Right to Privacy in Artificial Intelligence Legislations: Analyzing International Soft Law Frameworks(*)

Yapay Zeka Mevzuatında Mahremiyet Hakkı: Uluslararası Yumuşak Hukuk Çerçevelerinin Analizi

ASM Mahmudul HASAN(**)

Abstract:

The article examines the evolving intersection of privacy rights and artificial intelligence (AI) governance, focusing on the role of international soft law frameworks in shaping privacy protections. Recognizing privacy as a fundamental human right enshrined in various global and regional legal instruments, the study highlights its critical dimensions in the context of emerging AI technologies, which pose unique challenges and opportunities for data governance. The methodology includes an analytical review of significant legislative and policy frameworks, such as the European Union Artificial Intelligence Act, UN General Assembly Resolutions on AI and cybercrime, the UN Global Digital Compact, and the Council of Europe Draft Framework Convention on Artificial Intelligence. These frameworks are assessed for their principles and mechanisms aimed at embedding privacy protections throughout AI systems, emphasizing transparency, accountability, fairness, and international collaboration. Findings indicate growing integration of privacy considerations in AI governance through measures like privacy-by-design, risk management, and restrictions on mass surveillance and untargeted data scraping. Key provisions include robust data governance, transparency requirements, safeguards against discriminatory outcomes, and harmonized privacy standards via international cooperation. The study concludes that international soft law frameworks provide a crucial foundation for embedding privacy protections into AI systems, reflecting a global consensus on safeguarding this right amid technological advances. By harmonizing principles across jurisdictions, fostering multi-stakeholder engagement, and promoting ethical AI development, these initiatives support a human-centric approach to AI governance. The research offers insights for international policymakers to align AI innovation with fundamental rights.

Keywords:

Right To Privacy, UN, EU, Artificial Intelligence, International Soft Law.

(*) Araştırma Makalesi / *Research Article*
Yayın Kuruluna Ulaştığı Tarih: 20.01.2025
Yayınlanmasının Kabul Edildiği Tarih: 28.08.2025
DOI: 10.58733/imhfd.1624022
Bu makaleye atıf için; HASAN, ASM Mahmudul, "Right to Privacy in Artificial Intelligence Legislations: Analyzing International Soft Law Frameworks", **İMHFD**, C. 10, S. 2, 2025, s. 995-1024

(**) *Dr. Öğr. Üyesi*, Karabük Üniversitesi, Uluslararası İlişkiler Bölümü, Uluslararası Hukuk Anabilim Dalı, Karabük - Türkiye
E-posta: abusalehhasan@karabuk.edu.tr
Orcid: 0000-0001-8833-5101

Öz:

Bu makale, mahremiyet hakları ile yapay zeka (YZ) yönetişiminin gelişen kesişimini inceleyerek, uluslararası yumuşak hukuk çerçevelerinin mahremiyet korumalarını şekillendirmedeki rolüne odaklanmaktadır. Mahremiyetin, çeşitli küresel ve bölgesel hukuki belgelerde güvence altına alınmış temel bir insan hakkı olarak tanınması bağlamında çalışma, yükselen YZ teknolojilerinin veri yönetişimi için ortaya çıkardığı özgün zorluklar ve fırsatlar üzerindeki kritik boyutlarını vurgulamaktadır. Yöntem, Avrupa Birliği Yapay Zeka Yasası, BM Genel Kurulu'nun YZ ve siber suç konulu kararları, BM Küresel Dijital Mutabakatı ve Avrupa Konseyi Yapay Zeka Taslak Çerçeve Sözleşmesi gibi önemli yasal ve politik çerçevelerin analitik bir incelemesini içermektedir. Bu çerçeveler, YZ sistemleri boyunca mahremiyet korumalarını yerleştirmeyi amaçlayan şeffaflık, hesap verebilirlik, adalet ve uluslararası iş birliğine vurgu yaparak, prensipleri ve mekanizmaları açısından değerlendirilmektedir. Bulgular, mahremiyet odaklı tasarım, risk yönetimi, kitlesel gözetim ve hedefsiz veri kazıma üzerindeki kısıtlamalar gibi önlemler yoluyla YZ yönetişiminde mahremiyet hususlarının artan entegrasyonunu ortaya koymaktadır. Önemli hükümler arasında güçlü veri yönetişimi, şeffaflık gereklilikleri, ayrımcılığa karşı koruma mekanizmaları ve uluslararası iş birliği yoluyla uyumlu mahremiyet standartları yer almaktadır. Çalışma, uluslararası yumuşak hukuk çerçevelerinin, teknolojik ilerlemeler karşısında bu hakkı koruma yönünde küresel bir uzlaşıyı yansıtarak, YZ sistemlerinde mahremiyet korumalarının yerleşik hale getirilmesi için önemli bir temel sağladığı sonucuna varmaktadır. Yargı bölgeleri arasında prensiplerin uyumlaştırılması, çok paydaşlı katılımın teşvik edilmesi ve etik YZ geliştirilmesinin desteklenmesi yoluyla bu girişimler, insan odaklı bir YZ yönetişimi yaklaşımını desteklemektedir. Araştırma, uluslararası politika yapıcılar için YZ yeniliklerini temel haklarla uyumlu hale getirme konusunda içgörüler sunmaktadır.

Anahtar Kelimeler:

Mahremiyet Hakkı, BM, AB, Yapay Zeka, Uluslararası Yumuşak Hukuk.

INTRODUCTION

The rapid proliferation of artificial intelligence (AI) technologies has fundamentally reshaped the landscape of data governance, raising profound ethical, legal, and societal questions. Among these, the right to privacy emerges as a cornerstone of contemporary debates, particularly given its universal recognition as a fundamental human right enshrined in numerous international and regional legal instruments. As AI technologies evolve, the interplay between innovation and individual rights intensifies, necessitating robust governance frameworks that can effectively balance technological advancement with the protection of privacy.

The right to privacy, characterized by its multidimensionality, encompasses concepts such as data protection, informational autonomy, and freedom from unwarranted intrusion. This right is increasingly tested by AI systems that often operate on vast amounts of personal data, employing sophisticated algorithms capable of deriving insights about individuals. Such capabilities, while driving innovation, also present significant risks of surveillance, discrimination, and erosion of individual autonomy[1]. As a result, the governance of AI demands proactive measures to embed privacy considerations throughout the lifecycle of these systems.

International soft law frameworks have emerged as pivotal mechanisms for addressing privacy challenges in AI governance. These non-binding legal instruments, including guidelines, resolutions, and policy frameworks, offer a flexible yet principled approach to harmonizing global standards. Luciano Floridi introduces the concept of 'soft ethics,' arguing that flexible ethical guidelines must complement soft law initiatives to ensure that AI systems respect human rights, including privacy, from design to deployment[2]. By fostering international collaboration, promoting ethical AI practices, and emphasizing principles like transparency, accountability, and fairness, these frameworks provide a foundational structure for safeguarding privacy rights in the AI era.

This study examines seven major international soft law initiatives relating to artificial intelligence governance and privacy protections. These include the UN Global Digital Compact, the United Nations General Assembly Resolution 79/243: United Nations Convention Against Cybercrime, the OECD Initial Pol-

1 HAYES, Paul; POEL, Ibo van de; STEEN, Marc, "Algorithms and Values in Justice and Security", **AI & Society**, Y. 2020, V. 35, No. 3, p. 534.

2 FLORIDI, Luciano, "Soft Ethics and the Governance of Artificial Intelligence", **Philosophy & Technology**, Y. 2018, V. 31, pp. 1-8.

icy Considerations for Generative Artificial Intelligence, the Council of Europe Draft Framework Convention on Artificial Intelligence, the European Union Artificial Intelligence Act, and the OAS Inter-American Guidelines on Data Governance and Artificial Intelligence. By analyzing these instruments comparatively, this study highlights how international organizations are converging - and at times diverging - in their efforts to integrate privacy safeguards into the global AI governance landscape. These instruments are examined for their contributions to embedding privacy protections into AI systems, highlighting mechanisms like privacy-by-design, risk management, and data governance. The analysis further explores the broader implications of these frameworks for aligning AI innovation with fundamental human rights, emphasizing the need for sustained efforts to ensure a human-centric approach to AI development.

In this context, the present research aims to contribute to the growing discourse on privacy and AI governance by elucidating the role of international soft law frameworks in advancing privacy protections. It underscores the importance of harmonizing principles across jurisdictions and fostering multi-stakeholder engagement to create a global consensus on ethical AI practices. Through this analysis, the study seeks to offer valuable insights for policymakers, researchers, and practitioners striving to uphold privacy rights in an increasingly data-driven world.

The analysis in this study follows an organization-based structure, examining international soft law frameworks in groups according to the institutions that produced them. United Nations initiatives are discussed first, followed by frameworks developed by intergovernmental organizations such as the OECD and the Council of Europe, and finally regional instruments such as those of the European Union and the Organization of American States. This institutional ordering provides clarity and highlights differences in regulatory approaches across international bodies.

In light of these objectives and the increasing global convergence on embedding privacy safeguards into AI systems, this study seeks to answer the following research question: How do international soft law frameworks embed and promote the right to privacy in the governance of artificial intelligence systems across global and regional jurisdictions? This guiding question allows for a comparative and critical examination of soft law instruments, focusing on their legal, ethical, and operational dimensions. It anchors the study's inquiry into the adequacy, effectiveness, and normative orientation of international policy responses to the privacy challenges posed by AI technologies, providing a structured basis for evaluating their human rights alignment.

I. THEORETICAL FRAMEWORK

This research adopts a Human Rights-Based Approach (HRBA) to analyze the intersection of privacy rights and artificial intelligence governance. The Human Rights-Based Approach emphasizes that technological innovation must be aligned with fundamental human rights, treating privacy not merely as a regulatory requirement but as an essential dimension of human dignity, autonomy, and freedom. A relevant example can be found in the United Kingdom, where the Human Rights Act 1998 operationalizes the European Convention on Human Rights within the domestic legal system, illustrating how international commitments are embedded at the national level while balancing parliamentary sovereignty and judicial oversight[3]. Under this framework, privacy protections are viewed as prerequisites for ensuring that AI systems do not undermine individual rights through surveillance, discrimination, or undue manipulation.

By using the HRBA, the study critically examines international soft law frameworks to assess whether they sufficiently safeguard privacy across the AI system lifecycle. The analysis particularly focuses on whether these frameworks embed privacy principles such as transparency, accountability, fairness, and risk management into the design, development, and deployment of AI technologies. This theoretical orientation ensures that the evaluation remains centered on human-centric governance and ethical AI development, rather than purely technical or economic considerations[4].

A. Key Concepts: Accountability And Transparency

In the governance of artificial intelligence systems, accountability and transparency function as foundational principles for safeguarding fundamental rights, particularly the right to privacy. Accountability requires that those who design, develop, and deploy AI systems accept responsibility for their systems' functioning and potential impacts. This principle encompasses mechanisms of oversight, monitoring, and redress to ensure that AI actors remain answerable for outcomes throughout the system's lifecycle. As articulated in the OECD Principles on Artificial Intelligence, accountability demands that "AI actors are

---

3 GILANI, Syed Raza Shah, Ali Mohammed ALMATROOSHI, and Ali Fayyaz AWAN, "An In-Depth Analysis of the Human Rights Act of 1998 and the Bill of Human Rights UK, Examining the Advantages and Disadvantages", **Current Trends in Law and Society**, Y. 2024, V. 4, No. 1, pp. 121-129.

4 UNITED NATIONS SUSTAINABLE DEVELOPMENT GROUP, **The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding among UN Agencies**, 2003, p. 1-4, https://unsdg.un.org/resources/human-rights-based-approach-development-cooperation-towards-common-understanding-among-un, A.D. 18.12.2024.

responsible for the proper functioning of AI systems in line with their roles, the context, and the state of the art[5]".

Transparency complements accountability by requiring that AI systems operate in a manner that is understandable, traceable, and explainable to relevant stakeholders. It extends beyond the mere disclosure of technical details, emphasizing the need for information to be communicated in a meaningful and accessible way to regulators, users, and those affected. Wachter, Mittelstadt, and Floridi note that transparency is a prerequisite for effective contestability and trust, enabling oversight and informed evaluation of AI systems[6]. In this study, these two concepts serve as analytical criteria for assessing whether international soft law frameworks embed sufficient safeguards to ensure that privacy protections are both operational and enforceable.

II. METHODOLOGY

This study employs a qualitative analytical methodology, grounded in a Human Rights-Based Approach. The analysis focuses on major international soft law frameworks that address artificial intelligence governance and the protection of privacy rights.

The selection of frameworks was based on the following criteria: (i) the framework's international or regional significance; (ii) its explicit focus on privacy rights in relation to AI systems; and (iii) its normative influence on shaping global digital governance practices.

Accordingly, the study analyzes instruments such as the European Union Artificial Intelligence Act, the United Nations General Assembly Resolutions on AI and cybercrime, the UN Global Digital Compact, the Council of Europe Draft Framework Convention on Artificial Intelligence, the OECD Initial Policy Considerations for Generative Artificial Intelligence, and the OAS Inter-American Guidelines on Data Governance and Artificial Intelligence.

The research adopts a comparative analytical approach, examining each framework in terms of:

---

[5] OECD, **OECD Principles on Artificial Intelligence**, OECD Publishing, Paris, 2019, https://www.oecd.org/en/topics/sub-issues/ai-principles.html, A.D. 05.08.2025.

[6] WACHTER, Sandra, Brent MITTELSTADT, and Luciano FLORIDI, "Transparent, Explainable, and Accountable AI for Robotics", **Science and Engineering Ethics**, Vol. 26, No. 4, 2020, pp. 2053-71.

- How it integrates privacy protections (privacy-by-design, data minimization, accountability, etc.),
- How it addresses risks associated with AI and personal data,
- How it balances innovation and the right to privacy.

By applying this structured analysis, the study evaluates the extent to which international soft law frameworks embed robust privacy safeguards into AI governance structures. Primary sources, such as legal texts and international resolutions, are analyzed alongside secondary sources, including academic literature, to ensure a comprehensive and critical evaluation.

The methodology also involves critical reflection on the theoretical and practical implications of privacy protection mechanisms, assessing their sufficiency in the context of evolving AI technologies.

In order to facilitate a structured comparative analysis, Figure 1 summarizes how each international soft law framework embeds key privacy principles. These dimensions - including privacy-by-design, risk management, transparency, and legal oversight - serve as the foundation for the subsequent detailed evaluation of each instrument.

Comparative Analysis of Privacy Provisions in AI Soft Law Frameworks

Framework	Privacy-by-Design	Risk Management	Transparency	Legal Oversight	Unique Focus
UN Global Digital Compact	Yes	Yes	Yes	Moderate	Cross-border data trust
OECD GenAI Guidelines	Yes	Yes	Yes	Strong	Generative AI risks
CoE Draft Convention	Yes	Yes	Yes	Strong	Procedural safeguards
EU AI Act	Yes	Yes	Yes	Strong	Biometric data protection
OAS Guidelines	Yes	Partial	Yes	Moderate	Latin American context
UNGA Cybercrime Conventio	Partial	Yes	Yes	Strong	Criminal enforcement

Figure 1. Comparative Analysis of Privacy Provisions in AI Soft Law Frameworks. Created by the Author.

III. THE RIGHT TO PRIVACY

The right to privacy is a fundamental human right recognized and protected by various legal frameworks worldwide. The European Convention on Human Rights, for instance, safeguards the right to respect for private life, home, and

correspondence, which encompasses the protection of personal communications such as messages, phone calls, and emails[7]. However, governmental interference in these rights is permitted only under strict legal conditions and when justified by significant reasons, such as ensuring national security or public safety[8].

Privacy, as a concept, is multifaceted and often challenging to define. Samuel Warren and Louis Brandeis famously articulated it as "the right to be let alone," a notion that has since evolved to encompass broader concerns in the modern era[9]. Privacy today is understood not only as seclusion or anonymity but also as control over personal information and the ability to limit access to one's personal sphere. Ruth Gavison identifies key components of privacy-anonymity, solitude, and secrecy-while Helen Nissenbaum emphasizes the dynamic nature of privacy, contingent on purpose, context, and trust[10]. Alan Westin adds a further dimension, identifying privacy's social, personal, and regulatory aspects[11]. Daniel J. Solove further emphasizes that privacy today must be understood as a complex network of protections, not merely as the right to secrecy but as control over personal information and autonomy in decision-making[12].

D. W. Prosser's seminal work in 1960 provided a legal taxonomy of privacy, categorizing it into four torts: intrusion upon seclusion, public disclosure of private facts, portrayal in a false light, and appropriation of name or likeness for personal gain. These categories underline privacy's broad relevance across legal, social, and ethical domains. In the digital age, this understanding has expanded to address the complexities of information control, data protection, and technological advancements[13].

Data protection, often regarded as a specific subset of privacy law, governs the collection, processing, and dissemination of personal information. It provides individuals with the right to access, correct, and control their data while

---

7 EUROPEAN CONVENTION ON HUMAN RIGHTS, "**Article 8**", Council of Europe, 1950, (Online), https://www.echr.coe.int, A.D. 20.01.2025.

8 ibid.; NYU LAW GLOBAL, "**Right to Privacy: An International Perspective**", (Online), https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html, A.D. 20.01.2025.

9 WARREN, Samuel D.; BRANDEIS, Louis D., "The Right to Privacy", **Harvard Law Review**, Y. 1890-1891, V. 4, No. 5, pp. 193-220.

10 GAVISON, Ruth, "Privacy and the Limits of Law", **The Yale Law Journal**, Y. 1980, V. 89(3), pp. 421-471.; NISSENBAUM, Helen, **Privacy in Context: Technology, Policy, and the Integrity of Social Life**, Stanford University Press, Stanford, CA, 2010, pp. 67-103.

11 WESTIN, Alan F., **Privacy and Freedom**, Atheneum Press, New York, 1967, pp. 52-63.

12 SOLOVE, Daniel J., **Understanding Privacy**, 2nd ed., Harvard University Press, Cambridge, MA, 2021, pp. 13-39.

13 PROSSER, William L., "Privacy", **California Law Review**, Y. 1960, V. 48(3), pp. 383-423.

imposing limitations on how organizations and third parties use such data. Independent regulators typically oversee data protection frameworks, ensuring accountability and imposing penalties for non-compliance. Exceptions exist for purposes like law enforcement and national security, reflecting a balance between individual rights and collective needs[14].

Despite its diverse interpretations, privacy is universally acknowledged as intrinsic to human dignity and essential for upholding other constitutional guarantees, such as freedom of expression and association. The Australian Privacy Charter, for example, underscores privacy as a cornerstone for preserving human dignity and other key values[15]. This universal recognition highlights privacy's critical role in facilitating autonomy, protecting reputation, and enabling individuals to maintain control over their personal lives.

As Shoshana Zuboff highlights in her seminal work *The Age of Surveillance Capitalism*, the expansion of data-driven technologies and AI poses profound risks to personal autonomy and privacy, transforming private human experience into a new source of economic value[16].

The right to privacy is a dynamic and multidimensional concept that adapts to societal, cultural, and technological contexts. Its foundational principles remain deeply rooted in human dignity and autonomy, serving as a vital safeguard against unwarranted intrusions and ensuring the protection of personal freedoms in an increasingly interconnected world.

IV. UNITED NATIONS FRAMEWORKS

A. United Nations General Assembly Resolution on Artificial Intelligence

The First United Nations General Assembly Resolution on Artificial Intelligence (AI) signifies a landmark commitment to promoting privacy within the governance of AI systems. This resolution emphasizes the need for AI systems to respect, protect, and promote human rights, particularly the right to privacy, across their life cycle. Below are eight key aspects demonstrating how this resolution upholds privacy as a fundamental principle.

---

14 AUSTRALIAN PRIVACY CHARTER COUNCIL, **The Australian Privacy Charter**, AustLII, 1995, https://www.austlii.edu.au, A.D. 10.01.2025.

15 Ibid.

16 ZUBOFF, Shoshana, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, Public Affairs, New York, 2019, pp. 233-254.

First, the resolution explicitly states that privacy-preserving mechanisms must be integrated into AI systems throughout their life cycle, from design to deployment and operation. This aligns with international human rights laws and underscores the necessity of embedding privacy protections in AI governance frameworks[17].

Second, it highlights the risks associated with improper or malicious use of AI systems, particularly those lacking adequate safeguards. Such uses can lead to unlawful interference with privacy, undermining the enjoyment of fundamental freedoms. The resolution calls for robust international safeguards to address these risks[18]. Sandra Wachter warns that AI profiling practices can lead to systemic discrimination and privacy erosion, particularly when algorithmic decision-making lacks transparency and accountability measures[19].

Third, the resolution encourages Member States to implement policies that ensure personal data protection and privacy across the AI system life cycle. This includes establishing transparency requirements, conducting risk assessments, and adopting privacy-preserving technologies[20].

Sandra Wachter argues that transparency mechanisms, though necessary, are insufficient alone to mitigate the risks of systemic discrimination and privacy violations arising from AI profiling practices[21]. The UNGA Resolution's emphasis on transparency and fairness marks a positive step; however, without strong mechanisms for algorithmic accountability and independent oversight, privacy vulnerabilities may persist at systemic levels, especially in opaque or high-risk AI applications.

Fourth, it underscores the importance of fair, inclusive, and responsible data governance frameworks. These frameworks must safeguard personal data, promote privacy preservation, and support trusted cross-border data flows, ensuring that data governance practices align with privacy principles[22].

---

17 UNITED NATIONS GENERAL ASSEMBLY, **Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (A/78/L.49)**, 2024, https://undocs.org, A.D. 25.12.2024.

18 UNITED NATIONS GENERAL ASSEMBLY, **Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence**, p. 3.

19 WACHTER,-Sandra, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", **Computer Law & Security Review**, Y. 2018, V. 34, No. 3, pp. 436-449.

20 UNITED NATIONS GENERAL ASSEMBLY, **Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence**, p.6.

21 WACHTER, pp. 436-449.

22 UNITED NATIONS GENERAL ASSEMBLY, **Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence**, p. 7.

Fifth, the resolution advocates for transparency and human oversight in AI systems to protect end-users privacy. It emphasizes the need for mechanisms that provide notice, explanation, and effective redress for individuals adversely affected by automated decisions[23].

Sixth, the resolution calls for inclusive and equitable AI systems that avoid biases or discriminatory outcomes infringing on privacy rights. This includes addressing algorithmic biases that may arise from inadequate data governance, thus ensuring fairness and privacy for all[24].

Seventh, international cooperation is encouraged to develop and implement standards and safeguards that protect privacy while promoting the responsible use of AI. This cooperation aims to ensure equitable access to AI benefits while upholding robust privacy protections[25].

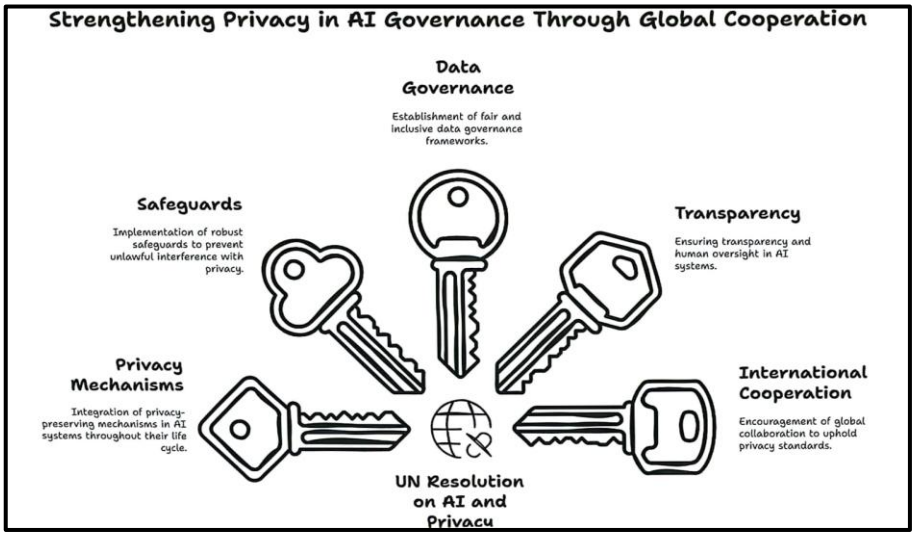

Figure 2. Strengthening Privacy in AI Governance Through Global Cooperation. Created by the Author

Finally, the resolution emphasizes addressing the gender digital divide, which includes promoting privacy and online safety for marginalized groups. This ensures that privacy considerations are integral to efforts aimed at enhancing digital literacy and accessibility[26].

[23] Ibid., p. 6.
[24] Ibid.
[25] Ibid.
[26] Ibid., p. 7.

The United Nations General Assembly's resolution strongly promotes the right to privacy by embedding it as a core principle in AI governance. Through its comprehensive framework, the resolution addresses the challenges posed by AI systems, emphasizing privacy-preserving measures, inclusive data governance, and international cooperation. These efforts reflect the global commitment to balancing technological innovation with the protection of fundamental rights.

B. UN Global Digital Compact

The UN Global Digital Compact, initiated by the United Nations Office of the Secretary-General's Envoy on Technology, sets out principles for inclusive, secure, and rights-based digital governance, prominently emphasizing the right to privacy in digital spaces. The UN Global Digital Compact (GDC) serves as a landmark framework for guiding digital governance, recognizing the critical role of the right to privacy in addressing the challenges and opportunities posed by emerging technologies such as artificial intelligence (AI). Privacy is woven into the fabric of the Compact, establishing it as an essential principle in the creation of inclusive, secure, and rights-respecting digital environments. Below, the various dimensions of privacy highlighted in the Compact are analyzed to underscore its robust commitment to safeguarding this fundamental right.

The GDC explicitly acknowledges the growing risks associated with the collection, sharing, and processing of data in digital and AI systems, emphasizing the necessity of personal data protection and privacy norms[27]. It commits to developing data governance frameworks rooted in international and regional guidelines, ensuring that privacy is at the core of data use. Notably, individuals are empowered with the ability to give or withdraw consent for the use of their personal data, which is further protected through legally mandated measures. These provisions reflect the recognition of privacy as a cornerstone of equitable and responsible digital transformation[28].

In line with its broader commitment to human rights, the Compact underscores that the development and use of digital technologies must adhere to international human rights law, ensuring the protection of privacy throughout the technology lifecycle. Governments are called upon to establish robust safeguards to mitigate adverse human rights impacts, including privacy violations.

---

[27] UNITED NATIONS, **Global Digital Compact**, United Nations General Assembly, 2024, https://www.un.org/techenvoy/global-digital-compact, A.D. 17.12.2024.

[28] UNITED NATIONS, **Global Digital Compact**, p. 1.

This responsibility extends to private sector actors, who are urged to align their operations with the UN Guiding Principles on Business and Human Rights to prevent privacy infringements[29].

The Compact also integrates privacy considerations into its focus on digital trust and safety. While addressing challenges such as hate speech, misinformation, and violence in digital spaces, the Compact insists that these measures must respect privacy and freedom of expression. It promotes collaborative efforts among national institutions to balance the protection of privacy with mitigating online harms, thus ensuring a comprehensive and rights-respecting approach to digital safety[30].

Transparency and accountability in digital ecosystems form another pillar of the GDC's privacy framework. Digital technology companies and platforms are encouraged to enhance transparency in their handling of user data, enabling users to make informed decisions about their privacy. Additionally, researchers are provided access to platform data under conditions that safeguard user privacy, fostering an evidence-based approach to policymaking and accountability in addressing online harms[31].

The Compact extends its privacy focus to the global dimension of cross-border data flows, emphasizing the importance of maintaining strong privacy safeguards in such processes. This commitment reflects the understanding that secure and trusted cross-border data flows are integral to a globally interconnected digital economy, and privacy protections are essential to achieving this trust[32].

Furthermore, the governance of artificial intelligence (AI) systems is identified as a critical area for upholding privacy rights. The Compact highlights the need for transparency, accountability, and robust human oversight of AI to ensure compliance with international human rights standards, including privacy protections. It also calls for collaborative efforts to design AI systems that respect privacy and mitigate risks associated with data misuse[33].

---

29 UNITED NATIONS, **Global Digital Compact**, p. 7.

30 Ibid., p.9.

31 Ibid., p.10.

32 Ibid., p.11.

33 Ibid., p.13.

Finally, the Compact reinforces the importance of international cooperation and capacity-building for privacy protections. Developing countries are identified as needing support to establish effective privacy frameworks. The UN is tasked with promoting capacity-building initiatives to advance responsible and interoperable data governance, ensuring that privacy protections are universal and equitable[34].

C. The UNGA Resolution 79/243: United Nations Convention Against Cybercrime

The United Nations General Assembly adopted Resolution 79/243, establishing the United Nations Convention against Cybercrime, with a strong emphasis on upholding human rights and protecting personal privacy during cybercrime enforcement.

The UNGA Resolution 79/243: United Nations Convention against Cybercrime represents a critical international framework addressing cybercrime while ensuring the protection of fundamental human rights, particularly the right to privacy. The resolution incorporates provisions that promote privacy as a foundational principle and introduces procedural safeguards to prevent undue interference with personal privacy in law enforcement activities. The following analysis highlights eight key provisions demonstrating how this resolution promotes and protects the right to privacy.

The preamble of the Convention establishes its foundational acknowledgment of privacy as a fundamental human right. It explicitly recognizes the need to protect individuals against arbitrary or unlawful interference with their privacy and emphasizes the importance of safeguarding personal data. This acknowledgment is not merely symbolic but sets a normative tone for the Convention, ensuring that all subsequent articles adhere to the principles of privacy protection[35].

Article 6, titled "Respect for Human Rights," further solidifies the commitment to privacy by mandating that the implementation of the Convention must align with international human rights law. The article specifically states

---

[34] Ibid., p.11.

[35] UNITED NATIONS GENERAL ASSEMBLY, **UNGA Resolution 79/243: United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes**, 2024, https://undocs.org/en/A/RES/79/243, A.D. 10.01.2025.

that no provision of the Convention should be interpreted as permitting the suppression of fundamental freedoms, including the right to privacy. This alignment with established human rights norms ensures that privacy remains a cornerstone even as States combat cybercrime[36].

Article 24, titled "Conditions and Safeguards," focuses on the procedural mechanisms through which law enforcement can access data. This article emphasizes the importance of proportionality, judicial oversight, and the availability of remedies to prevent misuse or overreach. By requiring these safeguards, the article ensures that procedural measures, such as data collection or interception, do not infringe unnecessarily on individual privacy. This balance highlights the dual objectives of enabling effective law enforcement while upholding the right to privacy[37].

Article 36, titled "Protection of Personal Data," directly addresses the handling of personal data in international cooperation. This article stipulates that personal data should only be transferred in compliance with domestic and international privacy laws and that effective safeguards must be in place. Furthermore, it mandates that any subsequent transfer of data to third parties requires authorization from the original State, ensuring transparency and accountability in data handling. This provision underscores the importance of protecting personal data in cross-border law enforcement efforts[38].

In addition to these overarching principles, the Convention incorporates specific provisions to criminalize privacy violations. Article 8, for example, prohibits the unauthorized interception of non-public electronic transmissions, ensuring that individuals are protected from illegal surveillance and breaches of private communications. Similarly, Article 16 addresses the non-consensual dissemination of intimate images, reinforcing the commitment to preserving personal dignity and privacy in digital spaces. These criminalization measures serve as deterrents against privacy violations and affirm the importance of privacy in the digital age[39].

The procedural safeguards related to data access and preservation are further elaborated in Articles 25 through 28. These articles detail the mechanisms

36 UNITED NATIONS GENERAL ASSEMBLY, **UNGA Resolution 79/243**, p. 6.

37 Ibid., p. 15.

38 Ibid., p. 21.

39 Ibid., p. 11.

for the expedited preservation of electronic data and traffic information, emphasizing the need for confidentiality, judicial authorization, and proportionality. By incorporating such safeguards, the Convention minimizes the risk of privacy infringements during the collection and use of digital evidence[40].

Articles 29 and 30, which govern the real-time collection of traffic and content data, impose strict limitations to ensure that such measures are only applied to serious criminal offenses. They further require that these intrusive practices comply with established safeguards, reinforcing the priority given to privacy in operationalizing these procedures. By restricting real-time data collection, the Convention emphasizes the necessity of balancing investigative needs with privacy rights[41].

Finally, Article 40, which addresses mutual legal assistance, ensures that international cooperation in evidence sharing and investigation adheres to privacy safeguards. It mandates that personal information shared across borders must be handled in a manner consistent with privacy and human rights protections. This reinforces a global commitment to maintaining privacy standards even in collaborative efforts to combat cybercrime[42].

The UNGA Resolution 79/243: United Nations Convention against Cybercrime represents a comprehensive international framework that not only addresses the challenges of cybercrime but also underscores the importance of safeguarding the right to privacy. Through its acknowledgment of privacy as a fundamental right, alignment with international human rights law, procedural safeguards, and specific provisions criminalizing privacy violations, the Convention demonstrates a robust commitment to privacy protection. These provisions highlight how the Convention strives to balance effective law enforcement with the protection of individual rights, ensuring that privacy remains a central pillar in the fight against cybercrime.

V. OECD FRAMEWORK

A. OECD Initial Policy Considerations for Generative Artificial Intelligence

The *OECD Initial Policy Considerations for Generative Artificial Intelligence* is a pivotal framework that underscores the importance of the right to

40 Ibid., pp. 16-18.

41 Ibid., pp. 18-19.

42 Ibid., p. 24.

privacy in the context of advancing artificial intelligence (AI) technologies. The document not only identifies the privacy risks inherent in generative AI systems but also strongly advocates for policies and practices that safeguard this fundamental right. Below, we explore eight key provisions and considerations highlighted in the document, illustrating its commitment to privacy as an essential aspect of AI governance.

The OECD framework acknowledges that generative AI systems pose significant risks to privacy, particularly due to their potential misuse in surveillance and the unauthorized use of personal data. The framework identifies that generative AI can amplify these risks through its ability to generate synthetic content, which may inadvertently disclose private information or be used to mimic individuals without consent. Such risks necessitate robust legal and policy frameworks to prevent harm to individuals' privacy[43].

A recurring theme in the OECD's considerations is the essential role privacy plays in ensuring the trustworthiness and inclusivity of generative AI systems. Privacy is highlighted as a foundational principle in AI governance, crucial for fostering public trust and encouraging responsible adoption of the technology. By emphasizing privacy as a key tenet of governance, the OECD positions it as a prerequisite for ethical and sustainable AI deployment[44].

The OECD framework promotes the development of ethical guidelines that prioritize privacy protection. These guidelines advocate for compliance with international standards such as the General Data Protection Regulation (GDPR) and encourage the adoption of privacy-by-design principles in AI development. Additionally, the document calls for data governance mechanisms to ensure that personal data used in training generative AI models is sourced and managed ethically[45].

Shoshana Zuboff critiques that, despite widespread advocacy for data minimization principles, real-world economic incentives frequently push AI developers toward expansive data collection practices[46]. This tension suggests that the

---

43 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), **Initial Policy Considerations for Generative Artificial Intelligence (OECD Artificial Intelligence Papers)**, 2023, p. 13, https://www.oecd.org/en/publications/initial-policy-considerations-for-generative-artificial-intelligence_fae2d1e6-en.html, A.D. 05.01.2025.

44 OECD, **Initial Policy Considerations for Generative Artificial Intelligence**, p. 27.

45 Ibid., p. 16.

46 ZUBOFF, **The Age of Surveillance Capitalism**, pp. 233-239.

OECD's emphasis on ethical AI development and responsible data stewardship, while normatively important, faces substantial practical challenges in the current commercial environment dominated by surveillance-driven business models.

Generative AI has significant implications for workplace privacy, as identified in the OECD document. AI systems deployed in workplace settings may increase surveillance of employees and lead to intrusive monitoring practices. The OECD emphasizes that protecting employees' privacy rights is vital to maintaining fairness and ethical standards in AI-driven workplaces. Concerns raised by employees about data misuse are particularly addressed, reflecting the importance of transparency and accountability in workplace AI applications[47].

Transparency is a cornerstone of the OECD's privacy framework. The document calls for transparency mechanisms that enable users to understand how their data is collected, processed, and utilized by generative AI systems. These mechanisms are critical for preventing privacy violations and ensuring accountability among AI developers and operators. For instance, the OECD recommends implementing watermarking and content provenance techniques to identify and trace synthetic content, thereby enhancing transparency[48].

To mitigate privacy risks, the OECD emphasizes data minimization as a critical strategy. This principle entails limiting the collection and use of personal data in training generative AI models to only what is necessary for their intended purposes. By adopting this approach, the document underscores the importance of reducing exposure to privacy risks while maintaining the functionality and effectiveness of AI systems[49].

The OECD document highlights the need for international cooperation to harmonize privacy standards across jurisdictions. Initiatives such as the Hiroshima AI Process are cited as examples of collaborative efforts to establish global norms and frameworks for protecting privacy in generative AI applications. Such international collaboration ensures that privacy protections are consistent and comprehensive, addressing cross-border challenges in AI governance[50].

---

47 OECD, **Initial Policy Considerations for Generative Artificial Intelligence**, p. 20.

48 Ibid., p. 15.

49 Ibid., p. 18.

50 Ibid., p. 9.

Finally, the OECD proposes a range of mitigation measures to address privacy risks associated with generative AI. These include the adoption of privacy-by-design principles, stringent data governance policies, and transparency frameworks. The document also warns of the risks posed by synthetic content training cycles, advocating for proactive measures to prevent compounding privacy violations over time[51].

The *OECD Initial Policy Considerations for Generative Artificial Intelligence* strongly promotes the right to privacy through its comprehensive policy recommendations and ethical guidelines. By addressing privacy risks, advocating for transparency, and encouraging international collaboration, the OECD framework lays a robust foundation for integrating privacy as a core principle in generative AI governance. These considerations not only safeguard individual rights but also enhance public trust and support the responsible development of AI technologies.

VI. COUNCIL OF EUROPE FRAMEWORK

A. Council of Europe Draft Framework Convention on Artificial Intelligence

The Council of Europe Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law presents a comprehensive approach to embedding privacy protections in AI governance. By addressing privacy explicitly and embedding it across key principles and obligations, the Convention underscores its commitment to safeguarding this fundamental right. Below, the provisions related to the right to privacy are examined.

The Preamble to the Convention highlights privacy as a cornerstone of its normative framework. The text highlights the enduring significance of privacy in the context of AI development, drawing on established frameworks such as the 1981 Council of Europe Convention 108 on data protection. Multiple iterations of the preamble (Options A, B, and C) underscore privacy protection as both a standalone right and integral to broader commitments to human rights and personal data protection[52].

---

51 Ibid., p.26.

52 COUNCIL OF EUROPE, **Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law**, 2023, Preamble p. 3, https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043, A.D. 05.01.2025.

The centrality of privacy protection is further elaborated in Article 10: Privacy and Personal Data Protection. This article mandates that States adopt measures ensuring compliance with applicable domestic and international privacy laws. These measures require AI systems to safeguard individuals' privacy throughout their lifecycle, including robust guarantees for data subjects as prescribed under national and international obligations. This provision integrates privacy deeply into the operationalization of AI systems, bridging legal requirements with technological innovation[53].

Further protection is provided in Article 15: Procedural Safeguards, which ensures individuals' autonomy and informed interaction with AI systems. By requiring notification mechanisms that inform users when they are engaging with AI rather than humans, the article enhances transparency. Additionally, it guarantees procedural safeguards and remedies for individuals impacted by AI decisions, reflecting a commitment to upholding human rights and the right to contest privacy-invading practices[54].

Article 16: Risk and Impact Management Framework institutionalizes a risk-based approach to safeguarding privacy. The Convention obliges States to undertake iterative risk assessments throughout the AI lifecycle, integrating stakeholder perspectives, including those whose privacy might be affected. This framework ensures accountability and ongoing adaptation to emerging privacy risks, reinforcing privacy protection as a dynamic process[55].

The General Obligations (Article 4) chapter asserts the overarching commitment to align AI activities with international human rights obligations, explicitly encompassing privacy rights. By embedding privacy into the Convention's foundational commitments, the text ensures that all subsequent principles and provisions are inherently aligned with this right[56].

Articles 7 and 8, within Chapter III, introduce procedural and operational principles to bolster privacy. Transparency measures in Article 7 aim to disclose the operations of AI systems in contexts where privacy might be at risk. Article 8 emphasizes accountability for adverse impacts on privacy, ensuring that responsible entities are held to account for violations[57].

---

53 COUNCIL OF EUROPE, **Draft Framework Convention on Artificial Intelligence**, p. 8.

54 Ibid., p. 9.

55 Ibid.

56 Ibid., p.7.

57 Ibid.

Finally, Article 20: Public Consultation in Chapter VI highlights the role of public dialogue in addressing AI's societal, legal, and ethical implications, including privacy concerns. By fostering multi-stakeholder consultations, the article integrates privacy into broader public governance frameworks, enhancing collective accountability[58].

The Council of Europe's Draft Framework Convention represents a significant step in embedding privacy protection into AI governance. By aligning its provisions with established international norms and introducing dynamic, risk-based, and participatory approaches, the Convention reaffirms privacy as an essential aspect of human rights in the era of artificial intelligence.

VII. EUROPEAN UNION FRAMEWORK

A. European Union Artificial Intelligence Act

The European Union (EU) Artificial Intelligence Act (AIA) represents a significant milestone in embedding the principles of the right to privacy within AI governance. As a legislative framework, it underscores the EU's commitment to ensuring that the development and deployment of AI systems respect fundamental rights, particularly the right to privacy. This analysis examines eight key provisions within the AIA that collectively establish a robust framework for privacy protection and demonstrate how the legislation strongly promotes this fundamental right.

First, the AIA explicitly integrates privacy protections within its foundational principles. It aligns with existing EU data protection laws, such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive, to safeguard the right to privacy and data protection. Recent scholarship emphasizes that the AI Act must also be interpreted in conjunction with the Data Governance Act, the Data Act, and forthcoming instruments such as the European Health Data Space, as their combined operation will shape future compliance landscapes and privacy safeguards within the Union[59]. In addition, scholars note that EU initiatives-including the Coordinated Plan on AI, national strategies from 2018 to 2021, and the Ethics Guidelines for Trustworthy AI-reflect a rapidly evolving regulatory environment addressing privacy, transparency, and

[58] Ibid., p. 10.

[59] GÜNEŞ PESCHKE, Seldağ, and Lutz PESCHKE, "Artificial Intelligence and the New Challenges for EU Legislation", **Yıldırım Beyazıt Hukuk Dergisi Prof. Dr. M. Fatih UŞAN'a Dekanlıkta 10. Yıl Anısına Teşekkür Armağanı**, No. 2022-2, Eylül 2022, pp. 1267-1292.

bias[60]. The Act emphasizes that AI systems must comply with established data protection laws and ensures that they do not infringe on the fundamental rights enshrined in the EU Charter of Fundamental Rights[61].

Second, the AIA prohibits AI practices that are inherently harmful to fundamental rights, including privacy. Notably, it bans the untargeted scraping of facial images from the internet or CCTV footage to create or expand facial recognition databases. This practice is recognized as a violation of the right to privacy and contributes to the feeling of mass surveillance. By prohibiting such intrusive practices, the Act reinforces the principle that privacy is a non-negotiable right[62].

Third, the AIA introduces stringent requirements for handling biometric data, acknowledging its sensitivity and potential for misuse. It mandates that AI systems involving biometric identification or categorization undergo rigorous scrutiny to prevent privacy violations. This provision aims to safeguard individuals from intrusive surveillance practices and ensures compliance with privacy and data protection laws[63].

Fourth, the Act incorporates the principles of "data protection by design and default," requiring developers to prioritize privacy throughout the AI system lifecycle. This includes implementing measures such as data minimization, anonymization, and encryption. Such safeguards ensure that privacy considerations are embedded in every phase of AI development, reducing the risk of data breaches and unauthorized data use[64]. Woodrow Hartzog contends that 'privacy by design' must move beyond compliance and embody fundamental constitutional values, suggesting that technical measures should internalize respect for privacy rather than treating it as an afterthought[65]. He also emphasizes that privacy-by-design must be understood not merely as a regulatory requirement but

---

60 PAWELOSZEK, Ilona, Narendra KUMAR, and Umesh SOLANKI, "Artificial Intelligence, Digital Technologies and the Future of Law: Literature Review", **Futurity Economics & Law**, Y. 2022, V. 2, No. 2, pp. 43-46.

61 EUROPEAN UNION, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Harmonised Rules for Artificial Intelligence (Artificial Intelligence Act), **Official Journal of the European Union**, L 1689, Y. 2024, pp. 1-144, http://data.europa.eu/eli/reg/2024/1689/oj, A.D. 05.01.2025.

62 Ibid., Recital 43, p. 10.

63 Ibid., Recital 38, p. 9.

64 Ibid., Recital 69, p. 24.

65 HARTZOG, Woodrow, **Privacy's Blueprint: The Battle to Control the Design of New Technologies**, Harvard University Press, Cambridge, MA, 2018, pp.1-18.

as a foundational constitutional safeguard within technological development[66]. In his view, technical compliance alone cannot guarantee substantive privacy protection unless design practices internalize respect for fundamental rights from the outset. Viewed through this lens, while the EU AI Act makes significant progress by embedding data minimization and encryption requirements, concerns persist about the enforceability and operationalization of these protections within diverse AI system architectures.

Fifth, the AIA ensures that privacy is preserved in the context of AI regulatory sandboxes-controlled environments for testing AI systems. The Act stipulates that any personal data processed within these sandboxes must adhere to strict privacy and security requirements, including limitations on data reuse. This provision guarantees that innovation does not come at the expense of individuals 'privacy[67].

Sixth, the AIA establishes guidelines for processing special categories of data in exceptional cases, such as bias detection. It requires the use of advanced privacy-preserving techniques, including pseudonymization and restricted access, to mitigate the risks associated with handling sensitive data. This approach balances the need for fairness in AI systems with the imperative to protect privacy[68].

Seventh, transparency and accountability are central to the AIA's framework, particularly for high-risk AI systems. Developers and deployers are required to maintain comprehensive documentation to demonstrate compliance with privacy regulations and facilitate oversight. This provision enhances trust by ensuring that privacy protections are both visible and enforceable[69].

66 HARTZOG, **Privacy's Blueprint**, p. 18.

67 Ibid., Recital 59, p. 19.

68 Ibid., Recital 5, p. 2.

69 Ibid., Recital 71, p. 25.

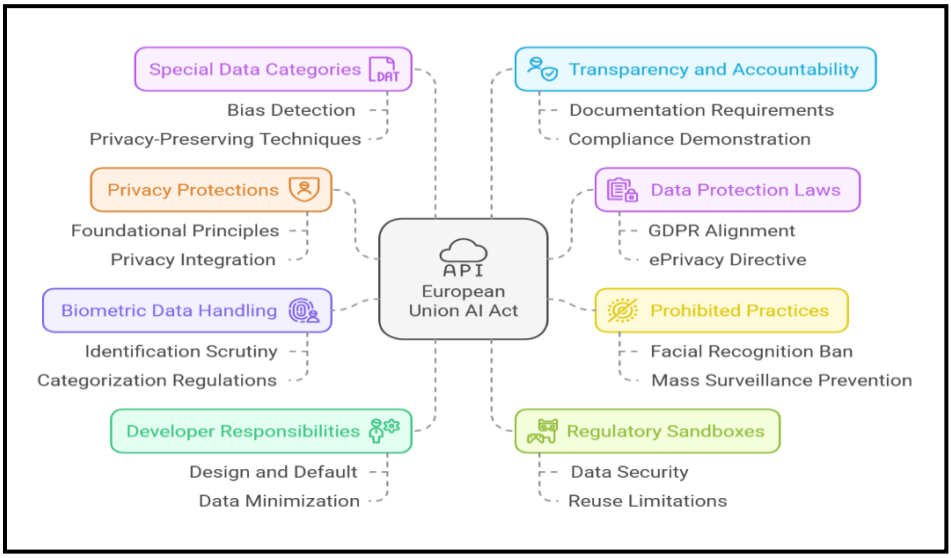

Figure 3. API European Union AI Act. Created by the Author

Finally, the Act explicitly addresses the risks of discriminatory and privacy-invasive outcomes in sensitive contexts such as employment or public services. It underscores the importance of designing AI systems that respect individuals' privacy and autonomy, thereby mitigating the potential for adverse impacts on vulnerable groups[70].

The European Union Artificial Intelligence Act establishes a comprehensive framework that strongly promotes the right to privacy. By integrating privacy protections into its core principles, prohibiting harmful practices, ensuring rigorous oversight, and embedding privacy-preserving techniques, the Act exemplifies a human-centric approach to AI governance. This legislative framework not only aligns with the EU's foundational values but also serves as a model for international efforts to balance innovation with fundamental rights.

VIII. ORGANIZATION OF AMERICAN STATES FRAMEWORK

A. OAS Inter-American Guidelines on Data Governance and Artificial Intelligence

The OAS Inter-American Guidelines on Data Governance and Artificial Intelligence represent a significant step in establishing a framework that robustly

[70] Ibid., Recital 57, p. 18.

safeguards the right to privacy in the context of artificial intelligence (AI) governance. By embedding privacy considerations throughout its provisions, the guidelines emphasize its integral role in ethical, transparent, and rights-based data governance. Below, ten key aspects demonstrate how the guidelines strongly promote and defend the right to privacy:

Firstly, the guidelines underscore the importance of updating regulatory frameworks related to data governance, ensuring that these frameworks include robust privacy and personal data protection provisions. By mandating compliance with such standards, the guidelines aim to fortify privacy safeguards in data-driven and AI initiatives[71].

Secondly, the guidelines specifically call for adherence to Inter-American principles regarding personal data protection and privacy. These principles are fundamental to maintaining transparency and ethical data usage, reflecting the commitment of the guidelines to uphold individuals' privacy rights[72].

Additionally, the guidelines advocate for the establishment of multi-stakeholder verification mechanisms involving civil society, academia, and the private sector. These mechanisms are designed to ensure the effective application of ethical guidelines, particularly concerning privacy safeguards throughout the data lifecycle[73].

The guidelines also emphasize the necessity of grievance and redress mechanisms for addressing privacy-related rights violations. These mechanisms provide individuals with avenues for recourse in instances where their privacy may have been compromised due to inadequate data management or misuse of AI systems[74].

Further reinforcing the protection of privacy, the guidelines integrate ethical and transparency principles into data governance strategies. These principles mandate a rights-based approach that prioritizes privacy considerations, thereby embedding privacy as a cornerstone of AI governance[75].

---

71 ORGANIZATION OF AMERICAN STATES, **Inter-American Guidelines on Data Governance and Artificial Intelligence**, 2024, p. 5, §1.3, https://www.oas.org/ext/en/democracy/inter-american-framework-on-data-governance-and-artificial-intelligence-migdia, A.D. 05.01.2025.

72 ORGANIZATION OF AMERICAN STATES, **Inter-American Guidelines on Data Governance and Artificial Intelligence**, p. 11, §5.3.

73 Ibid., p. 11, §5.7.

74 Ibid., p. 11, §5.8.

75 Ibid., p. 11, §5.5.

Another critical provision is the promotion of robust security measures, such as encryption and secure coding practices, to safeguard personal data. These measures are essential to protecting privacy across all stages of data collection, storage, and processing within AI applications[76].

The guidelines further advocate for the integration of privacy into cybersecurity strategies, ensuring that privacy protections are not only an independent consideration but also a core component of broader security frameworks. This approach aims to address potential threats to personal data from internal and external sources[77].

In addition to technical safeguards, the guidelines stress the importance of educational initiatives to raise awareness about privacy rights. These initiatives aim to empower public sector actors and citizens with knowledge about personal data protection, ethical technology use, and the associated risks of AI and data governance[78].

Moreover, while promoting open data policies, the guidelines insist on respecting personal data protection and privacy. They advocate for ensuring that privacy considerations are upheld even as governments pursue transparency and innovation through open data strategies[79].

The guidelines emphasize the necessity of aligning national frameworks with international privacy standards, such as UNESCO's ethical recommendations on AI. This alignment ensures that privacy protections are consistent with global best practices and frameworks, enhancing the region's ability to safeguard individual privacy rights in a globally interconnected context[80].

CONCLUSION

This study delves into the intersection of privacy rights and artificial intelligence (AI) governance, revealing the pivotal role that international soft law frameworks play in embedding privacy protections into the lifecycle of AI systems. By examining legislative and policy frameworks across multiple international organizations, this research illuminates the critical importance of harmonizing global privacy standards to address the unique challenges posed by AI technologies.

---

76 Ibid., p. 19, §§12.5, 12.8.

77 Ibid., p. 19, §12.1.

78 Ibid., p. 10, §4.2.

79 Ibid., p. 18, §11.6.

80 Ibid., p. 6, §2.1.

The findings underscore that privacy considerations are increasingly woven into AI governance through innovative mechanisms such as privacy-by-design requirements, risk management frameworks, and prohibitions against practices like untargeted data scraping and mass surveillance. The inclusion of robust transparency mandates, safeguards against discriminatory outcomes, and international collaboration efforts represents a major advancement in embedding ethical standards within AI governance initiatives.

The unique contribution of this work lies in its comparative, cross-institutional, and interdisciplinary analysis, bridging legal, technological, and policy dimensions to present a cohesive understanding of how various international organizations address privacy protections in AI governance. By mapping and critically evaluating a range of soft law initiatives, this study offers new knowledge about the emerging global consensus on privacy rights within AI development and deployment. It highlights the convergence of human-centric principles such as transparency, accountability, fairness, and ethical AI practices across diverse frameworks, while also identifying gaps that remain in enforcement and practical realization.

Furthermore, this research demonstrates the adaptability and normative relevance of soft law instruments in rapidly evolving technological contexts, adding depth to ongoing discussions on AI ethics, international governance, and human rights protection. By emphasizing the need to align technological innovation with human dignity and autonomy, it sets a foundation for future explorations into the strengthening of privacy safeguards in the digital era.

For an international readership, the findings hold significant implications. Policymakers are provided with actionable insights into best practices for harmonizing AI privacy standards across jurisdictions. Scholars and practitioners gain a foundational understanding of how soft law frameworks can be leveraged to mitigate privacy risks while fostering innovation. Stakeholders from diverse regions benefit from the emphasis on inclusivity, ethical considerations, and multi-stakeholder collaboration, ensuring that the right to privacy remains a universal safeguard amid technological progress.

In conclusion, this research not only advances the discourse on privacy and AI governance but also serves as a call to action for sustained international cooperation. As AI technologies continue to reshape societal structures, embedding privacy as a cornerstone of governance is essential to ensure that innovation aligns with humanity's shared values, securing the fundamental rights and dignity of individuals worldwide.

Hakem Değerlendirmesi : Dış bağımsız.
Çıkar Çatışması : Yazar çıkar çatışması bildirmemiştir.
Finansal Destek : Yazar bu çalışma için finansal destek almadığını beyan etmiştir.
Peer-review *: Externally peer-reviewed.*
Conflict of Interest *: The author has no conflict of interest to declare.*
Grant Support *: The author declared that this study has received no financial support.*

BIBLIOGRAPHY

AUSTRALIAN PRIVACY CHARTER COUNCIL, **The Australian Privacy Charter**, AustLII, 1995. https://www.austlii.edu.au, A.D. 10.01.2025.

COUNCIL OF EUROPE, **Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law**, Y. 2023, https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043, A.D. 05.01.2025.

ENCYCLOPEDIA BRITANNICA, "**Rights of Privacy**", Britannica.com. (Online), https://www.britannica.com/topic/rights-of-privacy, A.D. 20.01.2025.

EUROPEAN CONVENTION ON HUMAN RIGHTS, "**Article 8**", Council of Europe, Y. 1950 (Online), https://www.echr.coe.int, A.D. 20.01.2025.

EUROPEAN UNION, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Harmonised Rules for Artificial Intelligence (Artificial Intelligence Act), **Official Journal of the European Union**, L 1689, Y.2024, pp. 1-144. http://data.europa.eu/eli/reg/2024/1689/oj, A.D. 05.01.2025.

FLORIDI, Luciano, "Soft Ethics and the Governance of Artificial Intelligence", **Philosophy & Technology**, Y. 2018, V. 31, pp. 1-8.

GAVISON, Ruth, "Privacy and the Limits of Law", **The Yale Law Journal**, Y. 1980, V. 89(3), pp. 421-471.

GILANI, Syed Raza Shah, Ali Mohammed ALMATROOSHI, and Ali Fayyaz AWAN, "An In-Depth Analysis of the Human Rights Act of 1998 and the Bill of Human Rights UK, Examining the Advantages and Disadvantages", **Current Trends in Law and Society**, Y. 2024, V. 4, No. 1, pp. 121-129.

GÜNEŞ PESCHKE, Seldağ, and Lutz PESCHKE, "Artificial Intelligence and the New Challenges for EU Legislation", **Yıldırım Beyazıt Hukuk Dergisi Prof. Dr. M. Fatih UŞAN'a Dekanlıkta 10. Yıl Anısına Teşekkür Armağanı**, No. 2022/2, V. Eylül 2022, pp. 1267-1292.

HARTZOG, Woodrow, **Privacy's Blueprint: The Battle to Control the Design of New Technologies**, Harvard University Press, Cambridge, MA, 2018, pp. 1-18.

HAYES, Paul, Ibo VAN DE POEL, and Marc STEEN, "Algorithms and Values in Justice and Security", **AI & Society**, Y. 2020, V. 35, No. 3, pp. 533-555.

NISSENBAUM, Helen, **Privacy in Context: Technology, Policy, and the Integrity of Social Life,** Stanford University Press, Stanford, CA, 2010, pp. 67-103.

NYU LAW GLOBAL, "**Right to Privacy: An International Perspective**", (Online), https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html, A.D. 20.01.2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), **Initial Policy Considerations for Generative Artificial Intelligence (OECD Artificial Intelligence Papers),** Y. 2023, https://www.oecd.org/en/publications/initial-policy-considerations-for-generative-artificial-intelligence_fae2d1e6-en.html, A.D. 05.01.2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **OECD Principles on Artificial Intelligence,** OECD Publishing, Paris, Y. 2019, https://www.oecd.org/en/topics/sub-issues/ai-principles.html, A.D. 05.08.2025.

ORGANIZATION OF AMERICAN STATES, **Inter-American Guidelines on Data Governance and Artificial Intelligence,** Y. 2024, https://www.oas.org/ext/en/ democracy/inter-american-framework-on-data-governance-and-artificial-intelligence-migdia, A.D. 05.01.2025.

PAWELOSZEK, Ilona, Narendra KUMAR, and Umesh SOLANKI, "Artificial Intelligence, Digital Technologies and the Future of Law: Literature Review", **Futurity Economics & Law**, Y. 2022, V. 2, No. 2, pp. 43-46.

PROSSER, William L. "Privacy", **California Law Review**, Y. 1960, V. 48(3), pp. 383-423.

SOLOVE, Daniel J, **Understanding Privacy,** 2nd ed. Harvard University Press, Cambridge, MA, 2021, pp. 13-39.

UNITED NATIONS GENERAL ASSEMBLY, **Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (A/78/L.49).** 2024, https://undocs.org, A.D. 25.12.2024.

UNITED NATIONS GENERAL ASSEMBLY, **UNGA Resolution 79/243: United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.** 2024, https://undocs.org/en/A/RES/79/243, A.D. 10.01.2025.

UNITED NATIONS SUSTAINABLE DEVELOPMENT GROUP, **The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding among UN Agencies,** Y. 2003, https://unsdg.un.org/resources/human-rights-based-approach-development-cooperation-towards-common-understanding-among-un, A.D. 18.12.2024.

UNITED NATIONS, **Global Digital Compact,** United Nations General Assembly, Y. 2024, https://www.un.org/techenvoy/global-digital-compact, A.D. 17.12.2024.

WACHTER, Sandra, Brent MITTELSTADT, and Luciano FLORIDI, "Transparent, Explainable, and Accountable AI for Robotics", **Science Robotics**, Y. 2017, V. 2, No. 6, eaan6080. https://doi.org/10.1126/scirobotics.aan6080, A.D. 05.08.2025.

WACHTER, Sandra, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", **Computer Law & Security Review**, Y. 2018, V. 34, No. 3, pp. 436-449.

WARREN, Samuel D., and Louis D. BRANDEIS, "The Right to Privacy", **Harvard Law Review**, Y. 1890, V. 4, No. 5, pp. 193-220.

WESTIN, Alan F, **Privacy and Freedom,** Atheneum Press, New York, 1967, pp. 52-63.

ZUBOFF, Shoshana, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,** Public Affairs, New York, 2019, pp. 233-254.