https://doi.org/ 10.62585/ilhr.v5i1.184

Volume and Issues Obtainable at Centeriir.org
Journal of International Law & Human Rights
ISSN (Print): 3007-0120 ISSN (Online): 3007-0139
Volume 5, No.1, 2026
Journal Homepage: http://journals.centeriir.org/index.php/jilhr

Use of AI and the Right to Privacy under International Law

Muqarrab Akbar [1] **Saira Akram** [2] **Ahsan Riaz**[3]

[1]Chairman, Department of Political Science, Bahauddin Zakariya University, Multan, E-Mail: muqarrabakbar@bzu.edu.pk
[2] Lecturer, Department of Political Science, Bahauddin Zakariya University, Multan. E-Mail: Saira.akram29@yahoo.com
[3] Assistant Professor, Department of Political Science,The Islamia University of Bahawalpur. E-Mail: ahsan.riaz@iub.edu.pk

ABSTRACT

The artificial intelligence technologies (AI) usage has rapidly changed the ways and working of states, corporations and other actors through collecting, processing, analyzing, inferring, and using personal information. AI has changed and reshaped the the multiple aspects of individual's life. AI systems can be used to analyze vast amounts of data, find patterns that humans might not recognize, make predictions about people and help or make decisions that impact employment, healthcare, policing, migration, education, financial services and access to public services. They offer vast opportunities for social and economic development but at the same time raise unprecedented questions about the right to privacy. What's actually becoming a growing worry is the ability of AI systems to not only track individuals and their behavior but also to predict sensitive characteristics.

This article takes a doctrinal and comparative legal approach to explore if existing international law sufficiently protects human privacy from interference by AI. It examines international human-rights instruments, regional case law, materials prepared by the UN, Council of Europe's standards, UNESCO's Recommendation on the Ethics of Artificial Intelligence and a selection of comparative regulatory developments. It states that current international human-rights law is still relevant and offers a moral compass to govern the development of AI, however, it needs to be more precisely applied. The article suggests an approach to rights, which is rooted in lawfulness, necessity, proportionality, transparency, accountability, privacy by design, human oversight, impact assessments, independent oversight and effective remedies. It argues that in order to govern AI properly, the right to privacy must be considered a core human right and not only a secondary ethical consideration, and should affect all aspects of the AI lifecycle.

Article History: Received: 01-01-2026 **Accepted**: 11-04-2026 **Published**: 30-06-2026
Keywords: Artificial Intelligence, right to privacy, Surveillance, AI Governance, Legality, UDHR.

Corresponding Author's Email: muqarrabakbar@bzu.edu.pk

https://doi.org/ 10.62585/ilhr.v5i1.184

1. Introduction:

AI is considered among the most modern and impactful technological advancements of the modern global era. With ever growing influence of AI is also raising the increasing concerns regarding privacy and human rights. AI is now an integral part of our life ranging from personal digital footprint to moving vehicle record navigating through the roads. It is not a new phenomenon as the history of AI can be traced back in 20th century when Alan Turning explored that machines were able to perform multiple function as substitute of human beings and human minds (Rayhan and Rayhan, 2023). Biases of algorithms are also posing serious challenges by escalating the human rights violations and invading privacy. New AI systems can not only handle but can easily process the large data sets, detect relationships from multilayered complex patterns, make predictions, create human-like text, support or automate decisions that were previously made by humans. AI has gained traction in various fields, including healthcare, education, law enforcement, border security, employment, banking, and national security, among others. The relationship between technology and basic rights has thus been radically changed by the increasing assimilation of AI into regular social and governmental practices. AI has impacted the right to privacy more than anything else sometimes directly and sometimes indirectly. Privacy is not just the right to be private or to be left alone. It also includes the right to be protected against unlawful encroaching and arbitrary interference in someone's private life, family life, home and correspondence and the right to be protected against the unjustified collection, retention, analysis and dissemination of personal information in the digital environment. As AI becomes more sophisticated, privacy issues can arise even if the information isn't made public. An AI system could potentially merge seemingly unrelated bits of data to determine a person's health status, political leanings, religious beliefs, relationships, pattern of travels, financial situation or psychological state. Thus, AI transforms privacy interference from merely acquiring information to ongoing observation, prediction and inference. States, at national levels, are also struggling in formulating a comprehensive strategy, rules and regulations to protect the privacy rights of individual in the age of AI. Although a unified, coherent and universally agreed comprehensive legal policy frame work related to AI is difficult to develop at international level yet the global and regional organizations and multiple states are making commendable efforts to overcome this herculean task. Re-imagining human rights and international law are now a days not a choice but an obligation to safeguard the privacy of individuals. Prosser (1960) points out that privacy can be defined in four terms in the context of legal taxonomy; portrayal in a false night, public disclosure of private facts, appropriations of names or likeness for personal gain, and intrusion upon seclusion.

There is a solid international legal basis for privacy. UDHR in its article 12 clearly says that no one should be subjected to "arbitrary interference" with privacy of individual, privacy of family, home or personal correspondence. Moreover, ICCPR through its article 17 imposes a binding treaty obligation on States Parties (United Nations, 1966, art. 17). The provisions show that privacy is not just a domestic issue but an accepted human right in international law. The Human Rights Committee (1988, para.5) has also clarified the obligation of the States to protect individuals from unlawful or arbitrary interference with their privacy and the fact that relevant protections apply to any technology used to interfere with the identity of the individuals.

The rise of AI thus does not pose a completely new legal issue, but merely a variation on an old theme. Instead, it establishes a new technological context in which traditional human rights standards will have to play their role. The real issue is whether the current international law is clear and useful enough to control an AI system that can operate in ways that are opaque, international and generate new information about people. This question is now even more urgent since AI systems often rely on large data sets. Generative AI models, facial-recognition systems, recommendation algorithms and predictive systems

may require the processing of information relating to millions of individuals. Information could be gathered from Internet sites, social media, public records, cellphones, market databases, and more. Sometimes, people might be unaware that their data is being used or that it is being utilized to train an AI model. Where information is initially lawfully acquired, its further use for a new AI related purpose could trigger purpose limitation, proportionality and legitimate expectation issues.

There are other concerns when it comes to governmental usage of AI. By using facial recognition, authorities can identify people in public areas. Predictive policing systems can be used to analyze past data and look for patterns or clusters of locations or people that are likely to be involved in future crimes. Biometric and behavioral data can be analyzed by automated border-control systems. Algorithm systems can be employed by intelligence agencies to handle communications and metadata on a massive scale. The use cases outlined here illustrate how AI can be used to expand the speed, scale and persistence of State surveillance. Another aspect of the problem is the private sector. New technology firms and other firms have vast amounts of individual information and could use AI to forecast what individuals do and how to advertise to them, to determine credit worthiness, to screen staff members or create commercial products. International human-rights law is primarily relies on States' obligations, which poses a problem when privacy interference is caused by corporate activity. The United Nations Guiding Principles on Business and Human Rights still recognize the duty of the business to respect internationally recognized human rights. (United Nations Office of the High Commissioner for Human Rights [OHCHR], 2011). These kinds of measures are necessary to adopt as the Office of the High Commissioner for Human Rights (OHCHR) pointed out multiple incidents and cases of human rights violations in the wake of AI usage in their multiple reports (Billeh et. Al. , 2024, 345)

Recent international developments indicate recognition of these challenges. The Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law in 2024. This Convention emphasizes on ensuring human rights, democracy and the rule of law in all AI related activities and expressly addresses privacy and personal-data protection (Council of Europe, 2024, art. 10, 11; Billeh et. Al, 2024). UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence similarly identifies privacy and data protection as central principles for responsible AI governance (UNESCO, 2021, para. 18). These are still the geographically dispersed elements of the international framework. There is no specific mention of AI in the ICCPR. International privacy standards have been formulated without the advent of modern generative AI, large facial recognition systems, and foundation models. Greater protections are provided through regional legal systems, however they do not provide a geographic boundary. Soft Law instruments are important tools for principles but may not actually be enforceable. Furthermore, technological advances are often out pace international law-making.

1 Hassan (2025) claims that international committee of nations have developed the soft law framework to address the challenges of privacy in the age of AI governance. Human Rights-Base Approach (HRBA) points out that any new development that can affect the human including the AI must be adopted and implemented by keeping in view the core and fundamental principles of human rights and privacy as it is very vital aspects of human freedom and privacy. It is sometimes becomes very complex to uphold the right of privacy in the digital age due to maintaining the equilibrium between collective interest of the society and individual rights.

2 Many scholars such as Zuboff (2019) and Wachter (2018) have identified that personal privacy and autonomy is at severe risk due to ever increasing expansion of AI and data driven technology through violation of privacy in the wake of AI profiling practices that can lead towards weak transparency and absence of accountability due to decision making based on algorithm. However, the global community can develop a global digital legal framework where the rights and privacy of the individual are not compromised, at least not at risk.

This paper then looks at the potential role of international law for safeguarding privacy in an AI era. It claims that the modern framework of international human-rights is strong in terms of norm, but protection of rights needs to be reinterpreted and successfully practiced by reconstructing existing rights in a new institutional and procedural framework. Data should be collected and retrieved within the context of confidentiality, all models should be developed with the perspective of confidentiality, the deployment of the model should also help to maintain confidentiality, and monitoring, modifying the models and eventually retiring the models should be done with respecting the confidentiality of data.

2. The Idea of Artificial Intelligence along with the Privacy Rights:

AI is not just one technology, it is a general term for a cluster of computing methods that can be used to do things that humans can too. Modern AI encompasses multidimensional traits, such as deep learning, machine learning, natural-language processing, computing codes, and automated decision-making systems. Unlike the classic models, machine-learning systems typically detect patterns within data sets and not only follow hard-coded instructions. The effectiveness of these systems thus relies heavily on the availability of data, both in terms of quantity, quality, and characteristics. Finally, it is important to note the bond between AI and data, as fundamental to understanding the privacy problem. The typical concerns of privacy involved the gathering of personally identifiable data like names, addresses, medical records or communications. AI also increases the problem by its ability to find information that wasn't given directly to a system. Many of these characteristics can be aggregated from a person's online activities, transactions, and social relationships, and combine to allow a system to make inferences that are not explicitly included in any one of these categories. It is then more important to differentiate between data and inference. When, for example, an AI system determines that someone is likely to have a medical condition, or a certain type of psychological trait, and makes an inference based on that, the person's private life could be impacted as a result, even though the individual did not provide the data themselves. Protection of privacy should therefore not just consider the collection of personal information, but also the creation of personal knowledge, as a result of algorithmic inferences.

This is a conceivable evolution covered by the concept of privacy as understood in international human-rights conventions. Article 17 of the ICCPR guarantees coverage against invasion of privacy of a person’s life, his family life, his home and his correspondence for human rights individuals. The Human Rights Committee also emphasizes that the collection of personal information on computers, data banks and other digital devices should be under the legal rules and regulations. In addition to this, the individuals having access to such information should use storage and use of their personal data in the light of national and international privacy practices (United Nations Human Rights Committee, 1988, para. 5). A extensive and comprehensive legislation is required to identify and punish such individuals who are responsible of immoral and illegal usage of data by themselves or by leaking it to others (Lubis, 2016).

The notions of lawfulness and arbitrariness are crucial in the context of AI. If the technology is useful, a State cannot justify its intrusive uses with that alone. The interference needs to be on a legal ground, and cannot be arbitrary. It is therefore crucial to assess AI systems when the use of AI causes a violation in privacy in line with the principles of necessity and proportionality in international human rights law. Intrinsic links also exist between Privacy and other rights. Wide-spread surveillance can impact freedom of expression, in that people can change their actions when they feel they are being monitored. AI profiling may have an impact on equality and non-discrimination if algorithmic predictions have a discriminatory effect. When social and political relations among individuals are monitored, there may be interfered with the freedom of association through automated processing of personal information. This therefore is not a right to privacy, but a precondition for practicing a myriad of other human rights. As a result, today's

understanding of the right to privacy must encompass at least four related aspects: informational privacy, spatial privacy, decisional privacy and communicational privacy. Informational privacy concerns personal information, spatial privacy protects places and environments of private life, decisional privacy protects personal autonomy and communicational privacy protects letters and communications. All four can be impacted by AI.

3. International Legal Foundation of the Right to Privacy

3.1 Universal Declaration of Human Rights:

The modern international recognition of privacy begins with Article 12 of the UDHR. The provision establishes that individuals should not be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honor and reputation. For the most part, the UDHR can be regarded as a declaration and not a treaty, however it has been a keystone document for the advance of global human-rights law.

Article 12 is technology agnostic. Does not limit protection against interference to specific forms of interference. This is a crucial point to make in the AI arena since technology is fast-changing. Having to keep playing the catalogue of technologies will soon make this privacy right rapidly outdated. The general statement can be used in new ways of surveillance and information processing. Also equally significant is the concept of "arbitrary" interference. An interference can be illegal under domestic law but nevertheless be arbitrary, meaning that it is unreasonable, disproportionate or runs counter to the aims and the safeguards of human rights.

3.2 International Covenant on Civil and Political Rights

Article 17 of the ICCPR provides the principal treaty-based international protection of privacy. It prohibits arbitrary or unlawful interference with privacy, family, home or correspondence and unlawful attacks on honor and reputation (United Nations, 1966, art. 17). The fundamental treaty-based international protection of privacy is given by ICCPR Article 17. It should also be protected from such interference or attack by law. The ICCPR is notable, in particular, for the Binding nature that it imparts on States Parties. The right to privacy is thus not simply a principle but a treaty obligation. States need to put in place legal and institutional processes that prevent and respond to unlawful or arbitrary interference.

The Human Rights Committee's 'General Comment' No. 16 is still very much pertinent. The Committee has clarified that the application of Article 17, on the access to and control of personal information, involves a "regulatory approach" on restrictions on the collection and retention of personal information as well as on its misuse. While the General Comment was a long time before modern AI, the concept can be applied to automate data management. In particular, with the advent of AI, it is crucial for individuals to be unable to learn the algorithm's workings. If the government involved is relying on an opaque predictive system, the concerned individual may not be aware of the information it took into account, how it processed this data or what effect it had on a decision. But if there is no meaningful transparency, this can have a positive effect on the vulnerability of providing the effective protection as guaranteed in Article 17 United Nations Human Rights Committee (1988).

3.3 The Right to Privacy in the Digital Age

Technological advances over the last several years have been accompanied by an increased focus by the United Nations on the need to revisit privacy concerns in this realm. The right to privacy in the "digital age" has been recognized in UN decisions, which state that human rights extend to the Internet, just as they do to physical space. In the context of AI, this principle is fundamental: changes in the technology will not detract from human-rights considerations of the conduct United Nations General Assembly (2013). The digital age privacy guidelines have highlighted issues like the droves of surveillance, wiretapping, metadata gathering, data storage and the profiling of communications. AI further exacerbates each of these challenges as AI systems can process information at a level and pace that was not possible prior to the advent of machine learning.

3.4 European Human-Rights Law

There is also the ECHR, where the protection of privacy is considered ‘is article 8.Another important source of international law for privacy protection, is provided by article 8 of the ECHR. It provides protection and respect for the private personal life and family life; home and correspondence. However interestingly ECHR allows interference exceptionally only where, as prescribed and allowed by law, and obligatory in a democratic society, for specified lawful purposes and legally permissible aims.

There is a substantial body of law under the European Court of Human Rights in the area of surveillance and personal data. Under the auspices of the European Court of Human Rights, there's quite a large amount of existing law about surveillance and personal data. For instance, the decisions of the European Court of Human Rights in cases of Roman Zakharov v. Russia, Klass and Others v. Germany, Big Brother Watch and Others v. United Kingdom and S and Marper v. United Kingdom, have shown that the protection of privacy also involves high-tech methods of surveillance and processing of personal data by governments. In S. and Marper the Court discussed the retention of fingerprints and DNA profiles and placed a priority on the protections which should be afforded where there is a concern with personal data. The case shows how privacy could be violated with the mere retention of information, not just the initial collection (*S. and Marper v. United Kingdom*, 2008, para. 103). The reasoning directly applies to AI. Collection of such information can last far longer than retention for the purpose of its original training. Such information may be retained by AI Systems well beyond the purpose for which it was collected in the first time. As a result, the retention and purpose limitation issues are of increasing importance.

4. AI-Driven Threats to Privacy

The affects of AI on the societies are unlimited and its potential impact is increasing with every passing day on the individual privacy. On one side AI is being used for positive aspects such as debate, negotiations, dialogue and trade whereas on the other side it’s negative use include cyber terrorism (Roumate, 2021) . AI has not only threatened the national and international security but also being used as weapon against individual privacy in some cases.

4.1 Mass Data Collection

Data is fundamental for the operation of AI systems. The more data there is in the overall system and the more varied, the more that can be done with it for analysis. This makes it easy for organizations to gather data for other uses beyond what's needed for the purpose at hand.

Mass collection can pose a threat to privacy because it can reduce users' real choices over understanding and controlling data about them. The problem is especially critical when data is gathered without any

intervention from the person or individuals working in the collection process, like mobile devices, connected objects, web pages, cameras, online platforms, etc. One possible answer to this is the principle of data minimization. Collecting information for the future − because it may be useful (be it or not) − is not enough. What should take precedence when designing an AI should be the need for the data to be used for the specific purpose intended?

4.2 AI Profiling and Inference

AI profiling poses a greater privacy problem. The conventional privacy framework tends to be reactive, pertaining to information that an individual is aware of giving up. With the help of AI, what may appear ordinary information can generate sensitive inferences. In fact, an algorithm can analyze data that covers location history, search data, purchasing habits and social networking, to logically determine health status, political affiliation or any other thing. If each individual piece of information alone might seem innocuous, it can combine to self-reveal some very personal traits. It is thus the transformation of data into knowledge, which harms privacy. There is no objective reason for International law to deny the existence of the generation of sensitive inferences, which itself may be an interference with private life. The modern system of AI can threaten the individual privacy by taking pictures of movement of individuals, particularly if they are anti government in case of dictatorship, by the government in case of human rights violations.

4.3 Facial Recognition

Face recognition is perhaps one of the most blatant examples of the invasion of privacy carried out by AI technologies. Faces can be captured by the camera and people unknown to the family can be seen as a familiar face by AI systems due to no interaction or consent.

The use of facial recognition in public environments offers the potential for perpetual facial ID in public places. Conventional surveillance can only monitor a many number of people through manual identification while the automatic recognition process the many number of people in real-time. The concern is especially severe not only because individuals ought to be free to go through a public area without, say, having their particular style of walking or gait gleaned from their footsteps, but also because they may reasonably expect to remain anonymous on their way to the job or to other appointments. A distinction between 'ordinary observation' and technologically enhanced surveillance which allows persistent identification should, therefore, be made in international human-rights instruments.

4.4 Generative AI and Personal Data

Generative AI raises new privacy issues. Although the generative AI is not a new concept yet the concerns about it with respect to privacy were raised in 2022 (García-Peñalvo & Vázquez-Ingelmo, 2023). The training of LLM and other BMs can take place with vast amounts of available public or private data. If personal data is contained in training datasets, the question of whether there has been legitimate collection, purpose limitation, storage and later release of data arises. Uddagiri and Isunuri (2024) claim that generative AI is posing risk to violate the personal information safeguard and a mechanism should be devised to devise an ecosystem that can not only gurantee the privacy of individual but also may place it at the top priority. Hence privacy law and anti-discriminatory law are trying to address the concerns due to generative AI (Xiang, 2024).

Personal information might also be generated or inferred by generative systems based on users' requests. So the question is: “should someone have the right to know if their information has been part of a model and the right to correct or remove it from the model?”The challenge of making changes to trained models does not negate the duty to safeguard privacy. Rather, it calls for designing systems in such a way that privacy considerations are taken into account before implementation.

4.5 Predictive Behaviour Technologies

Predictive models of individuals are becoming more common with the help of AI systems. Predictive models concerning individuals are becoming more and more common through the use of AI systems. These can include credit worthiness forecasts, suitability for work, likelihood of committing a crime, risk of health issues, or consumer behavior. The problem that arises when relying on predictive systems is that it is possible to influence a person not in relation to their actions, but with regard to what the system predicts the person will do. These systems might also be perpetuating history of discrimination. The structural inequalities in training data can lead an AI to learn and reinforce those patterns. This chimes with the themes of equality and non-discrimination and privacy. Muhlhoff (2021) points out that there are chances of “prediction gap” in the age of AI where a large data is analyzed to predict the behaviour of the individual and the privacy of the individual is also violated in the context of data protection.

4.6 Location and Behavioral Tracking

With the help of AI, location data can be used to map a full narrative of a person's daily routine. AI can interpret the location data and draw a comprehensive conclusion and image of what a person has been doing for much of the day. Patterns of location data can help describe a person's residence, occupation, places of religious worship, access to medical treatment, and the places they visit and engage in socializing. Although information at an individual location point may not be sensitive, extended aggregation may result in very sensitive information. This is a great example of how it is important that AI privacy regulation will take into account the aggregated impact of data processing and not the individual data at a time. Sadaf et. al. (2025) point out that reverse engineering is used in multiple applications to track location and behaviour. They emphasize that multiple steps may be taken such as transparent regulations, secured AI models and user permission to secure privacy of location and behavioral tracking.

5. Artificial Intelligence, Surveillance and Biometric Identification

The human rights problems posed by AI use by States is especially grave as the State also has coercive powers which private actors don't typically have. Police forces have the power to force a person's cooperation, obtain police records, and take legal action against a person.

As a result, AI powered surveillance can significantly augment the State's power. Facial recognition, automated license-plate recognition, predictive policing, social network analysis and big data analysis can enable governments to establish connections and patterns that would have otherwise demanded heavy manpower costs. While international human-rights law prohibits excessive surveillance, it does not rule out all forms of surveillance. States have legitimate interests in national security, in prevention of crime and public safety. There are two main issues for determination: surveillance measures are required to meet the criteria of legality, necessity and proportionality.

The European Court of Human Rights, in its numerous rulings on issues of surveillance, has repeatedly

emphasized the need to protect against the abuse of surveillance systems. In Roman Zakharov v. Russia, the Court considered the issue of secret surveillance and found that the court's legal architecture was overly lacking in guarantees against any arbitrary or manipulative use of it (*Roman Zakharov v. Russia*, 2015, para. 165).

This is a fundamental that is closely applicable to AI surveillance. The more sophisticated a surveillance system is, the more robust should be the safeguards. Governments should refuse to utilize AI systems when only because of technical availability. They should have a clearly demonstrated legitimate purpose, have a human rights impact assessment, minimize information gathering, have access restrictions, keep information, and have an independent supervising authority.

Biometric systems are systems that need specific examination as biometric identification is closely related to the physical identity of the person. Biometric characteristics can't be changed if compromised as easily as passwords can be. You can never change the face or fingerprint of a person, but you can change a password, which is why having a stolen password is a problem. Facial recognition should, therefore, be used with increased protections. The terms "narrowly targeted" and "indiscriminate" should be used to differentiate identification of individuals "narrowly" or "indiscriminately" based on the ground of reviewing an individual's conduct in light of judicial or legal criteria from the indiscriminate identification of all persons entering into a public space (Council of Europe, 2024, art. 10).

There is an overall human-rights perspective reflected in the Framework Convention of the Council of Europe which explicitly calls on Parties to ensure that AI activities do not contradict human rights and provide mechanisms for risk assessment and risk reduction. It is also important for its lifecycle, as human rights protection should be applied when developing through deployments, and then monitored.

6. AI, Private Corporations and Responsibility for Privacy

Corporations are developing the algorithms not only to monitor but in many cases to control the human decision that is leading towards a struggle between privacy of the individual, commercial interests and transparency (Lu, 2022). A major deficiency in conventional international human rights law is that it takes a State-centric approach. Though data brokers, advertising platforms, technology firms and AI developers may hold large amounts of personal data, they typically are not signatories to international human-rights treaties. This should not be an excuse for corporations to be non-existent in international human-rights law. The UN Guiding Principles on Business and Human Rights set out that businesses have the duty to respect human rights and shouldn't cause or be responsible for adverse impacts on the human rights of others (United Nations Office of the High Commissioner for Human Rights [OHCHR], 2011). Katyal (2019) points out that the world is over emphasizing over states' responsibility regarding privacy concerns over the use of AI algorithms states but in actual the private corporations' involvement and activities are increasing day by day hence the concerns about privacy and accountability are increased. So there is a dire need to focus the private corporations to address the issue of privacy in the context of AI.

The AI subject area needs to have these duties turned into real-world work. Developers building AI systems need to conduct privacy impact assessments, understand risks linked with training data, put in place processes to address requests for personal-data, and offer valuable transparency on their systems. Companies have a significant role when supplying AI systems to governments, especially with regard to corporate responsibility. The government should not be blamed for using the technology when it was a company who created or designed it, did further development or materially worked on its implementation.

A better plan would be to embrace a shared-ownership model. The Government of a country, state or region should be held responsible not only for the functioning of public companies, but also for ensuring that they do so in compliance with the human-rights obligations. Companies should have independent duties regarding the design, development and provision of AI systems. This is especially tricky in situations that are transnational. An AI company can establish a company in a first country, create an AI system based on the data of individuals from a second country and export the system to a third country to the government. Jurisdictional frameworks based on traditional notions of territorial jurisdiction may, therefore, cause a lack of clarity for individuals with respect to the ability to have a remedy. International action is therefore crucial to tackle cross-border issues of privacy harms arising from Artificial Intelligence.

7. International and Regional Legal Responses

7.1 Council of Europe Framework Convention

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024) is one of the most important developments in the international field of AI governance. Adoption took place on 17 May 2024 and it was opened for signatures on 5 September 2024. It is in fact the first international legally binding treaty on human-rights, democracy and the rule of law, specifically focused on AI, according to the Council of Europe.

The Convention is based on a lifecycle strategy. It does not just target specific applications but applies to the activities related to AI systems throughout their lifecycle. This is significant as there are opportunities for privacy issues to occur during data collection and model processing before the introduction of an AI system (Council of Europe, 2024, art. 10).

The Convention places focus upon privacy and protection of personal data as also part of human rights protection. This thereby reflects an advance from technology-centered regulation to one based on human rights government.

The main constraint to its operation is the geographical one and its institutional size-up. The Convention is financed for an international character and it is open for non-European States but its efficient implementation will rely on the ratification, implementation and enforcement of the Convention at national level.

Its significance goes beyond mere membership, however. It can shape the creation of globally agreed standards and laws, and serve as a common language for assessing AI systems.

7.2 Ethics of AI and Recommendations of UNESCO

In 2021, the 193 member States of UNESCO have accepted the Recommendation on the Ethics of Artificial Intelligence, which is one of the biggest global soft law tools. The document is not a treaty, so it doesn't include conventional binding obligations, but will offer norms to guide States as they establish AI governance frameworks

One of its concerns is privacy. The Recommendation encourages values, such as taking personal data protection, transparency, accountability and human rights seriously. It also promotes approach to privacy by design as well as impact assessments. The Recommendation has a special relevance to the countries beyond Europe given that UNESCO is a global community. It offers a mutually agreed basis that could

help developing States develop their national AI policies, aligned with the human-rights frameworks. The main drawback of it is that it is not enforceable. Implementation will to a very large extent be reliant on national governments. Yet, soft law instruments have an impact on the understanding and evolution of norms under international law, and can, over time, lead to customary law (UNESCO, 2021).

7.3 European Union as a Comparative Model

Although the European Union is a regional organization rather than a universal international-law institution, its regulatory framework provides an important comparative model. The General Data Protection Regulation (GDPR) provides extensive rules concerning personal-data processing, transparency, automated decision-making, data-subject rights and accountability. The EU Artificial Intelligence Act (AI Act) represents a further development by establishing a risk-based framework for AI systems. Its significance for international law lies partly in its extraterritorial influence. Global technology companies may modify their practices to comply with European requirements even where their activities extend beyond Europe. The EU experience demonstrates that AI regulation can combine privacy law, fundamental-rights protection and risk-based technological regulation. Fitriyah and Abdulvona (2024) claim that EU is one of the entities that has took the lead in making AI regulations to safeguard the privacy and human rights.

However, European regulation cannot simply be transplanted into the international system. States have different legal systems, technological capacities and institutional structures. International regulation must therefore establish minimum human-rights standards while permitting appropriate domestic implementation. Suleimanova (2024) states that legal initiatives of EU regarding the protection of human rights and privacy in the age of AI such as the Council of Europe's AI Convention and The EU Artificial Intelligence Act (AI Act) are unable to safeguard the privacy of the individual and human rights due to some deficiencies on one hand and because of existing gap between national security and private sector regulations on the other hand.

7.4 Regional Human-Rights Systems

Privacy protection also exists within other regional human-rights systems. John and Panachakel (2024) point out that different IEEE regions have developed their own AI policy landscape to safeguard the human rights and privacy of the individual in the age of AI. The American Convention on Human Rights protects privacy through Article 11, while the African human-rights system has increasingly addressed digital rights and data protection.

The diversity of regional approaches can contribute to the development of international standards. However, fragmented regional approaches may also create inconsistent levels of protection. A global AI privacy framework should therefore seek convergence around minimum principles rather than requiring identical regulatory systems.

8. Adequacy and Limitations of Existing International Law

It is not an easy task to secure data privacy, individual's privacy and human rights in the age of AI in modern era and it was not imagined ten years ago that AI would be involved and ingrained in our daily routine life. Moreover the development of Laws related to AI and International Law are not growing at the speed with which the AI development is growing. The proliferation and penetration of AI is known as "the power behind the throne" (Lu, 2022). The analysis shows that there is no full vacuity of the existing

international law, and at the same time its relevance and application are not completely exhausted. ICCPR, UDHR, many regional human-rights treaties and points of precedent permit protections of privacy from interference by AI.

The first has to do with the technology. Many current international instruments were created before the advent of AI. They are broadly worded, allowing for technological adaptation, but do not cover in detail examples such as training datasets, algorithmic inference, foundation models or generative AI.

The second restriction is related to transparency. Traditional legal remedies assume that individuals are able to see the interference that is going on around them. AI systems can make it challenging as decisions could rely on complex statistical relationships that may not be easily interpreted even by the operators of the system.

The third one is accountability. AI systems often have multiple players – from developers to data suppliers to deplorer's and end users. It can therefore be hard to determine who is at fault for a privacy violation.

The fourth restriction is the worldwide element of AI. Data can move across borders in virtually real-time. A single entity can be processed by artificial intelligence a company thousands of kilometers from there. There is a need to have more efficient cooperation and remedies according to international law in such cases.

The fifth is about private actors. Generally international human rights treaties bind States. States do have responsibilities for regulation of corporations, but there is fairly strong reliance on domestic law for enforcement against private companies.

Lastly, there is a remedy gap. An individual might find that an AI system has utilized his/her personal information without having a means in practice to identify the information that was used, to understand what that processing might have done, nor to be able to ask the AI system to delete the data. Procedural rights that can render substantive rights meaningful must therefore be granted to support the right to privacy.

9. Human-Rights-Based International Framework for AI and Privacy

Solove (2021) explains that privacy does not mean only rights to secrecy but it entails the autonomy of decision making by controlling the personal information. The scope of an international principle for privacy should be rooted in the fundamental human right of privacy, and not just an ancillary ethical issue.

Firstly, There should be a human right and privacy impact assessment of all major AI systems handling personally identifiable information. Categories of data processed, the purposes of their processing, the population that might be affected, risks of discrimination, surveillance risks and safeguards should be identified by the assessment.

Secondly, there needs to be legality, necessity and proportionality in the way AI systems are used. It is not acceptable that governments use or test AI-powered surveillance solely for ease of operation, rather than for a specific objective. It is essential that there is a well-defined legal objective and evidence that the interference is necessary to achieve a legitimate objective.

Third, privacy should be built-in from the start and it should be a default setting. Developers should minimize collection of user's personal data, implement appropriate security measures and not keep unnecessary data.

Fourth, individuals should have informative transparency and informational rights. If there are substantial impacts on a person's rights or interests, considering the use of AI, the person should be informed that AI was used and sufficient information should be provided to inform the person of the nature of the processing of the information.

Fifthly, there are effective mechanisms for access, correction and challenge. If there has been misinformation or non-legally produced information collection which has an impact on a person, then that person should be able to seek correction and challenge the use of information.

Sixth and last, high-risk AI systems should be monitored independently. Regulators should be able to carry out audits of systems, investigate complaints, impose sanctions, and demand corrective action.

Finally, biometric surveillance should have minimum protections under international law. For the potential of this to turn public space into a place where continuous, non-discriminatory and misdirected use of biometric identifiers is a possibility, it is imperative that these uses meet rigorous requirements.

Eighth, States need to make companies accountable. Helping technology companies to fulfil human-rights due diligence obligations, to keep adequate documentation on their processes, to evaluate their training datasets, and to assist in compliance with legislation.

Ninth, international cooperation is needed on cross-border AI processing. States should establish ways of cooperation between data protection authorities and human rights institutions and human rights courts.

Tenth, it is suggested that the international organizations encourage the capacity building in developing countries. No global 'privacy regime' can be working if advanced States alone are able to police it. Technical expertise, regulatory resources and access to independent auditing mechanisms are required in developing countries.

Last but not least, human oversight must be maintained over impactful decisions in an international framework of governance of AI (Council of Europe, 2024, art. 10). AI must be used where it fits, but must not be the substitute for humans' role in making pivotal decisions with considerable human impact on fundamental rights. The Framework Convention of the Council of Europe is an important basis for this approach as it addresses AI governance in linkage with human rights, democracy and the rule of law. AI governance can also be tailored around human rights, even at the global level, as shown by UNESCO's framework. The aim should not be to stifle technological development. Instead the international law should guarantee innovation in a structure that takes into account human dignity and individual autonomy (UNESCO, 2021).

10. Conclusion

AI is a paradigm-shift in the dynamics of person-to-person, person-to-information and person-to-power. Its ability to gather, merge, analyze and infer information offers great opportunities, but poses risks of interference to the right to privacy, which were never anticipated when the main international privacy instruments were drawn up. he AI governance by securing the privacy can be strengthen only by

developing privacy mechanism,adopting safeguarding principles, making data governance mechanism, promoting transparency through global cooperation.

Internationally, a right to privacy is an entrenched human-rights value. There are good bases in articles 12 of the UDHR, article 17 of the ICCPR, in regional instruments and judicial decisions covering more in detail the norms around surveillance and data retention/personal information. Thus, the legal framework is sufficiently broad to be applicable to AI. However, technological advances have brought tangible and ethical dilemmas. AI systems have the ability to create personal data from inferences, surveil over large-scale populations, analyze biometric data, create copies of personal data, make predictions about people, etc.

Therefore, this article's main argument is that the legal right to privacy is not a missing element, in fact, it exists; rather, the question is whether the current legal framework applies to fast-changing technologies of AI effectively.

The moment when the Council of the European Union's Framework Convention for the Protection of Human Rights, Democracy and the Rule of Law with AI is being discussed or created is relatively new, as it will provide an international legally binding framework specifically for the issue of AI and human rights laws. An additional global normative framework, the Recommendation of UNESCO, places a special focus on privacy, accountability, transparency and human rights (Council of Europe, 2024, art. 10). These developments are evidence that the international governance about AI is evolving towards a rights framework. But there is still the need for further development. International law ought to create more clarity regarding how AI is used for surveillance, biometric identification, profiling, automated decision making, the processing of training data and algorithmic inferences. States should mandate privacy/HR impact assessments, privacy by design, transparency, independent oversight, effective remedies. Further meaningful due diligence obligations on private companies on the question of human rights are necessary.

Tracking privacy in an AI era has to be considered more than simply the right to privacy of information. It is a right that guarantees a freedom from suffering and a freedom from being watched or manipulated unnecessarily by technology. It’s a right to have autonomy, dignity, and identity, freedom from the unnecessary observation or manipulation by technology. If artificial intelligence is allowed to anticipate what people are going to think, where they are going to go, and what they may do, privacy will be impossible to separate from freedom of human beings

International law needs, therefore, to shift from when it is already behind the times to become a preventative model where human rights are integrated from the start of the design, development and use of AI. Technology is not the only solution that should be considered when deciding on the future of AI governance. It must also be determined by what international human-rights law permits technology to do to human beings (UNESCO (2021).

Ethical use of AI can be one of the parameters through which the personal data usage may be safeguarded from misuse. Multi-pronged strategy may be adopted to achieve this objective.

References:

Billeh, Tareq Al, Ruba Hmaidan, Ali Al-Hammouri, Mohammed AL Makhmari (2024) The Risk of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards, Jurnal Media Hukum, Vol. 31, No.2, 333-350.

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Fitriyah, Aidatul and Daryna Dzemish Abdulovna (2024) 'EU's AI Regulation Approaches and Their Implication for Human Rights, Media Iuris Vol.7, No.3, 417-438.

García-Peñalvo., F. J. & A. Vázquez-Ingelmo (2023) What Do We Mean by GenAI? A Systematic Mapping of The Evolution, Trends, and Techniques Involved in Generative AI, INT'L J.INTERACTIVE MULTIMEDIA &A.I.7, 12.

Hasan Mahmudul (2025) Right to Privacy in Artificial Intelligence Legislations: Analyzing International Soft Law Frameworks, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi (İMHFD) Cilt: 10 - Sayı: 2 - Eylül.

John, A. M., & Panachakel, J. T. (2024, October). Navigating AI policy landscapes: Insights into human rights considerations across IEEE regions. In *2024 IEEE 12th Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 1-6). IEEE.

Katyal, Sonia K. (2019) Private Accountability in the Age of Artificial Intelligence, UCLA Law Review, 66, 54

Lu, S. (2022). Data privacy, human rights, and algorithmic opacity. *California Law Review*, *110*(6), 2087-2147.

Lubis, Muhammad Ikhsan (2016)'The Relationship of International Human Rights Law with Humanitarian Law in Situations of International Armed Conflicts', International International Journal of Indonesian Legal Studies , 1.1, 13-34.

Mühlhoff, R. (2021). Predictive privacy: towards an applied ethics of data analytics. *Ethics and Information Technology*, *23*(4), 675-690.

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

Rayhan, R., & Rayhan, S. (2023). AI and human rights: Balancing innovation and privacy in the digital age. *Comput. Sci. Eng*, *2*(353964), 10-13140.

Roumate Fatima (2021) Artificial Intelligence, Ethics and International Human Rights Law, International Review of Information Ethics, Vol.29, issue 03, 1-10.

S. and Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 50 (2008).

Sadaf, M., Naeem, A., Rehman, S. U., Sabir, T., Ali, Q., & Nishat, F. (2025, July). Unveiling Covert AI: Reverse Engineering Android Apps to Expose Behavioral Tracking. In *International Conference on Emerging Technologies and Intelligent Systems* (pp. 115-136). Cham: Springer Nature Switzerland.

Solove, Daniel J. (2021), Understanding Privacy, 2nd ed., Harvard University Press, Cambridge, MA, 13-39.

Suleimanova, S. (2024). Comparative Legal Analysis of the Role of Artificial Intelligence in Human Rights Protection: Prospects for Europe and the Middle East. *Pakistan journal of Criminology*, *16*(3), 907.

Uddagiri, C., & Isunuri, B. V. (2024). Ethical and privacy challenges of generative AI. In *Generative AI: Current trends and applications* (pp. 219-244). Singapore: Springer Nature Singapore.

United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations Human Rights Committee. (1988). *General comment No. 16: Article 17 (Right to privacy).* United Nations. https://www.refworld.org/legal/general/unchr/1988/en/38822

United Nations Office of the High Commissioner for Human Rights. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381137

United Nations. (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations General Assembly. (2013). *The right to privacy in the digital age* (A/RES/68/167). https://docs.un.org/en/A/RES/68/167

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

Xiang, A. (2024). Fairness & Privacy in an Age of Generative AI. *Science and Technology Law Review*, *25*(2), 288-312.

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