

Dr. Ahmed Mohamed Salah

Professor of Public International Law, Faculty of Law
Beni-Suef University

Human Rights in the Era of AI: Privacy, Discrimination, and What States and Corporations Do?

- **Correspondence:** Dr. Ahmed Mohamed Salah
Professor of Public International Law, Faculty of Law
Beni-Suef University.
- **DOI:** 10.54873/jolets.v5i1.219
- **E-mail:** ahmedelalfy274@gmail.com
- **Citation:** Ahmed Mohamed Salah
Human Rights in the Era of AI: Privacy, Discrimination,
and What States and Corporations Do?
Volume 05, Issue 01 April 2025

Abstract

»This paper examines the impact of Artificial Intelligence (AI) on human rights, with a particular focus on privacy and discrimination, alongside the responsibilities of states and corporate actors. As AI becomes increasingly integral to various aspects of life, it presents both significant opportunities and substantial risks. Key concerns include potential privacy violations and the emergence or exacerbation of algorithmic discrimination.

This study analyzes these impacts through the scope of international human rights law, investigating the corresponding obligations of states and companies to ensure the ethical and equitable development and deployment of AI systems. Employing a mixed-methods approach, this research integrates legal analysis, case studies, and policy reviews. The objective is to evaluate the effectiveness of existing regulatory frameworks, including the EU's Artificial Intelligence Act (AI Act), in addressing these challenges.

The potential for AI systems to perpetuate biases, infringe upon privacy rights, and introduce novel forms of discrimination underscores the necessity for robust governance measures. The research indicates that states have a critical responsibility to regulate AI technologies, while companies should adopt human rights-based approaches within their AI practices. Consequently, this study highlights the urgent need for international cooperation to establish clear legal and ethical frameworks to safeguard human rights in the era of AI.

Keywords: Artificial Intelligence (AI), Human Rights, AI Governance, EU Artificial Intelligence Act (AI Act) and International Human Rights Law.

Introduction

The rise of artificial intelligence (AI) has brought profound changes to our society. It affects how we interact, work, and live. AI brings many benefits, like boosting efficiency and improving decision-making. It also raises major concerns for human rights, especially about privacy and discrimination. AI systems can keep biases alive. This can cause unfair results and harm privacy rights. They often gather and use a lot of personal data without being clear or accountable.

There is a lot of research on AI and human rights. Still, we need a thorough look at how states and companies are tackling these issues. This matters a lot under international human rights law and new rules, like the EU's AI Act. Many discussions about AI focus on technology. They often miss the legal and ethical responsibilities of important people in protecting human rights.

1. Current Understanding and Gaps in the Literature

Current research shows key challenges of AI. These include amplifying existing biases, violating privacy, and lacking transparency in decision-making. The international human rights framework is now often used to tackle these challenges. It highlights the need for a comprehensive approach. This should include legal remedies, moral justification, and political analysis. We should look at how AI affects important human rights such as privacy and non-discrimination. We must consider how international law can hold states and companies accountable.

2. Significance of the Study

This study aims to contribute to the existing discourse by examining four critical aspects of the AI-human rights nexus:

I. Impacts of AI on Privacy: Exploring how AI collects and uses personal data, and what this means for privacy rights.

- II. AI and Discrimination: Examining how AI affects discrimination, especially for marginalized groups.**
- III. States and Corporations' Responsibility under International Human Rights Law.**
- IV. Obligations of the European Union Artificial Intelligence Act (AI Act): Understanding the EU's AI rules and their impact on human rights.**

3. Potential Contributions

This study has the potential to make a substantial contribution to the field by:

- Providing a detailed analysis of AI's impact on privacy and discrimination.
- Clarifying what states and corporations must do under international human rights law.
- Offering insights into the effectiveness of the EU AI Act in protecting human rights.

4. Method and Structure

The study will use a mixed-methods approach. It will combine legal analysis, case studies, and policy reviews.

The paper has five main sections:

- **An introduction**
- **A literature review**
- **An analysis of AI's impact on privacy and discrimination.**
- **A discussion on state and corporate responsibilities.**
- **A conclusion**

The conclusion discusses the findings and offers recommendations for future policy development.

This research looks at important issues. It aims to better understand how AI, human rights, and regulations relate to each other. The goal is to help create fairer AI technologies that respect rights.

1. Impacts of AI on privacy:

AI technologies have changed how we collect, process, and use personal data. This raises important concerns about privacy and human rights. AI systems now use a lot of personal information. This raises ethical concerns about their data handling. This is especially true when considering international human rights standards. This change requires us to examine current privacy rules in detail. We also need to create new ways to protect people's rights in the AI era.

Louis Brandeis defined privacy as a person's right to be left alone. It protects against unwanted sharing of personal facts, thoughts, and feelings⁽¹⁾. Many regional and international documents include this idea. The Charter of Fundamental Rights of the European Union (CFREU), the Universal Declaration of Human Rights (UDHR), and the American Convention on Human Rights are key documents. Article 12 of the ICCPR says everyone has a right to privacy. It highlights the need to protect personal information from unauthorized access.

However, the advent of Artificial Intelligence (AI) has intensified privacy challenges. AI systems collect large amounts of data. This can identify individuals and pose a serious threat to privacy. It's important to balance AI's usefulness with its intrusive nature to protect privacy. Data collection is crucial in all stages of AI system development: training, testing, evaluation, and deployment. Corporations often take advantage of this by collecting personal data. This data includes fingerprints, travel details, interactions, and medical

1- Warren, Samuel D., and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4, no. 5, Dec. 1890, p. 193.

reports. They then use AI to process and create profiles based on this information ⁽²⁾.

Moreover, the impact of AI on marginalized communities further complicates the privacy landscape. Bias in AI algorithms often comes from discriminatory data. This can result in unfair treatment of vulnerable groups in law enforcement, housing, and jobs. These biases weaken AI systems and increase existing inequalities. This raises worries about human rights, especially privacy and protection from discrimination. Big tech companies hold significant power, which can increase discrimination against vulnerable groups. ⁽³⁾

Companies like High Flyer Hedge Fund the owner of DeepSeek—and OpenAI Inc., among others, provide a diverse array of innovative services across the technology and investment sectors., which means they collect and keep a lot of data. This makes it harder to regulate them than smaller businesses. Often, organizations collect data for sorting, scoring, and ranking individuals without consent. Data rules, like the General Data Protection Regulation (GDPR), require data collectors to inform people and get their consent. But, AI systems work on their own, so it's hard to challenge data misuse. These large tech companies can collect and analyze huge amounts of data. This lets them influence and even control groups of people. This raises serious concerns about group privacy dynamics ⁽⁴⁾.

AI has also altered group privacy dynamics. Big data from vulnerable groups can cause social suppression and violate their privacy. China's social scoring system shows how data can control access to key services. This includes credit, housing, and jobs. Fears of "data exploitation" during COVID-19 highlight a broader privacy

2 - Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology*, vol. 30, no. 1, 2015, p.78.

3- Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, 2018, p.180.

4- SA, Jane, "Artificial Intelligence: A Threat to Privacy?", *Nirma University Law Journal*, vol. 8, no. 2, 2019, p. 33.

concern. These technologies can quickly and deeply change our societal norms ⁽⁵⁾.

The COVID-19 pandemic highlighted contact-tracing apps. It also raised concerns about data misuse. These apps often use AI and machine learning. They can collect data without users fully aware or in control of who sees it. This situation raised fears of data misuse in other AI applications. However, governments are working to implement legal solutions to address these risks ⁽⁶⁾.

AI algorithms play a crucial role in preserving or breaching privacy. The Google Spain case highlighted the importance of protecting privacy from AI data use. The CJEU's ruling, based on the Data Protection Directive, allows data subjects to correct, delete, or block data processing that breaks the rules. This judgment was a big step. It helps protect privacy from unchecked AI use by big companies. This legal case and the next rule focus on reducing risks and damages from the AI systems mentioned ⁽⁷⁾.

Subsequent EU case law has further emphasized privacy protection. The CJEU and ECJ have used the GDPR to create a safer environment for individuals. The Facebook case showed how important it is to safeguard privacy from new tech. It dealt with the collection of web-surfing data from non-users ⁽⁸⁾.

The recent TikTok case related to "TikTok Lite Rewards programme" showed how important privacy settings are for minors under the Digital Service Act (DSA). The EU's AI Act sets key rules on privacy. AI systems must maintain high data quality and integrity at every stage of their lifecycle. Recitals 27 and 69 detail this.

5- Scassa, Teresa, Jason Miller, and Kelly Bronson, "Privacy, Ethics, and Contact-Tracing Apps." *Vulnerable: The Law and Policy of COVID-19*, edited by Colleen M. Flood et al., University of Ottawa Press, 2020, p.4

6- Ibid.

7-Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

8-Case C-645/19 Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit, (June 15, 2021).

AI risks to privacy highlight the urgent need for a global data protection framework. Legal and cultural views on privacy vary. These differences can lead to more exploitation and surveillance. This is especially true in areas with weak regulations. Better privacy protections can build public trust in AI systems. They also ensure developers take responsibility. This way, everyone can enjoy the same level of protection, no matter where they are.

2. Impacts of AI on Discrimination:

AI is now key in many sectors. It affects decision-making and improves how operations run. The use of AI systems brings up serious issues about algorithmic discrimination. This happens when systems unfairly treat people because of traits like age, race, ethnicity, gender, or disability. This risk is especially high when AI systems learn from bad or unrepresentative data. This can lead to results that mirror human biases.

For instance, AI-driven predictive policing systems have faced criticism for perpetuating racial bias. A 2016 study by ProPublica found that an AI system in the U.S. justice system labeled black defendants as future criminals twice as often as white defendants⁽⁹⁾. This example illustrates how biased data can lead to discriminatory outcomes.

The application of international human rights law to AI systems presents several challenges. There are clear concerns about workers' rights. AI is changing the job market and altering what employers want. This could result in layoffs and less job security. Privacy issues arise from using AI in data processing. This raises questions about informed consent and data protection rights. AI systems are complex. This makes it tough to find out who is responsible when harm occurs⁽¹⁰⁾.

9- Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

10- Canales, Maria Paz, Ian Barber, and Jacqueline Rowe, "What Would a Human Rights-Based Approach to AI Governance Look Like?" Carnegie Council for Ethics in International Affairs, Global partners digitals, 19 Sept. 2023. Available

United States like Colorado and Illinois are making new laws. They are responding to worries about AI discrimination. These laws aim to control the use of AI in hiring and job settings. These laws tell businesses using AI for hiring to be clear, handle risks, and be accountable. For instance, Colorado's AI Act says employers must inform consumers when they use an AI system. The state's attorney general will enforce this rule. We can tackle these challenges with laws and rules. This may help reduce the negative effects of algorithmic discrimination. It can also support fairer use of AI technologies in society⁽¹¹⁾.

AI discrimination can manifest as over- or under-representation of certain groups. AI can cause biased predictions based on race. It can also lead to discrimination against women. There's unequal targeted advertising too. Plus, linguistic minorities may face discrimination in translation or education⁽¹²⁾. Also, AI can worsen social inequality. For example, people in high-crime areas often pay more for insurance. This is due to the perceived risk.

A recent case highlighting these concerns is the Schufa case⁽¹³⁾. The CJEU ruled that Schufa's AI credit scoring process can greatly affect people. It uses personal data to profile individuals. This can result in significant legal and economic effects, such as loan denials. This decision emphasizes the importance of non-discrimination principles in automated decision-making. The GDPR says that organisations using these systems must have safeguards. This helps prevent discrimination and ensures decisions are fair and justifiable.

at: www.gp-digital.org/what-would-a-human-rights-based-approach-to-ai-governance-look-like/.

11- Melissa McNeilly, The Human Rights Risks of Artificial Intelligence (AI), New Tactics in Human rights, July 24, 2023. Available at: <https://www.newtactics.org/perspectives/human-rights-risks-artificial-intelligence-ai/>

12-Shabani, Sanaz, and Niki Jabbari. "The Impacts of Technology on the Human Rights of Linguistic Minorities." *Specialusis Ugdymas/Special Education*, vol. 1, no. 43, 2022, p. 3216.

13-Case C-634/21, Court of Justice of the European Union, 7 Dec. 2023.

3. States and Corporates responsibility under International Human Rights Law Concerning Artificial Intelligence:

Both States and corporations share a key duty to protect and preserve human rights. The Universal Declaration of Human Rights (UDHR) is key to State responsibility. It lists rights and states that countries must respect, protect, and fulfil these human rights as their main duty. The ‘Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights’ outline important corporate duties. They require businesses to respect, protect, and provide remedies within set frameworks⁽¹⁴⁾.

One party’s responsibility cannot override the others. Principle I of the Norms makes this clear. It states that States have the main duty to uphold human rights. The same principle keeps corporate responsibility to their own areas of activity and influence. This builds a supportive connection between state duties and corporate responsibilities, not a substitute⁽¹⁵⁾.

In the field of artificial intelligence (AI), international human rights law clearly holds both States and companies responsible. They must ensure that AI systems are used in ways that respect human rights. States and corporations must follow any general responsibilities and accountability frameworks related to AI. This is especially important due to the lack of specific international rules in this area. Many international agreements set rules for protecting human rights. However, there is still little specific guidance on how to protect these rights when using AI.

A complete review of human rights obligations for States and companies would be quite detailed. However, two key documents outline these responsibilities. Many other conventions cover different parts of human rights. Applying them to AI needs careful thought about each rule. This document examines certain norms that focus

14-United Nations, Sub-Commission on the Promotion and Protection of Human Rights, E/CN.4/Sub.2/2003/12/Rev.2.

15-Ibid.

on human rights and AI. Obligations may change depending on the situation and the people involved. However, we can find general principles in the existing literature.

Many documents discuss AI's impact on human rights. They also cover other topics.

Key examples are:

- **General Comments on the Right to Science**
 - **General Data Protection Regulation (GDPR)**
 - **UN High Commissioner for Human Rights' report on the right to privacy in the digital age.**
1. **General Comments on the Right to Science** ⁽¹⁶⁾: Part 3 states that States have positive and negative duties. Everyone should allow themselves to take part in science. They must enjoy scientific progress and benefit from it, without discrimination. Complementing these are five interrelated elements: availability, accessibility, quality, acceptability, and protection. AI is included in this entitlement because of Section E of Part 5. This section defines artificial intelligence as an emerging technology based on scientific knowledge.

So, it falls under the scope of this declaration. States have specific obligations. They must adopt policies and measures. These should expand the benefits of new technologies. At the same time, they need to reduce the risks involved.” States also have detailed tasks. They must encourage international cooperation. They need to decide how to develop and use these technologies while respecting human rights. They should ensure non-state actors follow human rights due dili-

16-(E/C.12/GC/25) (General comment No. 25 (2020) on article 15: science and economic, social and cultural rights).

gence. Additionally, they must pay special attention to issues like long-term job loss and data ownership.

2. **General Data Protection Regulation (GDPR):** The GDPR focuses on privacy and data protection. It also has important rules about automated decision-making. Article 22 bans unauthorized processing and profiling. This applies if it legally affects individuals or significantly impacts them. The GDPR is a major step forward in AI regulation. It has strict rules. Businesses that don't follow them face clear penalties, like fines, when developing AI. Responsibility under Article 22 begins when automated decision-making leads to legal effects or other major impacts. Recital 71 and the Article 29 Working Party's 2018 Opinion impact civil and political rights.

These rights include:

- The freedom to associate.
- The right to vote.
- Choices about immigration or citizenship.
- Protection against job denials that cause serious disadvantages.

Effects that trigger Article 22 often affect a person's legal or contractual rights. They often come from exploiting vulnerability or disadvantage. So, corporations must take responsibility for AI decisions that affect human rights. They also need to follow GDPR rules in these cases⁽¹⁷⁾.

3. **UN High Commissioner for Human Rights Report on The Right to Privacy in The Digital Age⁽¹⁸⁾:** This report outlines

17-Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev. 01, adopted on 3 October 2017/21-22.

18-(A/HRC/39/29). <https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commission->

what states and companies must do to protect privacy. States must protect the right to privacy in the digital age. This includes putting in place proper safeguards and ensuring strong oversight. The latter includes setting up a framework to prevent undue interference. It also offers rules and checks for surveillance and communication interception, as shown in Part Four.

Part Five covers corporate duties related to the “responsibility to protect.”

Corporations must: (a) avoid causing harm; (b) not add to harm, either directly or through others, like governments or businesses; and (c) help stop or lessen any negative human rights impacts linked to their operations, products, or services, even if they don’t contribute directly ⁽¹⁹⁾.

While based on the UN Guiding Principles on Business and Human Rights (UNGPs), successful implementation also needs to consider digital rights. Furthermore, the responsibility to provide remedy is obligatory for both groups.

II. Directly Relevant International Instruments Concerning AI and Human Rights:

Secondly, a limited number of international documents specifically establish rules regarding artificial intelligence.

Key documents include:

- The Toronto Declaration: Safeguarding Equality and Non-Discrimination in Machine Learning Systems.
- The OECD Recommendation on Artificial Intelligence.

[er-human](#)

19-“The corporate responsibility to respect human rights: an interpretive guide”, OHCHR, (2012).

- UNESCO's Recommendation on the Ethics of Artificial Intelligence.
 - The Ethics Guidelines for Trustworthy AI.
 - The EU AI Act.
 - The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law.
1. Toronto Declaration: This declaration seeks to boost inclusion, diversity, and equity while protecting equality.

States and corporations work together to:

- prevent discrimination,
- follow human rights laws and standards,
- protect marginalized groups.

Specific responsibilities are outlined for each:

- State Responsibilities: States must maintain updated regulatory systems and consider potential risks. Where harm occurs, States must provide effective remediation and redress. They must carry out regular assessments, audits, and tests. This helps them spot risks and reduce harmful outcomes. States must ensure accountability and require maximum transparency. This means systems should be clear and easy to understand. We must avoid “black box systems” that resist real accountability and transparency. They need to adopt diverse hiring policies. Also, they should provide human rights training for the right authorities. Then, they must set up independent oversight systems. States should create regulations that respect human rights. This will help

monitor the private sector, following the UN Committee on Economic, Social and Cultural Rights' comments ⁽²⁰⁾.

- Corporate Responsibilities: These involve respecting human rights on their own. They also include following human rights due diligence (HRDD) frameworks.

HRDD has three main parts:

- Identifying possible discriminatory outcomes.
 - Taking action to prevent and reduce discrimination.
 - Tracking responses and being open about these efforts.

Corporations should make sure that people and groups can get real and effective solutions.

1. OECD Recommendation: This aims to boost AI innovation and protect human rights. It urges global stakeholders to use AI responsibly for human rights. They should also set up the right mechanisms and safeguards. Other principles are transparency and responsible disclosure. This means allowing those harmed by an AI system to challenge its results. Actors must ensure traceability to analyse AI system outcomes and respond to inquiries. They should also use a systematic risk management approach. This approach addresses risks such as privacy violations and bias. Actors are responsible for ensuring that systems related to human rights work properly. Principles focus on States, encouraging them to invest in and support a fair AI environment. They also promote cooperation among States and other actors on AI issues. This aims to balance tech progress with labour rights ⁽²¹⁾.

2. UNESCO Recommendation: This document addresses val-

20-(E/C.12/GC/20, par. 11).

21-(OECD/LEGAL/0449).

ues and principles for AI use. It focuses on ethical issues but requires States to protect and respect human rights. This includes promoting dignity, equality, diversity, inclusiveness, peace, justice, and fairness. States must follow human rights laws in their actions. Key principles highlight important human rights obligations. These include doing risk assessments and taking steps to prevent harm to human rights. AI actors should promote social justice and ensure fairness. They must follow international law and protect privacy. This can be done through governance, impact assessments, design methods, and legal consistency. It recognises that AI systems can have ethical and legal responsibility, like for remedy purposes. However, it also states that ultimate human responsibility and accountability cannot be replaced. Transparency is key for challenging possible infringing outcomes. It also connects to explainability, which helps us understand and trace results. Responsibility and accountability are highlighted for States and other actors, including corporations ⁽²²⁾.

3. Ethics Guidelines for Trustworthy AI: These rules help protect human rights when using AI. They are similar to the UNESCO Recommendation. They clearly show the link between ethics and human rights.

They say, “Respecting basic rights in democracy and the rule of law helps us find ethical values for AI.” The five key rights for trustworthy AI are:

- Respect for human dignity
 - Freedom of the individual
 - Respect for democracy
 - Justice and the rule of law

22-(SHS/BIO/PI/2021/1)

- Equality, non-discrimination, and solidarity⁽²³⁾.

1. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law sets rules for states and companies⁽²⁴⁾. These rules aim to protect human rights as States need to make strong laws and rules. These should ensure AI systems respect human rights, democracy, and the rule of law. This includes mandating transparency, accountability, and fairness in AI development and deployment. Private actors must follow these rules. They should conduct thorough human rights impact assessments. They must ensure ethical AI practices and maintain strong oversight mechanisms. States and private actors must work together. AI technologies should not violate basic rights. These include privacy, freedom of expression, and non-discrimination. This will help create a safe and fair digital environment.

4. Obligations under the European Union Artificial Intelligence Act (AI Act)

The European Union's Artificial Intelligence Act (AI Act) is a key regulatory framework. It stands out mainly because it uses a risk-based approach to classify AI systems. This methodology categorises systems based on the potential risks they pose. So, certain duties apply to key players like providers, deployers, importers, and distributors. These rely on how the system is classified. They need safety, trust, and human-focused rules to comply.

I. Prohibited AI Practices (Unacceptable Risk):

The Act names a group of AI systems that are seen as having an “unacceptable risk.” These systems are banned from the EU market.
23- (Ethics Guidelines, p. 9).

24- Council of Europe. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. CETS No. 224. Adopted 17 May 2024. Council of Europe Treaty Office, www.coe.int/en/web/conventions/full-list?-module=treaty-detail&treaty-num=224.

Article 5 lists prohibited practices, including:

- Social scoring systems used by public authorities.
 - Untargeted scraping of facial images to create databases.
 - Real-time biometric ID systems can be used in public for law enforcement. There are some exceptions.
 - Emotion recognition systems in workplaces and schools, unless needed for safety or health reasons.
- **High-Risk AI Systems:**

A significant portion of the Act's regulatory focus targets “high-risk” AI systems. Experts identify these systems as a major risk to the health, safety, or rights of individuals. You can do this through Annex III listing or their inherent function. This category has strict rules. It needs thorough actions to guarantee safe and compliant use. High-risk AI system providers must comply with the AI Act and all related Union and national laws.

The main duties for high-risk systems are mainly found in Articles 9 to 15. These articles are in Chapter 2 of Title III of the Act.

These mandatory requirements include:

- Setting up strong risk management systems.
- Using strict data governance practices.
- Creating and keeping detailed technical documentation.
- Having automatic record-keeping (logging) features.
- Ensuring transparency and sharing information with users.
- Supporting effective human oversight.
- Achieving the right levels of accuracy, robustness, and cybersecurity.

▪ **General-Purpose AI Models (GPAI) and Systemic Risk:**

The AI Act focuses on General-Purpose AI (GPAI) models. It highlights those that could pose “systemic risks.” These models may face extra obligations. These could overlap with or add to the rules for high-risk systems. GPAI models are seen as risky when the total computation for training goes over a certain limit. These models can be risky on their own or when used in other AI systems.

To mitigate these risks, providers of GPAI models with systemic risk face specific obligations.

Here are the tasks:

- Keep technical documentation updated.
- Provide essential information to downstream providers who want to integrate the GPAI model.
- Conduct thorough model evaluations using standard protocols.
- Implement strong risk assessment and mitigation strategies.
- Ensure good cybersecurity protection.

Also, it’s important to follow Union copyright law. This is especially true for being clear about the content used to train the model.

▪ **Transparency and Human Oversight:**

The Act has rules that create a safe space for people to interact with AI. It also strengthens human control. The transparency obligation is central to this aim. AI systems that interact with people, create synthetic content (like “deepfakes”), or use biometric classification and emotion recognition need to follow clear transparency rules. Users must typically be informed when they are interacting with an AI system, and appropriate disclosures regarding the system’s nature and data processing must be made. The AI Act highlights

the need for human control and agency over AI systems. High-risk AI systems must be designed for effective human oversight. This means humans should be able to intervene or override system decisions when needed.

▪ **Accountability and Liability:**

The AI Act makes accountability clear and improves liability rules to ensure effectiveness. Providers, deployers, and others must be responsible for the systems they sell or use. This includes how they deploy them and their results. This means following the Act's rules. Non-compliant AI systems can cause legal issues under Union or national law if they harm someone.

Disclaimer: This summary is based on the provided text and general knowledge of the AI Act. To get accurate legal details and specific duties, check the official Regulation text.

Conclusion:

This research explores the link between the rise of Artificial Intelligence (AI) and the protection of basic human rights. It especially highlights privacy and non-discrimination. As AI systems play a larger role in our lives, we must consider the roles of governments and companies. They have a responsibility to guide how AI affects individuals and society.

Our analysis shows that AI technologies pose a real threat to privacy. They change how data is collected and processed, and current rules can't keep up. Large data harvesting and algorithmic profiling can harm marginalized communities. Biased data processing and complex privacy issues make this worse. There's a clear need for strong safeguards, transparency, and user control. This is especially important because of the power of big tech companies. Judicial cases such as Google Spain and Facebook under GDPR, plus new rules like the EU AI Act, are key steps forward. But, since AI is global, we need wider, standard ways to protect data.

Furthermore, the findings underscore the persistent risk of algorithmic discrimination. AI systems often learn from biased or unrepresentative data. This can worsen existing societal biases. This leads to unfair results in key areas such as jobs, credit scoring (like the Schufa case), and law enforcement. New laws are starting to appear in some areas. To tackle this issue, we need to take action. This means finding and reducing bias, making clear decisions, and holding people responsible for unfair results.

States and corporations play different but connected roles in international human rights law. States hold the main responsibility to respect, protect, and fulfill human rights. This includes overseeing AI development and use in their areas. As international AI treaties are still in the works, many guidelines are emerging. These include interpretations of rights like the right to science and privacy. Recommendations from groups like the OECD and UNESCO also play a role. Ethical guidelines and the Council of Europe's Framework Convention set clear expectations for everyone. They stress important principles such as legality, necessity, proportionality, transparency, accountability, and non-discrimination.

The EU's AI Act is a key effort to implement these responsibilities. It uses a detailed, risk-based regulatory framework. However, it focuses primarily on the region. It bans risky practices and has strict rules for high-risk systems.

These rules focus on important areas:

- Data governance
- Risk management
- Human oversight
- Transparency
- Accuracy

- Cybersecurity

It also sets clear duties for General-Purpose AI models and stresses accountability. This could serve as a guide for creating AI governance that respects rights.

These findings highlight a critical juncture. AI has great potential, but its current path threatens basic rights. It often moves faster than our legal and ethical protections. There is a gap between fast tech growth and how well current human rights laws and regulations can adapt. Thus, ensuring AI serves humanity requires a concerted, multi-stakeholder effort. States should create and enforce flexible, human rights-focused rules. Corporations need to include ethical principles and HRDD throughout the AI process. Also, countries must work together to tackle the global nature of AI. Building an AI ecosystem that supports human rights is not a tech or legal issue. Must for creating fair and societies in our digital world.

References

Books, Articles, and Reports:

- 1- Canales, M. P., Barber, I., & Rowe, J. (2023, September 19). *What would a human rights-based approach to AI governance look like?* Carnegie Council for Ethics in International Affairs, Global Partners Digital. <https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-ai-governance-look-like/>
- 2- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- 3- McNeilly, M. (2023, July 24). *The human rights risks of artificial intelligence (AI)*. New Tactics in Human Rights. <https://www.newtactics.org/perspectives/human-rights-risks-artificial-intelligence-ai/>
- 4- SA, J. (2019). Artificial intelligence: A threat to privacy? *Nirma University Law Journal*, 8(2).
- 5- Scassa, T., Flood, C. M., & others. (2020). Privacy, ethics, and contact-tracing apps. In C. M. Flood et al. (Eds.), *Vulnerable: The law and policy of COVID-19* (pp. xx–xx). University of Ottawa Press.
- 6- Shabani, S., & Jabbari, N. (2022). The impacts of technology on the human rights of linguistic minorities. *Specialusis Ugdymas / Special Education*, 1(43).
- 7- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. <https://doi.org/10.2307/1321160>
- 8- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>

Cases:

- 1- **Court of Justice of the European Union. (2014, May 13).** *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12).*
- 2- **Court of Justice of the European Union. (2023, December 7).** *SCHUFA Holding AG (Scoring) (Case C-634/21).*
- 3- **Court of Justice of the European Union. (2021, June 15).** *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit (Case C-645/19).*

International Instruments, Declarations, and Guidelines:

- 1- **Article 29 Data Protection Working Party. (2017, October 3).** *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 rev. 01).*
- 2- **Council of Europe. (2024, May 17).** *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 224).* Council of Europe Treaty Office. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>
- 3- **European Commission, High-Level Expert Group on AI. (2019).** *Ethics guidelines for trustworthy AI.*
- 4- **Office of the United Nations High Commissioner for Human Rights (OHCHR). (2012).** *The corporate responsibility to respect human rights: An interpretive guide.*
- 5- **Organisation for Economic Co-operation and Development (OECD). (2019).** *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449).*
- 6- **UNESCO. (2021).** *Recommendation on the ethics of artificial intelligence (SHS/BIO/PI/2021/1).*
- 7- **United Nations, Committee on Economic, Social and Cultural Rights. (2020).** *General Comment No.*

- 25 (2020) on science and economic, social and cultural rights (Article 15) (E/C.12/GC/25).
- 8- **United Nations High Commissioner for Human Rights. (2018).** *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights* (A/HRC/39/29). <https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-human>
- 9- **United Nations, Sub-Commission on the Promotion and Protection of Human Rights. (2003).** *Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights* (E/CN.4/Sub.2/2003/12/Rev.2).