacy Enhancing Technologies (PETs) can bridge this gap to a large extent to help with data management and privacy safeguards (Al-Billeh et al., 2024; Maxwell, et. al., 2024).

4.3. Council of Europe Ethical Principles on Artificial Intelligence

According to the guidelines published by the Council of Europe in 2019, a trustworthy AI must meet the following 7 basic requirements (European Comission, 2019):

1) Oversight of human activities:

AI should empower individuals and support them in decision-making. In addition, it is important that artificial intelligence systems are controllable.

2) Technical infrastructure and security:

Artificial intelligence systems need to be strong and stable in terms of infrastructure. It is also critical to prevent security breaches.

3) Privacy and data management:

Artificial intelligence systems should provide legitimate access to data and pay due attention to its quality and confidentiality.

4) Transparency:

Artificial intelligence applications should follow a transparent management policy. Users should be informed about whether they are interacting or not. In addition, users should be informed about the capabilities and limitations of artificial intelligence applications.

5) Fairness:

AI models should treat users equally and fairly. It should be ensured that all users can access AI models without any discrimination.

6) Social contribution:

Artificial intelligence models should benefit all of humanity, with future generations in mind. They should also be respectful of the environment and take care to provide social benefits.

7) Responsibility:

Mechanisms are needed for artificial intelligence applications to fulfill their responsibilities and to be accountable within the framework of these responsibilities. it is also important that the design processes of the data can be audited.

Sonuç

Artificial intelligence has been used extensively in marketing in recent years. Due to increased competition, businesses want to increase their market share or at least maintain their status. Consumers have many options when making purchasing decisions. Considering that consumers want to choose the brands that provide the most suitable personalized products/services with the increase in their alternatives, businesses may have to benefit from artificial intelligence in order to fulfill the wishes of consumers. Artificial intelligence can collect consumer data, analyze it, and then make it available to marketing practitioners. Collecting, analyzing and transforming consumer data into useful information is a complex and difficult process that can only be accomplished through AI-enabled applications with current technology (Neves and Pereira, 2025).

Artificial intelligence applications should pay attention to legal regulations when obtaining consumer data and take the necessary measures for the use of personal data. When collecting personal data, it should be transparently explained to consumers what data is collected and for what purpose. Businesses should not ignore the principle of transparency in order to gain the trust of consumers. In addition to affecting consumer trust, breach of personal data may put businesses in a difficult situation in front of the law. Therefore, businesses that follow an artificial intelligence-supported marketing strategy should pay close attention to the security of personal data and the privacy of private life (Kır, 2024: 71).

Artificial intelligence applications used by businesses must fulfill ethical and legal responsibilities when collecting personal data from consumers. Inappropriate collection of personal data and sharing it with third parties without permission may lead to personal data breach and may result in legal sanctions. Ensuring global cooperation and the necessary sanctions by states by taking measures against personal data breach can prevent the improper collection of personal data breach. In addition, artificial intelligence developers should have the ability to communicate with consumers when necessary and build infrastructure systems to prevent the improper collection of personal data (Muvva, 2025).

Kaynakça

Abudureyimu, Y. ve Oğurlu, Y. (2021). Yapay zekâ uygulamalarının kişisel verilerin korumasına dair doğurabileceği sorunlar ve çözüm önerileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 20(41), 765-782, doi:10.46928/iticusbe.863505

Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., & Makhmari, M. (2024). The risks of using artificial ıntelligence on privacy and human rights: unifying global standards. *Jurnal Media Hukum*, *31*(2), 333–350. https://doi.org/10.18196/jmh.v31i2.23480

Akyol, İ.T. ve Özkan, N.A.Ş. (2023). Yapay zeka uygulamalarinin yerel hizmet sunumuna etkisi, *Tokat Gaziosmanpaşa Üniversitesi Sosyal Bilimler Araştırmaları Dergisi*, 120-134.

Avrupa İnsan Hakları Komisyonu. (2019). Unboxing artificial intelligence: 10 steps to protect human rights, Erişim Adresi: chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/unboxing-artificial intelligence-10-steps-to-protect-human-rights-reco/1680946e64 Erişim Tarihi: 16.02.2025

Binbir, S. (2021). Pazarlama çalışmalarında yapay zeka kullanımı üzerine betimleyici bir çalışma, *Yeni Medya Elektronik Dergisi*, 5(3), 314-328.

Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, *6*. https://doi.org/10.3389/fhumd.2024.1421273

Danışman, G.T. (2023). Artificial Intelligence in Terms of Digital Marketing: A Conceptual Examination. In: Fettahlıoğlu, H. S. & Bilginer Ozsaatcı, F. G. (eds.), *Digital Transformation of Marketing: Marketing 5.0*. Özgür Publications. DOI: https://doi.org/10.58830/ozgur.pub254.c1340

Dost, S. (2023). Yapay zekâ ve uluslararası hukukun geleceği' 13(2) *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 1271, 1313.

Eltimur, D.E. (2022). İnsan haklarının korunması bağlamında yapay zekâ uygulamaları, *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 12(2), 559-594.

European Comission. (2019). Ethics guidelines for trustworthy AI, Erişim Adresi: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, Erişim Tarihi: 18.02.2025

European Data Protection Board. (2025). Erişim Adresi: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en, Erişim Tarihi: 20.02.2025

Gezici, H.S. (2023). Kamu yönetiminde yapay zekâ: Avrupa Birliği, *Uluslararası Akademik Birikim Dergisi,* 6(2), 111-128.

Gonçalves, A. R., Pinto, D. C., Rita, P. ve Pires, T. (2023). Artificial Intelligence and its ethical implications for marketing, *Emerging Science Journal*, 7(2), 313-327. doi: 10.28991/ESJ-2023-07-02-01

Gül, H. (2018), Dijitalleşmenin kamu yönetimi ve politikaları ile bu alanlardaki araştırmalara etkileri, *Yasama Dergisi*, 36, 5-26.

Huang, M.H. ve Rust, R.T. (2022). A framework for collaborative artificial intelligence in marketing. *Journal of Retailing*, 98(2), 209–223.

Kır, B. (2024). AI Pazarlama: Yeni Bir Paradigma, (Ed. M. Nur Erdem, Cansu Maya), Marka İletişimi Tüm Boyutlarıyla Marka ve Tüketici Etkileşimi (içinde), Palet Yayınları: Konya

Öz, G.A. (2020). Corona (Covid 19) gölgesinde geleceğin hukuku ve dijital ekonomi çağında rekabet hukuku, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 69 (1), 33-56.

Shrestha, A. K., & Joshi, S. (2025). Toward Ethical AI: A Qualitative Analysis of Stakeholder Perspectives. https://doi.org/10.48550/arxiv.2501.13320

Maxwell, W., Girot, C. ve Perset, K. (2024). Six crucial policy considerations for AI, data governance, and privacy: Insights from the OECD, Erişim Adresi: https://oecd.ai/en/wonk/six-policy-considerations-ai-data-governance-and-privacy, Erişim Tarihi: 19.02.2025

Moch, E. (2024). Liability Issues in the Context of Artificial Intelligence: Legal Challenges and Solutions for AI-Supported Decisions. *East African Journal of Law and Ethics*, *7*(1), 214–234. https://doi.org/10.37284/eajle.7.1.2518

Mooradian, N., Franks, P. C., & Srivastav, A. (2025). The impact of artificial intelligence on data privacy: a risk management perspective. *Records Management Journal*. https://doi.org/10.1108/rmj-06-2024-0013

Muvva, S. (2025). Ethical AI and responsible data engineering: A framework for bias mitigation and privacy preservation in large-scale data pipelines. *Indian Scientific Journal of Research In Engineering and Management*, 09(01), 1–8. https://doi.org/10.55041/ijsrem10633

Neves, J. ve Pereira, M. C. (2025). A marketing perspective on the roles of AI and ML in shaping contemporary programmatic advertising. *International Journal of Digital Marketing, Management, and Innovation* (IJDMMI), 1(1), 1-14. https://doi.org/10.4018/IJDMMI.368043

Román, S., Cuestas, P., 2008. The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general Internet expertise and word of mouth: a preliminary analysis. *Journal of Business Ethics,* 83, 641–656.

The Guardian. (2018). Cambridge Analytica closing after Facebook data harvesting scandal, Erişim Adresi: https://www.theguardian.com/

uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say, Erişim Tarihi: 15.02.2025.

Xu, Y., Shieh, C., Van Esch, P. ve Ling, I. (2020). AI customer service: Task complexity, problem-solving ability, and usage intention, *Australasian Marketing Journal*, 28(4), 189-199.DOI:10.1016/j.ausmj.2020.03.005

Varkonyi, G.G. (2018). Robots with AI: Privacy considerations in the era of robotics. Law 4.0 1-12, Györ: Széchenyi István University, Erişim Adresi: https://www.academia.edu/36293091/Robots_with_AI_Privacy_Considerations_in_the_Era_of_Robotics Erişim Tarihi: 17.02.2025.

Verma, S., Paliwal, N., Yadav, K., & Vashist, P. C. (2024). *Ethical Considerations of Bias and Fairness in AI Models*, 2nd International Conference on Disruptive Technologies (ICDT), 818–823. https://doi.org/10.1109/icdt61202.2024.10489577

Welsh, C., Román García, S., Barnett, G. C., & Jena, R. (2024). Democratising artificial intelligence in healthcare: community-driven approaches for ethical solutions. *Future Healthcare Journal*, *11*(3), 100165. https://doi.org/10.1016/j.fhj.2024.100165

Willson, M. (2016). Algorithms (and the) Everyday, Information, Communication & Society.