ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Research Report

# EFFECTS OF ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS KOSOVO CASE

November 2024

**Publisher:** Institute for Technology and Society (ITS) in cooperation with Metamorphosis Foundation for Internet and Society

**Author:** Atdhe Lila – ITS

**Editor:** Mila Josifovska Danilovska - Metamorphosis Foundation for Internet and Society

**Financed by**: Western Balkans Fund (WBF)

Prishtina, 2024

The views expressed in this research are those of the authors and do not necessarily reflect the views of the Institute for Technology and Society, the Metamorphosis Foundation, or the Western Balkans Fund.

**Supported by:**

Institute for Technology and Society
Str. Zenel Salihu no. 28 Prishtina
https://institutets.com/

# Table of Contents

# Acronyms

AI - Artificial Intelligence

AIP - Agency for Information and Privacy

AIS - Agency for Information Society

ASYCUDA - Automated System for Customs Data

BIRN - Balkan Investigative Reporting Network

CCTV - Closed-Circuit Television

CEDAW - Convention on the Elimination of All Forms of Discrimination Against Women

CSA - Cyber Security Agency

CSOs - Civil Society Organizations

DPIA - Data Protection Impact Assessment

DSA - Digital Services Act

DTC - Digital Transformation Commission

EDPB - European Data Protection Board

EU - European Union

GDPR - General Data Protection Regulation

GIZ - German Society for International Cooperation

ICK - Innovation Center Kosovo

IMC - Independent Media Commission

ITS - Institute for Technology and Society

JIC - Jakova Innovation Center

KFOS - Kosovo Foundation for Open Society

KJA - Kosovo Journalists Association

NDI - National Democratic Institute

NGO - Non-Governmental Organization

NIS - Network and Information Systems

NIS2 Directive - Network and Information Security Directive 2

ODK - Open Data Kosovo

OES - Operators of Essential Services

RIT Kosovo - Rochester Institute of Technology Kosovo

SMEs - Small and Medium-Sized Enterprises

SMIL - Information System for Case Management

STIKK - Kosovo ICT Association

TAK - Tax Administration of Kosovo

UBT - University for Business and Technology (Kosovo)

UNDP - United Nations Development Programme

UNMIK - United Nations Interim Administration Mission in Kosovo

USAID - United States Agency for International Development

# Executive Summary

This paper, *The Effects of Artificial Intelligence on Human Rights: Kosovo Study Case*, explores the profound and evolving impact of Artificial Intelligence (AI) on **fundamental human rights**, particularly focusing on the **right to privacy, freedom of expression, and non-discrimination** within the context of Kosovo. As AI technologies become more embedded in daily life and governance, understanding their implications on human rights is essential for developing appropriate policies and safeguards.

The study begins by examining the global trends in AI development and their relevance to Kosovo, a country with a nascent AI landscape but a growing digital infrastructure. While AI holds tremendous potential for **economic growth and innovation**, it also presents significant risks, especially in societies with limited legal frameworks to regulate its use. The research highlights the particular vulnerabilities Kosovo faces due to its underdeveloped AI regulatory mechanisms and institutional capacity.

Key research questions addressed in this paper include:

- How AI affects human rights in Kosovo, particularly in relation to privacy, freedom of expression, and non-discrimination.
- What legal and policy measures are currently in place in Kosovo to address the challenges posed by AI, and how they compare to international standards.
- The current state of the AI ecosystem in Kosovo, including key technologies, stakeholders, and sectors utilizing AI.
- The level of preparedness among key stakeholders, such as government institutions, the private sector, civil society, and academia, in managing AI's ethical and societal implications.

Findings from secondary research, stakeholder interviews and surveys conducted with key actors and the general public reveal significant **gaps in awareness, preparedness, and regulation** regarding AI technologies. While there is high awareness of AI among the general public, the understanding of its implications remains superficial, often limited to generative AI tools like ChatGPT. Public institutions, meanwhile, lack the expertise and resources to effectively regulate AI or ensure its ethical application, leaving the door open to potential abuses in areas like surveillance, privacy violations, censorship and discriminatory practices.

The paper also identifies several opportunities for improving Kosovo's AI readiness. These include developing a comprehensive **AI governance framework**, aligning with **European Union standards**, and increasing investment in **capacity-building** for public institutions, the private sector, and civil society. The role of **international organizations** and **donors** is also highlighted as instrumental in driving AI-related reforms in Kosovo. Their support not only provides funding but also offers expertise and strategic guidance, helping Kosovo to align with global standards and accelerate its digital transformation.

The paper concludes with **policy and regulatory recommendations** aimed at ensuring AI technologies are implemented in a manner that upholds human rights, promotes accountability, and safeguards against misuse. The recommendations call for the development of clear legal frameworks, public awareness campaigns, and stakeholder collaboration to promote responsible AI use.

By providing an in-depth analysis of the AI landscape in Kosovo, this paper aims to spark meaningful dialogue among policymakers, industry leaders, civil society, and the public on the urgent need for AI regulation to protect fundamental human rights in the digital age

## Key Findings & Recommendations

### Key Findings

1. Kosovo is in the early stages of AI development, lacking a dedicated AI law, strategy, or governance bodies, which leaves a significant regulatory vacuum.
2. Existing laws, such as those on data protection and digital services, do not directly address the challenges posed by AI, including algorithmic accountability, ethical standards, and human rights implications.
3. The increasing use of AI systems poses risks to privacy, freedom of expression, and non-discrimination, particularly in sectors like healthcare, education, and justice.
4. Public institutions lack the expertise and infrastructure to effectively regulate or implement AI systems, which increases the risk of misuse or inefficiency.
5. Awareness of AI's societal and ethical implications remains low among public institutions, private sector actors, and civil society, hindering responsible AI adoption.
6. AI presents significant opportunities for economic growth, innovation, and modernization of public services, provided governance frameworks are established.
7. Kosovo can benefit from aligning with EU standards, such as the AI Act, Digital Services Act, and related frameworks, to ensure harmonized and effective AI governance.
8. Academic institutions and civil society organizations in Kosovo are underutilized in AI governance, despite their potential to contribute through research, policy advocacy, and public education.
9. Effective AI governance requires the involvement of diverse stakeholders, including public institutions, private companies, academia, and civil society.
10. Kosovo’s ongoing digitization efforts make it imperative to address AI governance proactively to ensure ethical and human-centered technology deployment.

### Key Recommendations

1. Develop a legal and strategic framework to address AI governance, ensuring alignment with EU standards while tailoring provisions to Kosovo's needs.

2. Create an advisory body to provide guidance on ethical AI deployment during the interim period before formal legislation and governance bodies are established.
3. Invest in training public officials, judiciary members, and law enforcement on AI-related topics such as data protection, algorithmic bias, and ethical governance.
4. Require public institutions to perform impact assessments before deploying AI systems, particularly in high-risk areas like surveillance, healthcare, and law enforcement.
5. Encourage companies to adopt transparent and ethical AI practices, offering incentives for SMEs to integrate AI responsibly.
6. Expand university curricula to include AI ethics, law, and governance, and fund research on AI's societal impacts.
7. Launch campaigns to educate citizens about AI technologies, their risks, and benefits, focusing on data privacy and algorithmic accountability.
8. Involve government, private sector, academia, and civil society in drafting AI policies to ensure inclusivity and transparency.
9. Implement regulatory sandboxes to test AI systems in controlled environments and identify potential challenges in governance frameworks.
10. Collaborate with the EU, international organizations, and neighboring countries to align AI governance with global best practices and secure funding for research and capacity building.

# Chapter I: Introduction

Throughout history, pivotal moments have significantly altered the course of civilization. One such moment was the cognitive leap millions of years ago, which led to the development of greater cognitive abilities and eventually gave rise to language and culture. Later, the Agricultural, Industrial, and Information Revolutions each brought profound advancements, but also introduced new ethical challenges and societal issues.

These revolutions have unfolded at an increasingly rapid pace—the Agricultural Revolution took millennia to develop fully, the Industrial Revolution spanned a few centuries, and the Information Revolution has transformed society in just a few decades. Now, we stand on the brink of another transformative period—the AI Revolution—which is evolving at an unprecedented speed.

AI promises to enhance various aspects of life, from healthcare to governance, through increased efficiency and automation. However, the accelerated pace of AI development, driven by advancements in computing power and data, magnifies its impact and poses significant risks, such as job displacement, privacy concerns, and algorithmic bias. This swift progression underscores the urgency of developing robust governance frameworks to address these challenges and ensure that society is prepared to harness the benefits of AI while mitigating its potential harms.

## Understanding AI

Before exploring the profound implications of the AI revolution, it is crucial to define what AI is. AI refers to systems designed to perform tasks that typically require human intelligence. These systems analyze their environment and make decisions to achieve specific goals, similar to how humans solve problems. As AI researcher Stuart Russell defines it, AI involves 'intelligent agents' that perceive their surroundings and act in ways that maximize their chances of success. [1] Expanding on this, Nick Bostrom describes AI as "*anything that performs tasks which, when performed by a human, would require intelligence.*" [2] This broad definition covers AI's range from simple data processing to complex autonomous systems.

While AI might seem like a recent phenomenon, the concept and development of AI have been around for decades. However, the progress in AI was relatively slow in its early stages, primarily due to technological limitations. It is only in the past few years that AI development has accelerated rapidly, driven by advances in computing power, availability of large datasets, and breakthroughs in machine learning techniques.

AI's development began in 1956 at the Dartmouth Conference, where researchers laid its foundational principles. [3] The 1960s saw the creation of ELIZA, one of the first chatbots, marking

[1] *World Economic Forum, What is AI? Stuart Russell Explains, 2022. Available at: https://www.weforum.org/agenda/2022/06/what-is-ai-stuart-russell-expert-explains-video/.*

[2] *Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies. Oxford University Press, 2014.*

[3] *AI Tools Explorer, The Dartmouth Conference: The Event That Shaped AI Research. Available at: https://aitoolsexplorer.com/ai-history/the-dartmouth-conference-the-event-that-shaped-ai-research/.*

an early step in natural language processing.[4] In subsequent decades, AI progressed steadily. IBM's Deep Blue made headlines in 1997 by defeating chess champion Garry Kasparov, and in 2011, IBM's Watson won Jeopardy! showcasing AI's real-time processing capabilities. [5]

Recently, AI's capabilities have expanded rapidly. In 2016, Google DeepMind's AlphaGo defeated the world champion Go player, illustrating AI's advanced strategic thinking. Around the same time, generative models like GPT-3 emerged, enabling AI to generate human-like text and assist in content creation. [6][7]

Early AI systems, known as "narrow AI," were slow and specialized, performing specific tasks within a limited scope.[8][9] However, as AI continued to develop, it found its way into consumer-facing applications like YouTube's recommendation system, which uses AI to personalize content suggestions based on user data.[10][11]These advancements illustrate AI's growing role in everyday life, from filtering emails to powering virtual assistants.

## Self-Learning AI

The evolution from slow, specialized AI systems to dynamic, self-learning machines marks a significant shift in the role AI plays in society. AI has become deeply integrated into everyday experiences, subtly influencing how people interact with digital content and services. This transformation is driven by the advent of self-learning AI systems—machines that improve their performance over time without explicit human intervention. These systems, also known as machine learning models, operate by analyzing vast amounts of data, identifying patterns, and making decisions based on that data. As they process more information, they refine their algorithms and predictions[12], becoming increasingly accurate and efficient in their tasks. [13]

Self-learning AI differs fundamentally from earlier, static AI models, which relied on manual programming and required constant updates by human operators. The ability of AI to learn and adapt autonomously accelerates the development of new applications and enables AI to solve problems and make decisions in ways previously unimaginable. This self-improving nature represents a significant leap forward, allowing machines to handle complex tasks such as speech

[4] *Samuel, A. L. Some Studies in Machine Learning Using the Game of Checkers. Journal of the ACM, 1959. Available at: https://dl.acm.org/doi/10.1145/365153.365168.*

[5] *IBM, Early Games in AI History, IBM History. Available at: https://www.ibm.com/history/early-games.*

[6] *BBC News, Google's AlphaGo: Five Moments that Showed How AI Beat a Go Master, 2017. Available at: https://www.bbc.com/news/technology-40042581.*

[7] *Jiang, Ji et al. Artificial Intelligence in Education: A Review. arXiv, 2020. Available at: https://arxiv.org/abs/2005.14165.*

[8] *Our World in Data, A Brief History of Artificial Intelligence, Available at: https://ourworldindata.org/brief-history-of-ai.*

[9] *World Economic Forum, What is AI? Stuart Russell Explains, 2022. Available at: https://www.weforum.org/agenda/2022/06/what-is-ai-stuart-russell-expert-explains-video/.*

[10] *McCarthy, John. What Is Artificial Intelligence?. AI Magazine, 2007. Available at: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/18139.*

[11] *Lu, Hui. Artificial Intelligence and Machine Learning in Healthcare: Opportunities and Challenges. SN Applied Sciences, 2020. Available at: https://link.springer.com/article/10.1007/s40747-020-00212-w.*

[12] *If you wish to learn more about Machine Learning and the types of Machine Learning: https://www.ibm.com/topics/machine-learning*

[13] *Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.*
*Link: Deep Learning by Goodfellow, Bengio, and Courville - MIT Press*

recognition, language translation, disease diagnosis, and even autonomous driving, with minimal human oversight.[14]

The capabilities of self-learning AI also introduce a range of new challenges and ethical concerns. While AI has the potential to greatly benefit society—enhancing efficiency, decision-making, and innovation—it also brings significant risks. The autonomous nature of these systems raises critical questions about accountability, transparency, and control.[15] For instance, if an AI system makes a harmful decision, it can be challenging to determine who is responsible: the developer, the operator, or the machine itself? Furthermore, the ability of AI to operate independently heightens concerns about privacy, security, and the potential for unintended consequences.[16]

Another critical issue is transparency. AI systems, especially those based on deep learning, often operate as "black boxes," making it difficult to understand how they arrive at certain decisions.[17] This lack of transparency can undermine trust and exacerbate inequalities, particularly when AI is used in contexts that impact human rights, such as criminal justice, employment, and access to social services. Bias in AI systems is another significant concern. AI models trained on biased data can perpetuate and even exacerbate societal inequalities, leading to discriminatory outcomes. This is particularly troubling in areas like hiring, law enforcement, and healthcare, where biased AI decisions can directly impact individuals' rights to equality and non-discrimination.

The privacy concerns associated with AI also have direct implications for human rights. AI systems often rely on extensive personal data collection and analysis, raising the potential for violations of the right to privacy. This is particularly concerning in contexts where AI is used for surveillance or data mining, which can lead to unwarranted intrusions into individuals' private lives.

These challenges underscore the dual-edged nature of AI—while it offers unprecedented opportunities for innovation and progress, it also poses significant risks to human rights.

## 1.1. AI Impact on Human Rights

As AI continues to permeate various aspects of society, its implications extend beyond mere ethical concerns to the very fabric of human rights. We discussed some of the risks associated with self-learning AI; now, we will examine the specific ways in which AI impacts fundamental human rights, focusing on privacy, freedom of expression, and equality.

### Privacy Rights

[14] *Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th Edition). Pearson.*
*Link: Artificial Intelligence: A Modern Approach by Russell & Norvig - Pearson*

[15] *Bostrom, N., & Yudkowsky, E. (2014). The Ethics of Artificial Intelligence. In F. Frankish & W. M. Ramsey (Eds.), The Cambridge Handbook of Artificial Intelligence (pp. 316-334). Cambridge University Press.*
*Link: The Ethics of Artificial Intelligence by Bostrom & Yudkowsky - Cambridge University Press*

[16] *Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.*
*Link: The Age of Surveillance Capitalism by Shoshana Zuboff - PublicAffairs*

[17] *von Eschenbach, W. (2021). "Transparency and the Black Box Problem: Why We Do Not Trust AI." Philosophy & Technology, vol. 34, no. 4, pp. 1699–1716, doi:10.1007/s13347-021-00477-0.*

One of the most significant human rights concerns associated with AI is the threat to privacy. AI systems often rely on vast amounts of personal data to function effectively, whether through data mining, surveillance, or algorithmic decision-making. The ability of AI to analyze and cross-reference massive datasets can lead to the creation of detailed profiles of individuals, revealing intimate aspects of their lives without their consent.

Surveillance is a key area where AI poses risks to privacy rights. Governments and corporations increasingly deploy AI-driven surveillance technologies, such as facial recognition and predictive analytics, to monitor public spaces and online activities. While these technologies can enhance security, they also risk infringing on the right to privacy by enabling unprecedented levels of monitoring and data collection. For example, the deployment of facial recognition technology in public places can lead to the continuous tracking of individuals' movements, often without their knowledge or consent. Data mining is another practice that raises significant privacy concerns. AI algorithms are often employed to sift through large datasets to uncover patterns and insights. [18]

The misuse of personal information by AI systems further exacerbates privacy concerns. When personal data is analyzed by AI without sufficient safeguards, it can lead to breaches of confidentiality and the exposure of sensitive information. This not only violates the right to privacy but also undermines the trust individuals place in the institutions that hold their data.

### Freedom of Expression

AI also has profound implications for freedom of expression, particularly through its role in content moderation, censorship, and the spread of disinformation and hate speech. As more online platforms rely on AI to manage vast amounts of user-generated content, the potential for AI to suppress free speech and facilitate the spread of harmful content increases.

Content moderation is a critical function of AI on social media platforms and other online services. AI algorithms are tasked with filtering out harmful content, such as hate speech, misinformation, and explicit material.[19] While this is essential for maintaining safe online environments, it can also lead to the overzealous suppression of legitimate speech. AI systems, often lacking nuanced understanding and cultural context, thus they may flag and remove content that falls within grey areas of expression, such as satire, cultural references or political commentary. This lack of contextual awareness can lead to unjust censorship, disproportionately affecting certain voices, particularly those from marginalized or culturally diverse groups.

Disinformation is another significant concern in the realm of freedom of expression. AI-driven systems can be used to create and disseminate false information at an unprecedented scale and speed, contributing to the spread of disinformation.[20] This not only undermines public trust in

[18] *United Nations Sustainable Development Goals, Navigating the Intersection of AI, Surveillance, and Privacy, available at: https://sdgs.un.org/sites/default/files/2024-05/Francis_Navigating%20the%20Intersection%20of%20AI%2C%20Surveillance%2C%20and%20Privacy.pdf.*

[19] *Bodyguard.ai, AI Content Moderation: Understanding the Benefits and Challenges, Bodyguard Blog, available at: https://www.bodyguard.ai/en/blog/ai-content-moderation.*

[20] *RAND Corporation, The Risks of Artificial Intelligence and Disinformation, available at:*

media and democratic institutions but also can lead to real-world harm, as individuals and groups act on false beliefs and narratives. The ability of AI to generate convincing fake content, such as deep fakes, further complicates efforts to combat disinformation and protect the integrity of information.

Hate speech is closely related to both content moderation and disinformation. AI systems used to detect and remove hate speech are not always perfect and can either miss harmful content or wrongly censor legitimate speech. Furthermore, AI can be exploited to amplify hate speech, allowing it to spread rapidly across platforms and incite violence or discrimination against vulnerable groups. Censorship is another area where AI's impact on freedom of expression is evident. Governments and private entities can use AI to enforce strict control over the flow of information, monitoring and blocking content that challenges the status quo or threatens their interests. [21]

## Equality and Non-Discrimination

AI's ability to process and analyze large datasets has the potential to revolutionize decision-making in various sectors. However, this same capability can lead to significant challenges particularly in the areas of equality and non-discrimination.

Hiring practices are increasingly influenced by AI-driven systems that screen job applicants and assess their suitability for roles. While these systems can enhance efficiency, they also risk perpetuating existing biases in the data they are trained on. If historical hiring data reflects discriminatory practices, AI systems may replicate and even amplify these biases, leading to unequal treatment of candidates based on race, gender, age, or other protected characteristics. This undermines the right to equal treatment and non-discrimination in employment.[22]

Law enforcement is another area where AI's impact on equality is pronounced. Predictive policing algorithms, for example, are used to identify potential criminal activity and allocate resources accordingly. However, these systems often rely on data that reflects existing societal biases, such as over-policing in certain communities. As a result, AI-driven policing can disproportionately target marginalized groups, leading to a cycle of discrimination and injustice.[23]

The risk of perpetuating discrimination through AI underscores the need for safeguards and oversight to ensure these technologies promote equality rather than deepen existing disparities. AI systems must be designed with a clear understanding of their potential impact on human rights and be continuously monitored to prevent discriminatory outcomes.

*https://www.rand.org/pubs/perspectives/PEA1043-1.html.*

[21] *Freedom House, Repressive Power of Artificial Intelligence, Freedom on the Net Report, 2023, available at: https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.*

[22] *Brookings Institution, Auditing Employment Algorithms for Discrimination, available at: https://www.brookings.edu/articles/auditing-employment-algorithms-for-discrimination/.*

[23] *MIT Technology Review, Predictive Policing Algorithms are Racist. They Need to be Dismantled, available at: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.*

### AI Impact on Human Rights in Kosovo

AI adoption in Kosovo is still in its infancy, with limited implementation across key sectors. The country's focus has been on building digital infrastructure and improving access to technology, rather than on the widespread deployment of advanced AI systems. As a result, the regulatory framework for AI is underdeveloped, and there is a lack of comprehensive policies addressing the ethical, legal, and societal implications of AI.[24]

Despite this, the potential for AI to impact human rights in Kosovo cannot be overlooked. The country’s digital transformation efforts, coupled with the gradual introduction of AI technologies, could soon bring the same risks seen in more developed regions. Without a robust legal and policy framework, Kosovo may struggle to protect its citizens from the adverse effects of AI, such as privacy violations, algorithmic discrimination, and limitations on freedom of expression.

## 1.2. Purpose of the Paper

The purpose of this paper is to examine the impact of AI on fundamental human rights in Kosovo, with a focus on privacy, freedom of expression, and non-discrimination. As AI technologies become more integrated into daily life, it is crucial to understand how they may affect these rights and what legal or policy measures, if any, are currently in place to address these challenges.

This paper will analyze Kosovo’s existing frameworks—or lack thereof—related to AI and its implications for human rights, identifying gaps in legislation, capacity, and governance. Additionally, we will map out the AI landscape in Kosovo, examining which technologies are being utilized and assessing the preparedness of key stakeholders, including the government, private sector, and civil society, to manage the ethical and legal challenges posed by AI.

By identifying these gaps and examining the current state of AI readiness, the paper will offer recommendations for strengthening governance and policy frameworks. Furthermore, it aims to raise awareness and spark a broader public debate on the ethical implications of AI, ensuring that future advancements are aligned with the protection of human rights in Kosovo.

In order to achieve the aim and objectives of this paper, four key research questions have been formulated to guide the analysis:

1. What legal and policy measures exist in Kosovo to protect human rights in the context of AI?
2. How is AI affecting fundamental rights such as privacy, freedom of expression, and non-discrimination in Kosovo?
3. What does the AI landscape in Kosovo look like, including the key technologies and stakeholders involved?
4. How prepared are key stakeholders in Kosovo to deal with the ethical challenges of AI?

[24] *BIRN report*

## 1.3. Methodology

The methodology of this paper is designed to provide a thorough analysis of the impact of AI on human rights in Kosovo. A mixed-methods approach is employed, combining both qualitative and quantitative research methods to ensure a comprehensive understanding of the subject matter.

The study begins with extensive desk research to review existing literature, legal frameworks, and policy documents related to AI and human rights. This includes examining Kosovo's current laws and regulations, as well as relevant EU and international standards. Comparative analysis is also conducted, drawing on examples from other countries to provide context and identify best practices for AI governance.

To gather insights from key actors in Kosovo, semi-structured interviews were conducted with representatives from the government, private sector, civil society, and academia. These interviews aimed to explore the level of awareness, preparedness, and the ethical considerations each stakeholder faces in relation to AI. The interviews also helped to uncover gaps in current policy frameworks and institutional capacity to manage AI-related risks and opportunities.

In addition to qualitative interviews, one survey was conducted to gather quantitative data from the general public. This survey aim was to measure awareness, perceptions, and concerns about AI technologies in Kosovo. The survey was done and distributed online.

The data collected through interviews and surveys were analyzed using a thematic analysis approach for qualitative data and descriptive statistical analysis for quantitative data. The findings from both methods were integrated to provide a well-rounded analysis of the current state of AI governance in Kosovo, identifying key trends, gaps, and opportunities.

# Chapter II: AI Legal and Policy Framework

This chapter examines the legal and policy frameworks that govern the development and application of AI, with a focus on both the European Union (EU) and Kosovo. The objective is to provide a clear understanding of how these frameworks are crafted to address the ethical, societal, and legal challenges posed by AI. By exploring regulatory approaches at both the EU and Kosovo levels, this chapter seeks to highlight the key elements, challenges, and opportunities within these jurisdictions, offering insights into how AI can be governed to ensure the protection of fundamental rights while fostering technological innovation.

Legal and policy frameworks are essential for guiding the responsible development and use of AI, ensuring systems are ethical, transparent, and aligned with societal values. Without comprehensive regulations, AI risks amplifying inequalities, infringing on privacy, and undermining freedom of expression. Understanding the legal landscape shaping AI is therefore crucial for policymakers, industry leaders, and civil society

We will analyze the EU's approach to AI regulation, as it has established a comprehensive legal and policy framework that balances innovation with the protection of fundamental rights. Key initiatives such as the Artificial Intelligence Act (AI Act)[25], a groundbreaking legal framework for AI. This act, along with other regulations like the Digital Services Act (DSA)[26] and the General Data Protection Regulation (GDPR)[27]demonstrates the EU's commitment to balancing innovation with the protection of fundamental rights.

As Kosovo works toward EU membership, we will examine the country's existing laws that indirectly affect AI and its impact on the identified human rights. Under Article 22 of the Constitution, international agreements on human rights and equality are directly applicable within Kosovo's legal framework; however, we will not review these as our focus is on the development of domestic regulations specific to AI.

## 2.1. European Union Legal and Policy Framework for AI

The EU has developed a comprehensive approach to AI, aiming to harness the technology's potential while ensuring it aligns with European values, including respect for human rights, privacy, and the rule of law.[28] At the core of the EU's approach is the principle that AI should be human-centric, meaning it should serve people and society as a whole. This perspective

[25] *European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.*

[26] *European Union, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, OJ L 277, 27.10.2022, p. 1–102. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065.*

[27] *European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.*

[28] *European Commission. "Europe's Digital Decade: digital targets for 2030." Available at: European Commission - Digital Strategy*

emphasizes that AI should enhance human capabilities, improve quality of life, and contribute to societal well-being, rather than advancing technology for its own sake.[29]

Recognizing the potential risks associated with AI—such as privacy violations, security concerns, and potential biases—the EU has introduced the AI Act, which aims to regulate the use of AI technologies, ensuring that they are transparent, accountable, and aligned with fundamental rights. Alongside this, the Digital Agenda for Europe supports a broader framework that promotes digital innovation while safeguarding privacy, security, and democratic values. Additionally, the EU has extended this vision to the region with the Digital Agenda for the Western Balkans, aiming to support digital transformation while adhering to European values.[30]

### 2.1.1. Artificial Intelligence Act

The AI Act, introduced by the European Commission in April 2021, which was conclusively adopted in April 2024 after a lengthy negotiation process, stands as the first comprehensive legal framework designed to ensure that AI systems are developed and deployed in a manner consistent with European values, particularly the protection of fundamental human rights.[31]

The AI Act employs a risk-based approach to classify AI systems into categories based on their potential risks to individuals and society. These classifications range from AI systems that pose an unacceptable risk, which are prohibited, to those with minimal risk, which face little to no regulation. This tiered regulatory approach is central to the Act's goal of preventing AI technologies from infringing on human rights while allowing innovation in less sensitive areas.[32]

A key objective of the AI Act is the protection of fundamental human rights. High-risk AI systems—those most likely to impact individuals' rights and freedoms—are subject to stringent requirements. These systems include AI applications used in critical areas such as healthcare, law enforcement, and employment. Article 6 of the AI Act specifically outlines the criteria for classifying AI systems as high-risk, focusing on their intended use in critical sectors. These requirements are intended to prevent AI systems from perpetuating discrimination, violating privacy, or causing harm to individuals.

The AI Act's emphasis on transparency is particularly relevant to human rights. Article 13 mandates that users and affected individuals must be informed about the capabilities and limitations of AI systems, including the processes behind automated decision-making. This transparency is essential for maintaining accountability and allowing individuals to challenge decisions made by AI systems, thereby safeguarding their rights to fair treatment and due process.

[29] *Ibid*

[30] *European Commission, Digital Agenda for the Western Balkans: EU Partners with Western Balkans to Develop Digital Economy and Society, European Commission Press Corner, 2018. Available at:* [https://ec.europa.eu/commission/presscorner/detail/es/ip_18_4242](https://ec.europa.eu/commission/presscorner/detail/es/ip_18_4242)

[31] *European Commission. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 19 April 2024 on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts." Available at: European Commission - AI Act.*

[32] *Ibid., Articles 5, 6*

Furthermore, the Act addresses ethical concerns by requiring that high-risk AI systems undergo rigorous conformity assessments before they can be deployed. Articles 16 and 17 detail these assessments, which include evaluations of the systems' robustness, accuracy, and cybersecurity measures. By enforcing these standards, the AI Act seeks to prevent harm and uphold the safety and dignity of individuals.

The AI Act also introduces the concept of regulatory sandboxes, outlined in Article 53, which are controlled environments where AI developers can test and refine their technologies under regulatory supervision. This approach allows for a careful balance between technological advancement and the protection of human rights, providing a space where ethical concerns can be addressed early in the development process.

Central to the AI Act is its focus on safeguarding human rights, with particular attention to privacy, freedom of expression, and equality.

### Privacy Rights

Under Article 10, the Act mandates that these systems must be trained, validated, and tested using high-quality, relevant, and representative data sets, ensuring alignment with the EU's stringent data protection standards, such as those outlined in the GDPR. This provision is crucial in preventing the misuse of personal data, which is a key aspect of protecting individuals' privacy.

Additionally, as we mentioned above Article 13 of the AI Act requires that users of high-risk AI systems be fully informed about how their data is being processed, including details about the AI system's capabilities, the logic behind its decision-making processes, and the data it utilizes. The Act also includes exemptions under Article 83 for AI systems used in law enforcement and national security contexts. These exemptions have raised concerns about potential privacy infringements, particularly in scenarios involving surveillance or border control, where AI systems might be deployed with less oversight and transparency.

### Freedom of Expression

The AI Act also directly addresses the implications of AI systems on freedom of expression, particularly in the context of content moderation on digital platforms. Article 52 mandates that AI systems used to filter or curate online content must operate transparently, providing users with clear explanations for content-related decisions. This requirement is intended to protect freedom of expression by ensuring that content moderation processes are not arbitrary or opaque, thus allowing individuals to understand and challenge decisions that may affect their ability to express themselves freely.

Despite these protections, there are concerns that the Act may not fully prevent AI-driven censorship, especially if platform operators are given excessive discretion in implementing AI systems without adequate external oversight.

### Equality and Non-Discrimination

Article 10 of the Act requires that AI systems be developed using data sets that are representative and free from biases that could lead to discriminatory outcomes. This provision is aimed at ensuring that AI systems do not unfairly disadvantage individuals based on race, gender, or other protected characteristics.

Furthermore, Article 61 mandates that high-risk AI systems undergo regular assessments to monitor and mitigate any discriminatory impacts. These assessments are intended to ensure that AI systems are not only fair in their design but also in their ongoing operation. However, the exemptions for public authorities provided in Article 83 have raised concerns. These exemptions mean that AI systems used by law enforcement or immigration authorities might not be subject to the same rigorous transparency and accountability standards.

In the broader context of EU AI governance, the AI Act complements other significant regulations, such as the GDPR and the DSA. Together, these frameworks create a comprehensive legal environment that prioritizes human rights in the digital age. The AI Act, in particular, reflects the EU's commitment to ensuring that AI technologies are not only innovative but also safe, transparent, and aligned with the fundamental rights of individuals.

However, the AI Act has not been without its critics. Amnesty International and other human rights organizations have raised concerns that the Act fails to adequately protect human rights in several critical areas. They argue that, despite its intentions, the AI Act leaves significant loopholes, particularly concerning the use of AI by law enforcement, migration authorities, and in border control. These areas, they claim, are prone to fundamental rights violations, and the Act's provisions do not go far enough to ensure transparency or accountability in these high-stakes contexts.[33]

By setting a high standard for AI governance, the AI Act positions the EU as a global leader in the ethical regulation of AI. It serves as a model for other jurisdictions, potentially influencing the development of AI laws worldwide. However, the true impact of the AI Act on human rights will depend on its implementation and the willingness of AI developers and operators to adhere to these rigorous standards.

### 2.1.2. General Data Protection Regulation

The GDPR, which came into effect on May 25, 2018, is one of the most significant data protection laws globally. It serves as a cornerstone for the EU's approach to data privacy and protection, with far-reaching implications for the development and deployment of AI systems.

The GDPR establishes stringent rules for how personal data must be collected, processed, and stored, with a particular focus on ensuring transparency, accountability, and individual control over personal information. These principles are critical when applied to AI systems, which often rely on vast amounts of data, including personal data, to function effectively.

One of the key aspects of the GDPR that directly impacts AI is the regulation of automated decision-making, including profiling. Article 22 of the GDPR specifically addresses this issue, granting individuals the right not to be subject to decisions based solely on automated processing,

[33] *Amnesty International. "EU's AI Act fails to set gold standard for human rights." April 3, 2024. Available at: Amnesty International.*

including profiling, which produces legal effects concerning them or similarly significantly affects them.[34] This provision is particularly relevant in the context of AI systems that make decisions without human intervention, such as in credit scoring, hiring processes, or personalized advertising.

The GDPR also imposes strict requirements on data processing, particularly concerning the principles of lawfulness, fairness, and transparency outlined in Article 5. AI systems must ensure that the data they process is handled in a manner that is lawful, fair, and transparent to the data subjects. This means that organizations deploying AI must provide clear and accessible information to individuals about how their data is being used, the purposes of the processing, and their rights under the GDPR.[35]

Moreover, the GDPR emphasizes the principle of data minimization, which requires that personal data collected is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.[36] This principle poses a significant challenge for AI systems that thrive on large datasets, often requiring data beyond what is strictly necessary to improve their algorithms.

Another crucial aspect of the GDPR that affects AI is the requirement for explicit consent in certain data processing activities, particularly those involving sensitive personal data, as outlined in Article 9.[37] For AI systems that process sensitive data, such as biometric information or health data, obtaining explicit consent from individuals is a legal necessity.

The GDPR also introduces the concept of data protection by design and by default (Article 25), which requires that data protection measures are integrated into the development and operation of processing activities from the outset.[38] For AI systems, this means that privacy considerations must be embedded into the system’s design and functionality, ensuring that data protection is not an afterthought but a fundamental component of the AI’s operation.

In addition to these provisions, the GDPR mandates that organizations conducting data processing that is likely to result in a high risk to individuals’ rights and freedoms must carry out a Data Protection Impact Assessment (DPIA) as per Article 35.[39]

The GDPR’s influence extends beyond the borders of the EU due to its extraterritorial scope. Organizations outside the EU that process the personal data of EU citizens are also subject to the GDPR’s requirements, which has a profound impact on global AI practices.

However, the GDPR was not specifically designed with AI in mind, leading to challenges in its application to complex AI systems. For instance, the requirement for transparency and explainability can be difficult to meet for AI systems that operate as "black boxes," where even the developers may not fully understand how certain decisions are made by the system. This has

[34] *European Parliament and Council. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)." Article 22. Available at: EUR-Lex GDPR.*

[35] *Ibid., Article 5.*

[36] *Ibid., Article 5(1)(c).*

[37] *Ibid., Article 9.*

[38] *Ibid., Article 25*

[39] *Ibid., Article 35.*

led to calls for more tailored regulations that address the unique challenges posed by AI while building on the GDPR's foundational principles.

### 2.1.3. Digital Service Act

The DSA, adopted by the EU in November 2022, represents a significant legislative framework aimed at regulating online platforms and digital services within the EU. The DSA is a cornerstone of the EU's broader strategy to create a safer digital space, where the fundamental rights of users are protected, and where online platforms are held accountable for their content and services. The DSA focuses on increasing transparency, accountability, and oversight of online platforms, particularly those with significant market power, often referred to as "gatekeepers".[40] The DSA introduces a series of obligations for different types of digital services, categorized based on their size, reach, and role in the digital ecosystem.

The provisions in the DSA include several key measures designed to ensure the responsible operation of online platforms. First, the DSA requires platforms to disclose detailed information about how their algorithms function, including the processes behind content moderation and the methods used to generate recommendations. This transparency is intended to help users understand how content decisions are made and to promote accountability in content moderation practices.[41] Additionally, the DSA imposes a duty of care on platforms, obligating them to mitigate various risks such as the dissemination of illegal content, the spread of disinformation, and other potential harms arising from digital services. Platforms are mandated to conduct thorough risk assessments and implement measures to address these risks effectively.[42]

Furthermore, the DSA strengthens users' rights by ensuring they have access to transparent and effective complaint and redress mechanisms. This includes providing users with the ability to challenge content moderation decisions and to receive clear explanations for those decisions. [43] Moreover, the DSA introduces new regulations concerning targeted advertising, requiring platforms to provide clear and accessible information about the use of personal data in advertisements and to obtain users' explicit consent. It also aims to combat "dark patterns"—manipulative online practices designed to trick users into making decisions they might not otherwise choose.[44]

The DSA has significant implications for the use of AI, particularly in the context of content moderation and recommendation systems. As AI is increasingly deployed by online platforms to automate content moderation, detect illegal content, and personalize user experiences, the DSA's stringent requirements for transparency, accountability, and user rights play a crucial role in shaping how these AI systems are developed and utilized.

[40] *European Parliament and Council. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: Digital Service Act*

[41] *Ibid., Article 23.*

[42] *Ibid., Article 26.*

[43] *Ibid., Article 17.*

[44] *Ibid., Article 24.*

The DSA mandates that platforms must disclose the algorithms and AI systems they use for content moderation. This includes providing detailed information on how these AI systems detect and manage illegal content, hate speech, or disinformation[45]. The transparency obligations under the DSA are designed to ensure that AI-driven content moderation does not infringe on users' rights, particularly their right to freedom of expression. By enforcing transparency, the DSA seeks to prevent arbitrary or biased content moderation decisions that could suppress lawful speech.

Moreover, AI plays a critical role in recommendation systems used by many online platforms to suggest content to users. The DSA's emphasis on transparency and user control requires that platforms provide clear explanations of how these AI-driven recommendation systems function. Users must be given the ability to modify or opt-out of these algorithmic recommendations, thereby granting them greater control over their online experiences.[46]

Additionally, the DSA's duty of care provisions require platforms to assess and mitigate the risks posed by their services, including those related to AI systems. This includes addressing the risks of AI spreading disinformation or exacerbating harmful content, which is crucial in ensuring that AI is used responsibly and does not contribute to the erosion of trust in digital services or the proliferation of harmful content.[47]

The DSA's strong focus on protecting fundamental human rights within the digital space is closely aligned with its regulation of AI systems.

The DSA enhances privacy rights by regulating how platforms use AI for targeted advertising and by enforcing transparency in data usage. Platforms are required to clearly inform users about how their data is employed in AI-driven advertisements, ensuring that privacy is respected and that users maintain control over their personal information.[48]

The DSA's transparency requirements for AI systems used in content moderation are essential for safeguarding freedom of expression. By making the workings of AI-driven moderation systems more transparent, the DSA aims to prevent unjustified censorship and protect users' rights to freely express themselves online. The right to appeal and obtain explanations for content decisions further strengthens these protections.[49]

The DSA's provisions on risk assessments and the duty of care require platforms to consider the potential discriminatory impacts of their AI systems. This is particularly important in ensuring that AI does not perpetuate biases in content moderation or recommendation algorithms, which could disproportionately affect marginalized groups. By mandating that platforms assess and mitigate these risks, the DSA significantly contributes to the promotion of equality and non-discrimination in the digital environment.[50]

[45] *Ibid., Article 23*
[46] *Ibid., Article 24*
[47] *Ibid., Article 26*
[48] *Ibid., Article 24*
[49] *Ibid., Article 17*
[50] *Ibid., Article 26*

### 2.1.4. The NIS2 Directive

The NIS2 Directive, formally known as the Directive on Security of Network and Information Systems, was adopted by the EU in December 2022 as part of a broader effort to enhance EU-wide cybersecurity. Building on its predecessor, the original NIS Directive, NIS2 significantly expands the scope and stringency of cybersecurity requirements across various sectors. It aims to bolster the resilience of critical infrastructure and essential services, such as energy, transport, healthcare, and finance, thereby ensuring a higher level of cybersecurity across the EU.[51]

Under the NIS2, operators of essential services (OES) and digital service providers (DSP) are mandated to implement comprehensive cybersecurity measures. These measures include rigorous risk management practices designed to protect network and information systems from cyber threats. Organizations must also ensure the availability, integrity, and confidentiality of their data, reflecting the Directive's focus on both technical and organizational security. Additionally, NIS2 enhances the powers of national authorities, allowing them to enforce compliance more effectively and impose significant fines for non-compliance.

The Directive broadens its scope significantly compared to the original NIS Directive by including more sectors and types of organizations, reflecting the increasing reliance on digital systems in a wide array of industries.

The NIS2 Directive has direct implications for AI systems, particularly those integrated into critical infrastructure and essential services. As AI becomes increasingly embedded in systems that manage energy grids, transportation networks, healthcare services, and financial systems, the security and resilience of these AI-driven systems are of paramount importance. The Directive's cybersecurity requirements are crucial in ensuring that AI systems are secure, reliable, and resilient against cyber threats.

AI systems used in critical infrastructure, such as energy grids or transportation networks, are subject to the stringent security requirements of NIS2. These systems must be designed and operated with a strong focus on security, incorporating risk management practices that address potential vulnerabilities to cyber threats. By mandating such measures, NIS2 ensures that AI systems do not become weak points in the security of essential services. Additionally, the Directive's incident reporting requirements extend to AI systems, meaning that any significant cybersecurity incidents involving AI must be promptly reported to national authorities. These reporting requirements are essential for ensuring that vulnerabilities in AI systems are quickly addressed and that coordinated responses mitigate their impact.

Moreover, the risk management practices required by NIS2 must account for the specific risks associated with AI systems. This includes assessing the potential for AI systems to be targeted by cyberattacks, ensuring that AI algorithms are secure, and protecting the data processed by AI

[51] *European Parliament and Council. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)." Article 1. Available at: EUR-Lex - NIS2 Directive.*

systems from unauthorized access or manipulation. By integrating AI-specific risks into broader cybersecurity strategies, NIS2 enhances the overall security of AI-driven operations.

While the NIS2 Directive primarily focuses on cybersecurity, its provisions have important implications for human rights. The Directive's emphasis on protecting the integrity and confidentiality of data directly impacts privacy rights by ensuring that AI systems in critical sectors are secure and resilient against cyber threats. Although NIS2 is not directly related to content moderation or information dissemination, its provisions indirectly support freedom of expression by ensuring that the digital infrastructure enabling free communication remains secure and reliable.

### 2.1.5. White Paper on Artificial Intelligence

The White Paper on Artificial Intelligence, published by the European Commission in February 2020, outlines the EU's approach to developing and regulating AI technologies. This document does not have legal power, it is a policy documents which sets forth a vision for balancing innovation with the need to ensure that AI systems are trustworthy, transparent, and aligned with European values and fundamental rights. The White Paper emphasizes the creation of an "ecosystem of excellence" to drive AI innovation and an "ecosystem of trust" to manage the risks associated with AI technologies.

The document proposes a risk-based regulatory approach, where the level of oversight is proportional to the potential risks posed by AI systems. High-risk AI applications, particularly in sectors like healthcare, transportation, and law enforcement, are highlighted as areas requiring stricter regulations, including mandatory transparency, accountability, and human oversight measures.[52] The White Paper also underscores the importance of ethical AI, drawing on the principles set out in the Ethics Guidelines for Trustworthy AI published in 2019. These guidelines advocate for AI that respects fundamental rights, promotes human agency, and operates in a transparent and fair manner.

One of the key proposals in the White Paper is the differentiated regulatory approach, which tailors the regulatory burden according to the risk associated with specific AI applications. High-risk systems, such as those involved in biometric identification or critical infrastructure, are subject to rigorous testing, validation, and transparency requirements. Lower-risk AI systems, however, would enjoy a more flexible regulatory environment, fostering innovation while still ensuring safety and trustworthiness.

The White Paper laid the groundwork for the subsequent development of the AI Act. Many of the concepts and regulatory approaches proposed in the White Paper, particularly the focus on high-risk AI applications and the need for a risk-based regulatory framework, were incorporated into the AI Act, which now serves as the binding legal framework for AI in the EU.

[52] *European Commission. "White Paper on Artificial Intelligence - A European approach to excellence and trust." February 2020. Available at: European Commission - White Paper on AI.*

The White Paper places a strong emphasis on safeguarding human rights within the context of AI development and deployment. Its proposals aim to ensure that AI systems respect fundamental rights such as privacy, freedom of expression, and non-discrimination.

### 2.1.6. Ethics Guidelines for Trustworthy AI

The Ethics Guidelines for Trustworthy AI, published by the European Commission's High-Level Expert Group on Artificial Intelligence in April 2019, represent a foundational document in the EU's approach to ensuring that AI technologies are developed and deployed in a manner that aligns with European values and fundamental rights. These guidelines outline the key principles and requirements that AI systems must meet to be considered trustworthy, thereby setting the ethical standards for AI development in Europe.

The guidelines propose that AI should be lawful, ethical, and robust, both from a technical and social perspective. These three components—lawfulness, ethics, and robustness—are considered essential for achieving trustworthy AI. The lawfulness component emphasizes the need for AI to comply with all applicable laws and regulations, ensuring that AI systems respect fundamental rights. The ethical component focuses on ensuring that AI systems adhere to ethical principles and values, even in areas where the law may not provide explicit guidance. Robustness, the third component, pertains to the technical and social reliability of AI systems, ensuring that they function safely and as intended in all situations.[53]

Central to the Ethics Guidelines are four ethical principles that AI systems must uphold: respect for human autonomy, prevention of harm, fairness, and explicability. These principles are intended to guide the development and use of AI in a way that respects human dignity and rights.

The guidelines also outline seven key requirements that AI systems should meet to be considered trustworthy: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination, and fairness, (6) societal and environmental well-being, and (7) accountability. These requirements are designed to operationalize the ethical principles and provide practical guidance on how to implement trustworthy AI in various contexts. For example, human agency and oversight emphasize the need for mechanisms that allow for meaningful human control over AI systems, while technical robustness and safety focus on ensuring that AI systems are secure and resilient against risks. Privacy and data governance highlight the importance of protecting personal data and ensuring that AI systems handle data responsibly, while transparency involves making AI systems understandable and open to scrutiny.

The Ethics Guidelines also stress the importance of diversity, non-discrimination, and fairness in AI systems, advocating for the inclusion of diverse perspectives in AI development and the avoidance of biases that could lead to discriminatory outcomes. Societal and environmental well-being calls for AI to be developed and used in ways that benefit society as a whole, including considering the environmental impact of AI technologies. Finally, accountability is emphasized as

[53] *European Commission's High-Level Expert Group on Artificial Intelligence. "Ethics Guidelines for Trustworthy AI." April 2019. Available at: Ethics Guidelines for Trustworthy AI.*

a crucial element of trustworthy AI, requiring that mechanisms be in place to ensure that those responsible for AI systems can be held accountable for their outcomes.

Although the Ethics Guidelines are not legally binding, they have significantly influenced the development of subsequent AI policies and regulations in the EU, including the AI Act. The Ethics Guidelines for Trustworthy AI are particularly relevant to the protection of human rights, as they provide a framework for ensuring that AI systems respect privacy, equality, and freedom of expression.

## 2.2. Kosovo AI Legal and Policy Framework

In examining the AI legal and policy framework of Kosovo, it is important to acknowledge that the country is in the early stages of developing its regulatory and policy landscape concerning AI. Kosovo’s approach to AI is less defined compared to that of the EU. However, as AI technologies increasingly permeate various sectors, there is a growing recognition of the need for a coherent and well regulated framework that addresses both the opportunities and challenges posed by AI.

Currently, Kosovo does not have a specific legal framework dedicated exclusively to AI. The regulatory landscape concerning AI is primarily shaped by broader laws and regulations that address related areas, such as data protection, cybersecurity, and non-discrimination. These existing legal instruments provide some foundational elements that could be extended or adapted to address the specific challenges and ethical concerns associated with AI technologies.

Despite the absence of a dedicated AI strategy or comprehensive regulation specifically targeting AI, Kosovo has shown engagement in international and regional discussions on AI and digital governance. As a country aspiring to join the EU, Kosovo’s alignment with EU standards, including those concerning AI, will be crucial. The development of AI policies and regulations in Kosovo is likely to be influenced by the EU’s AI framework, particularly as Kosovo continues to harmonize its laws with those of the EU as part of the European integration process. However, it is important to note that Kosovo's government remains at a relatively low level of development in terms of legislation that would systematically implement digital technologies in the public and private sectors.[54] Despite the lack of specific legal frameworks or guidance on AI, Kosovo’s involvement in the EU’s Digital Europe Programme is an important step toward advancing digital transformation. This initiative aims to improve digital accessibility for citizens, businesses, and institutions, while also promoting the development of AI through strategic grants, offering Kosovo the opportunity to align with broader EU objectives in this field.[55]

### 2.2.1. Digital Agenda of Kosovo 2030

The *Digital Agenda of Kosovo 2030* serves as the national strategy for advancing Kosovo’s digital transformation over the next decade. It outlines key initiatives aimed at fostering economic growth,

[54] *BIRN. "Balkan Govts Need To Create Strategies For Responsible Use of Artificial Intelligence," (2023). Available at: Final AI Report.*

[55] *Ministry of Economy, Republic of Kosovo. "Kosovo to join the 7 billion Euro Digital Europe Programme." Available at: Ministry of Economy - Kosovo Digital Europe Programme.*

innovation, and the digitalization of public services to meet the needs of citizens, businesses, and public institutions. The agenda aligns with the EU's *Digital Compass 2030*, reflecting Kosovo's ambition to harmonize its digital policies with EU standards while accelerating its own digital evolution.[56]

The *Digital Agenda 2030* consists of several key strategic objectives aimed at transforming Kosovo into a digitally advanced society. One of the primary goals is to establish a secure and high-speed digital infrastructure across the country, including broadband and 5G networks, ensuring that universal connectivity is achieved. Another important objective focuses on driving the digital transformation of businesses by encouraging the adoption of advanced technologies, such as AI, big data, and cloud computing, with a target of 80% of businesses integrating these technologies by 2030.

In addition, the agenda emphasizes the importance of digitalizing public services to make them more accessible, transparent, and efficient for citizens. It also aims to foster the development of digital skills among the population, creating a strong research and development ecosystem by promoting digital literacy and providing advanced education in technology-related fields. Furthermore, the agenda highlights the need for a robust cybersecurity infrastructure to protect critical digital services and ensure the safety of data, contributing to a secure and resilient digital environment.

The *Digital Agenda 2030* aligns closely with the EU's *Digital Compass 2030*, a policy program that outlines the EU's targets for digital transformation by the end of the decade. Kosovo's alignment with the EU's digital goals includes initiatives to promote gigabit connectivity, expand digital skills, enhance cybersecurity, and increase the use of AI and other emerging technologies.

AI is a central component of Kosovo's *Digital Agenda 2030*, particularly in the context of economic growth, public services, and innovation.[57] The agenda highlights AI as a critical tool for digital transformation, focusing on its adoption by businesses and government sectors to improve efficiency and drive innovation.

It is important to note that although the *Digital Agenda of Kosovo 2030* aligns closely with the EU's *Digital Compass 2030*, it appears to overlook a critical component emphasized by the European framework—the *Digital Rights and Principles*, which place people at the center of digital transformation. This omission is particularly important when considering the development and deployment of AI technologies, as these principles, such as *freedom of choice*, *safety and security*, and *solidarity and inclusion*, directly impact how AI systems affect human rights.

### 2.2.2. E-Government Strategy Kosovo 2023-2027

The *e-Government Strategy 2023-2027* outlines Kosovo's vision and approach toward enhancing digital governance, with the goal of transforming public administration to become more efficient,

[56] *Ministry of Economy, Republic of Kosovo, Digital Agenda of Kosovo 2030. Available at: Digital Agenda of Kosovo 2030*

[57] *Ministry of Economy of the Republic of Kosovo, Digital Agenda of Kosovo 2030, 2023.*

transparent, and citizen-centric.[58] This strategy aligns with Kosovo's broader goals of digital transformation as part of the *Digital Agenda of Kosovo 2030* and aims to foster a resilient, modern digital infrastructure for public services.

The overarching vision of the *e-Government Strategy* is to establish a modern and inclusive digital government that serves the needs of citizens, businesses, and public institutions. The strategy emphasizes the importance of digital transformation in improving service delivery, enhancing transparency, and ensuring that public administration is responsive to the needs of the population.[59]

The strategy is built around key strategic objectives, which include:

1. Establish effective coordination of e-Government initiatives across both strategic and operational levels to ensure a cohesive and streamlined digital government system.
2. Enhance the digital competencies of public sector employees to ensure they are equipped to develop, manage, and utilize digital government services effectively.
3. Develop a unified, "whole-of-government" enterprise architecture that is supported by clear standards and modern technology frameworks, enabling seamless communication and data sharing between public institutions.
4. Ensure that public e-services are designed to be inclusive, reliable, and user-friendly, putting the needs of citizens and businesses at the forefront of digital government.
5. Strengthen the ability of government organizations to protect themselves from cyber threats, safeguarding the integrity of their digital systems and services.
6. Support innovation in the public sector by fostering partnerships with private sector companies, both nationally and internationally, to drive the digital transformation of government services.[60]

The e-Government Strategy introduces key principles of digitization, designed to guide the development and delivery of digital government services, ensuring efficiency, inclusivity, and security. These principles serve as the foundation for transforming public administration into a modern, digital-first entity that responds to the needs of citizens and businesses in a rapidly evolving digital landscape.

The principles outlined in the strategy are: digital by design, integrating digital technologies into policymaking and service design; data-driven, where data is governed as a strategic asset; interoperability by design, ensuring seamless communication between systems; user-driven and inclusive, focusing on services shaped by citizen needs; once-only, reducing redundancy by asking for information only once; multi-channel delivery, providing access through various platforms; privacy by design, safeguarding individual privacy from the outset; trust and security, promoting a safe and trustworthy digital environment; and open innovation, fostering collaboration between the government, private sector, and citizens to create innovative solutions.[61]

[58] *Ministry of Internal Affairs of the Republic of Kosovo, e-Government Strategy Kosovo 2023-2027, 2023. Available at: e-Government Strategy*

[59] *Ministry of Internal Affairs, Republic of Kosovo, e-Government Strategy Kosovo 2023-2027, (2023) p. 2.*
*Available at: e-Government Strategy*

[60] *Ibid. p.3*

[61] *Ibid. p.5*

The *e-Government Strategy 2023-2027* highlights the potential for emerging technologies like AI to drive innovation within the public sector. While AI is not yet fully integrated into government processes, the strategy sets the groundwork for its exploration and future implementation. AI is mentioned as a key technology that could enhance public administration's ability to provide services efficiently and innovate across sectors.

As part of the strategic plan, Kosovo intends to establish an innovation cell within the Agency of Information Society (AIS) in 2025. This innovation cell will be responsible for researching and piloting emerging technologies, including AI, to support the government's broader goals of digital transformation.[62]

### 2.2.3. Data Protection and Privacy

In this section, we will focus on privacy rights and examine how existing legal frameworks in Kosovo protect personal data in the context of potential AI technologies. Although there is no specific law regulating AI in Kosovo, it is important to review the relevant laws that govern privacy and data protection, as any AI system deployed would need to comply with these regulations. We will briefly go through the *Constitution of Kosovo*, *Law No. 06/L-082 on Protection of Personal Data*, *Law No. 08/L-173 on Cyber Security*, and the *Criminal Procedure Code No. 08/L-032*.

#### 2.2.3.1. The Constitution of Kosovo

Article 36 of the Constitution of Kosovo affirms the right to privacy, stating that *everyone has the right to the respect of their private and family life, the sanctity of their home, and the confidentiality of their correspondence, telecommunications, and other forms of communication*. The article also specifies that any restrictions on these rights can only be imposed by judicial order, and only in circumstances such as criminal investigations or matters of national defense, as provided for by law. Furthermore, the article provides for the protection of personal data, ensuring that laws govern the processes of collecting, storing, accessing, correcting, and using personal data to uphold individuals' privacy.

#### 2.2.3.2. Law No. 06/L-082 on Protection of Personal Data

The *Law No. 06/L-082 on Protection of Personal Data* was enacted to regulate the processing of personal data in Kosovo and align with international standards, particularly the EU's GDPR.[63] While the law does not explicitly mention AI, any system, including AI technologies that processes personal data is required to comply with its provisions. This means AI systems used in Kosovo must adhere to the same legal standards as traditional data processing methods, ensuring that privacy, data protection, and individual rights are respected.

The law sets the foundation for data protection, imposing strict obligations on data controllers and processors, which apply equally to AI systems. This ensures that AI-driven data processing—

[62] *Ibid. p.27*

[63]*Law No. 06/L-082 on Protection of Personal Data, 2019, available at:* *https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=18616*.

whether in automated decision-making, profiling, or other activities—must respect the rights of individuals as laid out in the law.

Article 21 of the *Law No. 06/L-082 on Protection of Personal Data* addresses automated individual decision-making, including profiling. This article prohibits decisions that have legal or similarly significant effects on individuals if they are based solely on automated processing, such as AI-driven decisions, unless specific conditions are met. These conditions include obtaining the explicit consent of the data subject or when such decisions are necessary for the execution of a contract. For AI systems, this provision ensures that individuals are not subject to decisions made solely by algorithms without human intervention, particularly in areas like hiring, credit scoring, or law enforcement. The law mandates that individuals are informed about such automated decisions and given the opportunity to challenge them.

Article 24 mandates that organizations adopt data protection by design and by default, a principle that is crucial for AI systems. This means that privacy considerations must be integrated into the development of AI technologies from the earliest stages. AI systems that process personal data must be designed to ensure that only necessary data is collected and processed, and that robust security measures are in place to protect that data. For AI developers and organizations using AI, this article requires them to minimize the risk of privacy breaches by embedding privacy-enhancing technologies directly into their systems.

Article 12 of the law emphasizes the importance of fair and transparent processing of personal data. For AI systems, this provision is critical because it requires that individuals be informed about how their data is being processed by automated systems. AI systems must provide clear and accessible information about the nature of the data processing, the logic involved, and the potential consequences for the data subject. This transparency is especially important in AI-driven decision-making, where the complexity of algorithms can obscure how decisions are made. By requiring AI systems to explain their processing activities, this provision ensures that individuals are aware of how their personal data is being used and can exercise their rights, such as requesting access or rectification.

Article 4 lays out the core principles of data processing, including lawfulness, fairness, transparency, data minimization, accuracy, and integrity. These principles are directly applicable to AI systems that handle personal data, ensuring that AI technologies do not bypass fundamental data protection standards. For instance, AI systems must process data lawfully, ensuring they have a legitimate basis for processing, such as consent. They must also minimize the data they collect, ensuring that only relevant data is processed, and maintain the accuracy of that data to avoid harm caused by incorrect or outdated information.

Article 5 outlines the conditions for lawful processing of personal data, such as obtaining explicit consent from the data subject, fulfilling a legal obligation, or serving legitimate interests. In the context of AI, this article is particularly important because it governs the legal grounds on which AI systems can process personal data. AI systems must operate within these legal constraints, meaning that if an AI tool processes personal data, it must ensure that there is a lawful basis for doing so, such as informed consent or legitimate business purposes. This is especially relevant for

AI systems that process sensitive data, such as health or biometric information, which require explicit consent or other stringent conditions to be lawfully processed.

Controllers are responsible for ensuring the implementation of appropriate technical and organizational measures to secure personal data. For AI systems, this means deploying strong safeguards like encryption, pseudonymization, and regular security assessments to minimize risks related to data breaches or unauthorized access. Organizational measures would include establishing data protection policies, training staff on AI-related data protection risks, and ensuring regular audits of AI systems to verify compliance with privacy standards.

Article 35 mandates that a DPIA must be carried out when data processing is likely to result in a high risk to the rights and freedoms of individuals, especially when using new technologies. This provision is particularly relevant to AI systems, as they often involve large-scale or complex data processing that can have significant implications for privacy. A DPIA for AI systems would involve assessing the potential risks associated with the deployment of AI, such as profiling, automated decision-making, or the use of sensitive personal data.

While this Law similarly to the GDPR provides a good framework for the protection of personal data, it does not specifically regulate AI. This presents certain limitations when it comes to addressing the unique challenges posed by AI technologies. For example while the law requires that data controllers ensure compliance, it does not provide detailed provisions for accountability in AI-driven decisions. For example, in automated decision-making, it may be difficult to determine who is responsible for decisions made by AI algorithms.

In conclusion, while the law provides a solid foundation for regulating data protection in Kosovo, it does not specifically address the complexities and risks associated with AI systems. AI systems that process personal data are required to comply with the law, but the lack of explicit AI-related provisions leaves several challenges unaddressed, particularly in the areas of algorithmic transparency, accountability, and bias mitigation.

However, two new draft laws currently being developed by the Agency for Information and Privacy (AIP)—the Draft Law on the Protection of Personal Data by Law Enforcement Institutions and the Draft Law for the Protection of Individuals in Connection with the Automatic Processing of Personal Data—represent significant steps forward.[64] These laws could address some of the gaps in the current framework by providing clearer guidance on the use of AI in law enforcement and automated data processing.

### 2.2.3.3. Law No. 08/L-173 on Cyber Security

The Law No. 08/L-173 on Cyber Security safeguards the cyber security of essential services, digital service providers, and critical infrastructure in Kosovo.[65] It aims to align Kosovo's cyber security regulations with EU standards, ensuring that operators of essential services and digital

[64] *Legislative Programme for the Year 2024: Republic of Kosovo, The Legislative Programme for the Year 2024, available at: https://kryeministri.rks-gov.net/wp-content/uploads/2024/02/Programi-Legjislativ-per-vitin-2024-.pdf.*

[65] *Assembly of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, 2023. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933.*

service providers implement adequate security measures. The law is particularly relevant in the context of AI, as AI systems are increasingly being integrated into critical infrastructure, both as solutions for enhancing security and as potential sources of new vulnerabilities.

The law establishes the Cyber Security Agency (CSA), tasked with coordinating and enforcing cyber security measures throughout Kosovo. Article 2 defines the purpose of the law, which is to ensure the security of networks and information systems, particularly for essential services and digital service providers. This provision applies directly to AI systems, as AI technologies are becoming integral to critical infrastructure and digital services. Any AI systems involved in data processing, automated decision-making, or digital service delivery must comply with the law's cyber security provisions to protect against data breaches and unauthorized access, both of which could lead to privacy violations or misuse of AI algorithms.

The law refers to automatic processing in its definition of a computer system, described as a "device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data" (Article 3). This definition is relevant for AI systems, which often rely on automated data processing and decision-making.

Article 5 requires operators of essential services and digital service providers to implement organizational and technical security measures. This is especially important for AI systems, which must be designed and operated with security in mind. AI tools used in cyber security should be designed to adhere to principles like data protection by design and by default, ensuring that systems are resilient against attacks.

Article 7 extends this responsibility to digital service providers, requiring regular risk assessments and monitoring of information systems. AI systems, due to their complexity, must undergo continuous monitoring to detect vulnerabilities and prevent cyber incidents. The inclusion of AI tools in essential services heightens the need for effective security protocols to ensure that AI-driven processes do not introduce new risks.

Article 6 mandates that operators and providers report significant cyber incidents within 24 hours. This applies directly to AI systems that are used in critical infrastructure, as any cyber incidents affecting AI systems, such as data breaches or algorithmic manipulation, must be reported promptly. Failing to secure AI systems can lead to unauthorized use of personal data or manipulation of decision-making processes, both of which could have significant impacts on privacy and human rights.

Article 8 emphasizes the need for incident reports to include comprehensive information, which is crucial for AI-related incidents, as they often involve complex layers of data processing and decision-making. Proper incident reporting ensures that AI-driven breaches are identified and mitigated swiftly, protecting individuals' data and preventing further exploitation.

Article 9 highlights the role of the CSA in coordinating national cyber security efforts, while Article 16 emphasizes international cooperation. AI systems, especially those used in cross-border data exchanges, benefit from clear regulations on international cooperation, ensuring that AI-related cyber incidents are handled in alignment with international standards.

The law is significant for AI, even though it doesn't directly address AI. Its provisions have clear implications for AI systems in terms of security and protecting individual rights.

First, data protection and privacy are crucial when AI systems handle personal or sensitive information. AI systems are increasingly involved in data processing at various levels, and any vulnerabilities in those systems could lead to serious breaches of privacy. This law ensures that AI systems are held to high security standards, reducing the risk of unauthorized access to data or potential misuse of algorithms.

Second, the law's requirements for incident reporting make it easier to ensure accountability. If an AI system causes a data breach or is involved in a cyber-incident, this law mandates swift and transparent reporting. This process helps limit damage and ensures individuals are informed about any risks to their personal data.

Finally, while the law doesn't address bias or discrimination in AI systems, it sets an important precedent for AI tools used in cyber security. AI systems used to monitor and detect threats must be designed in ways that don't unfairly target specific groups or introduce biased decision-making into critical areas like law enforcement or digital services.

#### 2.2.3.4. Criminal Code No. 06/L-074 and the Law No. 08/L-188 on Amending and Supplementing the Criminal Code No. 06/L-074

The Law No. 08/L-188 introduces amendments to the Criminal Code No. 06/L-074 of Kosovo, particularly addressing cybercrimes. [66] The law, while not explicitly mentioning AI, covers a range of offenses related to digital data and cyber security, many of which are applicable to AI systems.

Article 277/D - Unauthorized Computer Access criminalizes unauthorized access to computer systems, data, or services. It is highly relevant to AI systems because advanced AI technologies could be used to gain access to sensitive data or systems without authorization. AI-powered tools designed for hacking or accessing restricted databases could potentially operate autonomously, making this provision crucial for preventing privacy infringements caused by AI-driven cyber-attacks. Unauthorized access could lead to data breaches where private, personal information is exposed, thereby violating individuals' rights to privacy.

Article 277/E - Unlawful Interception of Computer Databases prohibits the unlawful interception of data transmitted electronically, which includes communications, emails, and personal information. AI systems capable of intercepting digital communications or data transmissions without consent fall under this provision. For instance, AI tools used in advanced surveillance techniques or AI-driven cyber espionage that capture sensitive information from individuals or organizations would infringe on privacy rights. The law ensures that such unlawful interception, whether carried out by humans or AI systems, is punishable under the criminal code.

Article 277/F - Impeding the Operation of Computer and Information Systems focuses on impeding or disabling the operations of computer systems, including using cyber tools that disrupt

[66] *Assembly of the Republic of Kosovo, Law No. 08/L-188 on Amending and Supplementing the Criminal Code No. 06/L-074, 2019. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413&langid=2.*

services or cause system failures. AI systems used in cyber-attacks such as Distributed Denial of Service (DDoS) attacks or malware that targets infrastructure can indirectly impact privacy by preventing individuals from accessing secure services or causing the exposure of personal information. Disruptions caused by AI systems to sensitive systems holding personal data would fall under this article's purview.

Article 277/H - Theft of Identity and Credentials criminalizes identity theft and the misuse of personal credentials. AI systems that collect personal information, such as login credentials or biometric data, and use this information to impersonate individuals or commit fraud, would be subject to this law. AI systems can be designed to harvest vast amounts of personal data, leading to identity theft at a large scale. This article is crucial for protecting the privacy of individuals from AI-driven identity theft or unauthorized use of personal credentials.

While Law No. 08/L-188 does not directly mention AI, its provisions are highly applicable to AI systems in the context of privacy rights and the broader framework of human rights. The following sections explore how AI systems may infringe on privacy and how the law provides a legal framework to address these concerns.

AI systems, especially those used in data processing and surveillance, present significant privacy risks. They can collect, analyze, and use vast amounts of personal data, sometimes without explicit consent from the individuals involved. Articles such as 277/D (Unauthorized Access) and 277/E (Unlawful Interception) address AI-driven activities that could lead to unauthorized access to personal data or unlawful interception of communications.  For example, AI systems designed to hack into databases or intercept emails and messages could expose personal and sensitive information, violating individuals' right to privacy. These provisions ensure that AI tools and the individuals or organizations operating them are held accountable under the law for such breaches.

AI systems have the potential to act autonomously, meaning they could commit cybercrimes without direct human intervention. Provisions such as Article 277/H (Identity Theft) are highly relevant in this context. AI systems can be designed to gather personal data, including login credentials, personal identification, or biometric data, and use it for identity theft. By automating identity theft or fraud, AI systems pose a substantial threat to privacy, especially if deployed at a large scale.

The legal framework provided by Law No. 08/L-188 helps address these concerns by ensuring that AI systems, even when operating autonomously, fall under the same rules as traditional actors in cases of identity theft and data misuse.

The provisions on impeding computer systems and unlawful access help ensure that AI systems, which could be weaponized to attack critical infrastructure or personal data repositories, are subject to criminal prosecution. Cyber-attacks led by AI, such as DDoS attacks or AI-generated malware, can disrupt access to secure systems, indirectly impacting privacy by preventing individuals from safeguarding their personal data. Additionally, AI systems capable of breaking encryption or evading security measures can lead to unauthorized access to confidential data, which this law explicitly prohibits.

The Law No. 08/L-188 serves as a critical update to the legal framework in Kosovo for addressing cybercrimes, especially in the context of emerging technologies like AI. While the law does not explicitly regulate AI, it covers the key areas where AI systems could be used to infringe on rights.

### 2.2.4. Freedom of Expression

In this section, we will focus on freedom of expression and examine how the existing legal frameworks in Kosovo safeguard this fundamental right in the context of emerging AI technologies. Similarly to the Privacy section there is no specific law regulating AI, there also isn't a specific media law, specific online media regulation, a law or requirements for establishing online media, and no disinformation regulation,[67] it is essential to explore how existing laws govern freedom of expression, especially as AI systems are increasingly involved in content moderation, automated decision-making, and the dissemination of information.

#### 2.2.4.1. Constitution of Kosovo

Article 40, which guarantees freedom of expression, is particularly relevant when considering AI-driven content moderation. AI systems are now integral to moderating, filtering, and distributing information, particularly on digital platforms. These systems determine what content is allowed to remain online and what gets removed, potentially infringing on an individual's right to express opinions freely.[68] This constitutional protection also includes the right to disseminate and receive information without impediment, which means AI systems must carefully navigate the balance between upholding free speech and removing harmful content. However, the article allows for limitations on freedom of expression when it is necessary to prevent the provocation of violence or hostility based on race, nationality, ethnicity, or religion. This is particularly relevant for AI, as many algorithms are designed to detect and remove such harmful content. Yet, the challenge remains in ensuring these algorithms do not overreach and unjustifiably suppress lawful speech.

Article 42, which guarantees media freedom and pluralism, is central to the discussion of AI's role in content distribution and censorship. The Constitution explicitly forbids censorship, stating that no one can prevent the dissemination of information or ideas through the media unless it is necessary to prevent the provocation of violence or hostility. Additionally, the right to correct untrue or incomplete published information as provided in this article is relevant for AI systems, especially in the era of misinformation. AI tools used in content generation and distribution must ensure accuracy, and individuals should have mechanisms to challenge and correct misleading or harmful content produced or disseminated by AI systems.

#### 2.2.4.2. Law No. 04/L-137 on the Protection of Journalism Sources

[67] *Share Foundation, Regulatory Framework in the Field of Digital Rights, 2021, available at: https://www.sharefoundation.info/wp-content/uploads/Digital-rights-legal-analysis_EN-1.pdf*

[68] *Assembly of the Republic of Kosovo, Constitution of the Republic of Kosovo, adopted April 9, 2008. Available at: https://mapl.rks-gov.net/wp-content/uploads/2017/10/1.CONSTITUTION_OF_THE_REPUBLIC_OF_KOSOVO.pdf.*

The Law on the Protection of Journalism Sources primarily focuses on safeguarding the confidentiality of sources used by journalists.[69] While the law is fundamental in ensuring media freedom and press independence, it is not directly related to freedom of expression in the context of online content moderation, digital media regulation, or AI systems. However, it remains relevant to the broader discussion of how AI technologies may impact journalistic practices and the protection of confidential information.

The law grants journalists the right to withhold the identity of their sources, which is crucial for investigative reporting and protecting individuals who provide sensitive or controversial information. This principle is vital in maintaining a free press, which indirectly supports the exercise of freedom of expression.

In the evolving landscape of media and technology, where AI is increasingly used for data analysis, content generation, and even media surveillance, this legal protection could be interpreted as extending to ensure that AI systems used within media organizations do not compromise the confidentiality of sources. This law may serve as a foundation for requiring that AI-driven systems in the media sector adhere to existing standards of source protection, reinforcing the broader legal framework that supports freedom of expression in Kosovo.

#### 2.2.4.3. Law No. 06L-081 on Access to Public Documents

The Law No. 06/L-081 guarantees the right of every natural or legal person to access public documents produced, received, or maintained by public institutions.[70] While the law does not directly address the use of AI in this process, it provides a flexible framework that could accommodate AI-assisted requests for access.

AI systems could be used by individuals or organizations to automate the submission of requests for public documents. Since the law only recognizes natural or legal persons as legitimate requesters, any AI-generated request must remain legally tied to a person. The responsibility for the request would lie with the individual or entity that programmed or authorized the AI tool.

Additionally, public institutions may also employ AI systems to manage large-scale document requests or automate the process of retrieving and providing access to public documents. If AI systems are used by public institutions, transparency becomes a key issue. Citizens would need to know how the AI systems function, including how they process requests, retrieve information, and make decisions about granting or denying access.

There are potential concerns regarding the excessive or autonomous use of AI by individuals to submit multiple requests. While this is not explicitly regulated by the law, it could lead to ethical and practical issues, such as overwhelming public institutions with a high volume of requests or using the system in a way that might be seen as abusive.

[69] *Assembly of the Republic of Kosovo, Law No. 04/L-137 on the Protection of Journalism Sources, 2013. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=8864.*

[70] *Assembly of the Republic of Kosovo, Law No. 06/L-081 on Access to Public Documents, 2019. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=20505.*

#### 2.2.4.4. Law No. 02/L-65 Civil Law against Defamation and Insult

The Law No. 05/L-021 on Protection from Discrimination serves as a critical legal safeguard against both direct and indirect discrimination in Kosovo, encompassing areas such as employment, education, access to services, and public life.[71] The law protects individuals based on factors such as race, ethnicity, gender, religion, disability, and other characteristics. While the law does not specifically address AI or digital technologies, it has significant implications for the use of AI systems and digital platforms that may influence or perpetuate discriminatory practices.

In the digital era, AI technologies can also be used to monitor, filter, and moderate online content. While these tools are often employed to prevent harmful content, they also raise concerns about digital defamation and insults. If an AI system, directly or indirectly, facilitates online harassment, defamation, or the spread of hate speech targeting protected groups, it could fall under the purview of this law, which seeks to protect individuals from discriminatory or harmful practices. The law could also be extended to address cyberbullying, digital harassment, or defamatory AI-generated content that targets specific individuals or groups based on their protected characteristics.

AI systems, especially those involved in automated decision-making (e.g., hiring algorithms, credit scoring systems, or public service allocation tools), must align with the anti-discrimination principles laid out in this law. Ensuring fairness and transparency in the design and operation of AI systems is critical to complying with this law.

#### 2.2.4.5. Criminal Code No. 06/L-074 and Law No. 08/L-188 on Amending and Supplementing the Criminal Code No. 06/L-074

The Criminal Code No. 06/L-074 and its amendments in Law No. 08/L-188 are also relevant to the balance between freedom of expression and the need to regulate hate speech, racism, xenophobia, and other harmful content online. As AI systems become more prevalent in content moderation and decision-making, it is important to assess how these provisions apply to AI's role in filtering, amplifying, or suppressing digital content.

Article 277/A criminalizes the use of computer systems to distribute content that denies or minimizes genocide or crimes against humanity. This provision, aimed at combating harmful speech, addresses the challenge of maintaining dignity for affected groups while also safeguarding freedom of expression. AI systems could play a role in automatically detecting and distributing such content. However, this raises concerns about whether these systems are capable of distinguishing between harmful content and legitimate discourse, potentially leading to the suppression of lawful speech.

Similarly, Article 277/B targets threats motivated by racism or xenophobia disseminated through computer systems. AI systems designed for content moderation and hate speech detection would be central to enforcing this provision. Yet, there remains the challenge of ensuring that freedom of expression is not unduly restricted through overly broad or biased content moderation practices.

[71] *Assembly of the Republic of Kosovo, Law No. 02/L-65 Civil Law against Defamation and Insult, 2008. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=2503.*

These automated systems must be designed to strike a careful balance between removing harmful content and preserving the right to free speech.

The distribution of racist or xenophobic materials through digital platforms is addressed in Article 277/C, which prohibits such activities. In this context, AI algorithms often filter or amplify content on social media platforms. While the intent is to curb the spread of hate speech, there is a risk of overreach where these algorithms inadvertently censor legitimate speech, especially when they are not designed to handle complex language or cultural nuances. This is particularly concerning if biased algorithms disproportionately target minority voices under the pretense of moderating harmful content.

Article 277/F criminalizes activities that disrupt computer systems, which can interfere with online platforms where individuals express themselves. AI systems, either used for cyberattacks or in censorship efforts, could restrict access to digital platforms and infringe on freedom of expression. The growing reliance on AI in managing access to information and digital spaces must be monitored to ensure that these systems do not unintentionally limit people's ability to voice their opinions or engage in public discourse.

Within Chapter XVII, which outlines criminal offenses against human rights and freedoms, Article 141 penalizes those who incite or publicly spread hatred, discord, or intolerance based on characteristics such as race, religion, sexual orientation, or gender identity. In this context, AI systems involved in content moderation have a critical role to play in ensuring that these types of speech are effectively curbed while avoiding discriminatory bias that could unjustly censor speech.

Additionally, Article 70 stipulates that if a criminal offense is motivated by hatred, it is considered an aggravating circumstance for sentencing. AI systems tasked with identifying or assessing hate crimes may contribute to ensuring the accurate classification of such offenses. However, the effectiveness of these systems depends on their accuracy and impartiality, requiring regular audits to ensure they do not disproportionately target certain groups or individuals based on biased data or assumptions.

Overall, the provisions within the Criminal Code and its amendments reflect the need to regulate harmful online content, particularly in combating hate speech, defamation, and violent threats. The growing use of AI-driven content moderation and automated decision-making systems introduces a critical challenge in ensuring that these technologies do not infringe on freedom of expression.

### 2.2.5. Equality and Non-Discrimination

This sub-section will focus on the legal framework in Kosovo that addresses equality and non-discrimination, particularly in the context of AI technologies. While Kosovo has yet to implement specific regulations governing the use of AI, existing anti-discrimination laws play a vital role in ensuring that AI systems do not reinforce or exacerbate biases or inequalities. These laws are essential in areas such as employment, education, public services, and access to goods, where AI-driven decisions could potentially lead to discriminatory outcomes.

#### 2.2.5.1 Constitution of Kosovo

The Constitution of Kosovo establishes legal framework for ensuring equality and non-discrimination, which has significant implications for the use and regulation of AI technologies. Several key articles from the Constitution lay the groundwork for safeguarding human rights and ensuring that AI systems do not perpetuate or exacerbate bias, inequality, or discrimination.

Article 3, establishes the principle of equality before the law and emphasizes the protection of human rights for all individuals, regardless of ethnicity, gender, or other characteristics. In the context of AI, this provision requires that any AI system used by public institutions must treat all individuals equally and avoid bias or discriminatory practices. AI systems, especially those used for automated decision-making in public administration or law enforcement, must be designed to ensure that decisions made are free from bias and respect the principle of equal treatment.

Article 7 sets out the fundamental values of the constitutional order of Kosovo, including equality, non-discrimination, and the rule of law. These values are particularly relevant when considering the design and deployment of AI systems in Kosovo. Any AI technology used in employment, public services, or other areas must align with these values, ensuring that its operation does not violate the principles of equality and fairness. This article also emphasizes gender equality, which is an important consideration for AI systems that may be involved in hiring, promotions, or other decisions affecting individuals based on gender.

Under Article 22, international agreements related to human rights and equality are directly applicable within Kosovo’s legal framework. This ensures that any future international regulations or agreements on AI, such as those addressing algorithmic fairness or data protection, will automatically become part of Kosovo's domestic law.

Article 24 is central to the protection of individuals from discrimination. It guarantees equal legal protection for all, prohibiting discrimination based on characteristics such as race, gender, religion, and disability. For AI systems, particularly those used in automated decision-making processes, this article mandates that such systems must not discriminate based on these characteristics. AI algorithms, often reliant on historical data, must be designed to ensure they do not unintentionally perpetuate bias or reinforce inequalities.

Article 57 outlines the rights of ethnic, linguistic, and religious communities in Kosovo, ensuring that these groups are free from discrimination. In the context of AI, any system that processes data or makes decisions about individuals from these communities must respect their rights and avoid creating disparate impacts that disproportionately affect these groups. This is especially relevant for AI systems used in public administration or service delivery, where biased algorithms could undermine the constitutional rights of community members.

Article 58 mandates the protection of individuals from discrimination, hostility, and violence based on their identity. This is directly relevant to AI systems used for content moderation, social media monitoring, or public service delivery. AI systems must not be designed or used in ways that facilitate discrimination or hostility. Instead, they must be aligned with the state’s responsibility to protect individuals from such harm. This article also emphasizes the non-discriminatory exercise of rights, reinforcing the need for AI technologies to operate transparently and without bias.

The Constitution of Kosovo ensures equality and non-discrimination, particularly in the context of AI technologies. The principles outlined in Articles 3, 7, 22, 24, 57, and 58 establish legal protections that must be upheld when deploying AI systems in public and private sectors.

### 2.2.5.2. Law No. 06/L-082 on Protection of Personal Data, Law No. 02/L-65 Civil Law against Defamation and Insult and Criminal Code No. 06/L-074

We have previously analyzed Law No. 06/L-082 on Protection of Personal Data**,** Law No. 02/L-65 Civil Law against Defamation and Insult**,** and the Criminal Code No. 06/L-074, particularly in the context of privacy and freedom of expression. However, these laws are also highly relevant when considering equality and non-discrimination, particularly in the context of AI systems and their potential for bias or discriminatory practices.

Law No. 06/L-082 on Protection of Personal Data provides critical protections for individuals' personal data, ensuring that it is processed fairly and transparently. In the context of equality and non-discrimination, the law plays a key role by regulating how personal data is used in automated decision-making systems, including AI systems.

The law outlines several principles of data processing, including lawfulness, fairness, and transparency (Article 4), which are crucial for preventing discrimination. These principles require that personal data used by AI systems be handled in a way that does not create disparate impacts or reinforce existing biases.

Additionally, Article 21 specifically addresses automated decision-making and profiling, requiring that individuals are not subject to decisions made solely by automated systems that significantly affect them, unless specific safeguards are in place. This provision is particularly relevant to AI systems that may be involved in hiring, credit scoring, or access to services, as such systems must ensure that they do not disproportionately disadvantage certain groups based on protected characteristics like gender, ethnicity, or disability.

Law No. 02/L-65 Civil Law against Defamation and Insult primarily focused on protecting individuals from defamation and insults, this law also intersects with equality and non-discrimination. In digital environments, including social media platforms where AI systems are used for content moderation, this law can help ensure that discriminatory insults or defamatory content targeting individuals based on their race, gender, or other personal characteristics are appropriately addressed.

The Criminal Code No. 06/L-074, particularly Article 70, addresses the aggravation of punishment in cases where a crime is motivated by hatred. Hate crimes are defined as any crime committed against an individual, group of individuals, or property, motivated by characteristics such as race, color, gender, gender identity, religion, national origin, sexual orientation, or disability. This provision is essential for AI systems used in content moderation, law enforcement, or risk assessment, as it underscores the legal consequences of crimes motivated by discrimination or bias.

In the context of AI, this law reinforces the importance of ensuring that AI systems are not used to perpetuate discriminatory practices or to amplify hate speech. AI-driven platforms, such as those involved in social media monitoring or crime prevention, must ensure that they do not inadvertently reinforce harmful stereotypes or disproportionately target certain communities based on biased algorithms.

### 2.2.5.3. Law No. 05/L-020 on Gender Equality

The Law No. 05/L-020 on Gender Equality is an important piece of legislation in Kosovo aimed at ensuring gender equality and preventing discrimination based on gender.[72] It covers various areas such as employment, education, public life, and access to goods and services, and is grounded in both national and international frameworks, including the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which is directly applicable in Kosovo.

This law is relevant to our study of equality and non-discrimination in the context of AI systems because it establishes fundamental principles of equal treatment and non-discrimination that AI systems must adhere to when implemented in Kosovo. Article 4 of the law prohibits both direct and indirect gender discrimination and ensures equal access to resources and opportunities in all areas of social and economic life. This principle is crucial when considering AI systems, particularly those used in areas like employment or access to services, as they must be designed and operated in a way that does not reinforce or perpetuate existing gender inequalities.

Moreover, the law requires public institutions to adopt gender-sensitive policies and strategies, which could be directly applied to the development and regulation of AI technologies. Article 5 mandates that all legislative, executive, and judicial bodies must incorporate gender mainstreaming in their decision-making processes, including the development of policies and programs. This requirement highlights the need for AI systems to be gender-responsive and to ensure that gender biases are not embedded in their algorithms.

In addition, Article 15 emphasizes the prohibition of gender discrimination in employment. This is highly relevant when considering the use of AI in recruitment processes, where AI tools must ensure equal opportunities for all genders and avoid biased algorithms that might favor one gender over another. The law's principles also apply to areas like promotion, training, and pay equality, where AI systems can be used for decision-making but must ensure fairness and avoid indirect discrimination.

In the context of AI and human rights, the law is particularly significant as it requires both private and public sectors to implement temporary special measures (Article 6) to accelerate the realization of gender equality.

### 2.2.5.4. Law No.03/L –212 on Labour

The Law on Labour (No.03/L-212) primarily focuses on regulating the employment relationship between employees and employers, ensuring fair labor practices and the protection of workers'

[72] *Assembly of the Republic of Kosovo, Law No. 05/L-020 on Gender Equality, 2015. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=10923.*

rights.[73] Its core principles include prohibiting discrimination, ensuring equal opportunities, and promoting equality in the workplace. Article 5 of the law explicitly prohibits discrimination in employment and occupation based on several factors, such as race, color, gender, religion, and more. This directly aligns with our research on equality and non-discrimination.

In the context of AI, this law is relevant as AI systems could be used in hiring, managing, or firing employees. Such systems must be designed to avoid bias and ensure that employment decisions are made fairly, without discrimination. For instance, if AI tools are used in recruitment or performance evaluation, they must comply with Article 5, which prohibits any form of discrimination in employment. Additionally, the law mandates equal treatment in training, promotions, and working conditions, which would also apply to AI-based systems that might influence these areas.

Regarding human rights, the law provides an essential framework for preventing discrimination in AI applications within employment. It is vital to ensure that AI systems do not perpetuate bias, especially when making automated decisions about hiring, promotions, or dismissals. AI systems used in labor contexts must be transparent, and any decisions made must be in line with the legal framework that protects employees' rights to equality and non-discrimination. Furthermore, Article 17 ensures employees are assigned work based on their qualifications, which AI systems handling internal job placements must respect.

#### 2.2.5.5. Law No. 05/L-021 on the Protection from Discrimination

The Law No. 05/L-021 on the Protection from Discrimination aims at preventing and combating all forms of discrimination in Kosovo. The law prohibits discrimination based on various grounds such as race, gender, nationality, religion, and disability, ensuring that individuals have equal access to rights and opportunities in all areas of life, including employment, education, and public services.

This law is particularly relevant to our research on equality and non-discrimination as it directly addresses the need for equal treatment in society, a principle that also applies to AI systems. AI, when improperly designed or managed, can perpetuate or exacerbate existing biases, leading to discriminatory outcomes in areas such as employment, housing, and public services. Article 1 of the law establishes the principle of equal treatment as a fundamental right, which should be upheld in the use of AI technologies to avoid discriminating against individuals based on protected characteristics.

The law applies to both the public and private sectors and covers a wide range of areas, including access to goods and services, housing, social protection, and employment (Article 2). This means that AI systems used in these sectors must comply with the law's principles of non-discrimination and equal treatment. For example, Article 3 defines both direct and indirect discrimination,

[73] *Assembly of the Republic of Kosovo, Law No. 03/L-212 on Labour, 2010. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=2735.*

ensuring that even practices that are not overtly discriminatory but result in unequal outcomes (such as biased algorithms) are prohibited.

Article 4 specifies various forms of unequal treatment, such as harassment, segregation, and victimization, which could be relevant when analyzing how AI-driven systems moderate content or make decisions in employment or service delivery. AI systems must ensure that their processes do not inadvertently create a hostile or discriminatory environment, particularly in areas like content moderation or automated hiring systems.

Additionally, Article 19 of the law mandates reasonable accommodation for persons with disabilities, ensuring that they have equal access to employment and public services. This is directly relevant to AI systems used in hiring or service provision, as they must be designed to accommodate the needs of individuals with disabilities, ensuring that the technology does not create additional barriers to participation.

#### 2.2.5.6. Law No. 06/L-034 on Consumer Protection

The Law No. 06/L-034 on Consumer Protection aims to safeguard consumers from unfair commercial practices and ensure that their rights are respected in all business-to-consumer transactions. [74] The law covers various aspects of consumer protection, including transparency, fairness, and the prevention of deceptive practices. Although the law does not explicitly mention AI systems, its provisions have important implications for the use of AI.

This law is particularly significant in the context of AI-driven consumer services, such as automated customer support, personalized advertising, and automated product recommendations. Article 6 of the law prohibits unfair commercial practices, which could be extended to the use of AI algorithms that deceive or mislead consumers through biased or inaccurate recommendations. AI systems used in advertising.

Furthermore, the law requires that consumers are provided with clear and transparent information regarding the products or services they are purchasing. This includes information on pricing, terms of sale, and any relevant data usage. AI systems that are involved in the sale of digital products or the provision of digital services must ensure that they adhere to these transparency requirements.

The transparency requirements in Article 9 of the law also extend to advertising and labeling, areas where AI systems play a significant role in the digital marketplace. AI tools that analyze consumer behavior and provide personalized advertisements must ensure that the information presented is not misleading. Misleading consumers through biased or incomplete information could constitute a violation of this article, particularly in cases where AI systems prioritize certain products or services based on manipulative algorithms. Additionally, AI systems that involve automated decision-making must comply with the law's fairness provisions to ensure that consumers are treated equally and that no discriminatory outcomes arise from the automated processes.

[74] *Assembly of the Republic of Kosovo, Law No. 06/L-034 on Consumer Protection, 2018. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=16551.*

# Chapter III: Impact Assessment of AI on Human Rights in Kosovo

AI continues to evolve, its transformative impact on societies worldwide becomes increasingly evident. AI presents unprecedented opportunities for progress however, alongside these benefits, the rapid adoption of AI technologies brings significant risks, particularly to fundamental human rights.

In Kosovo, where AI adoption remains in its infancy, these risks are not yet fully realized. However, as the country embarks on a journey of digital transformation—guided by strategic policies such as the Digital Agenda of Kosovo 2030 and the E-Government Strategy 2023-2027—understanding and addressing the potential human rights implications of AI is critical.

This chapter examines the potential risks AI poses to human rights in Kosovo, focusing on key areas: privacy, freedom of expression, non-discrimination, accountability, and security. Additionally, it will explore how both public and private sector initiatives in Kosovo are utilizing AI, analyzing specific tools and technologies that employ AI, and the implications these may have on human rights. By considering global examples, regional trends, and practical applications of AI in Kosovo, this chapter aims to highlight the challenges that Kosovo might face and offers insights into how the country can mitigate these risks to uphold human rights in an increasingly digital world.

## 3.1. Data Protection and Privacy

AI technologies, particularly those relying on machine learning and big data analytics, thrive on large volumes of personal data to deliver services, optimize systems, and make predictions. This reliance on data, however, poses significant risks to individuals' privacy. Key concerns include mass data collection, lack of transparency, and inadequate accountability, which have sparked global debates about how to regulate AI effectively without infringing on fundamental human rights. While AI offers substantial societal benefits, it also raises significant concerns about privacy violations by various actors, including state actors, private companies, and even terrorist organizations. The absence of transparency and accountability in AI systems exacerbates these concerns, allowing various actors to infringe on privacy rights with little oversight.

### State Actors and Mass Surveillance

State actors have increasingly employed AI technologies to strengthen surveillance mechanisms, often justifying these actions as necessary for national security or public safety. For example, China has created one of the most sophisticated surveillance systems in the world, leveraging AI tools such as facial recognition and predictive policing. These systems are used to monitor the Uyghur Muslim population in the Xinjiang region. The Integrated Joint Operations Platform (IJOP), a big data system used in Xinjiang, tracks individuals' movements, phone activities, and even daily behaviors like power usage, flagging "abnormal" activities for further investigation.

This level of surveillance has led to mass detentions and widespread criticism for violating privacy rights and enabling the Chinese government's oppressive policies.[75]

In addition to China, other governments around the world have adopted AI-driven surveillance technologies, citing crime prevention and counterterrorism as justifications. For instance, the use of automated facial recognition by law enforcement agencies in Europe and the United States has raised alarms about privacy infringements, especially when these technologies are deployed without clear legal frameworks. These systems often operate in a legal gray zone, where citizens may be surveilled without their knowledge or consent, leading to concerns about disproportionate and discriminatory surveillance practices.

### Private Sector and Data Exploitation

The private sector plays a significant role in privacy concerns related to AI, particularly through the monetization of personal data. Meta (formerly Facebook), for instance, has been at the center of multiple privacy scandals, the most notable being the Cambridge Analytica case. Meta's AI-driven algorithms were used to harvest the personal data of over 87 million users without consent, which was later exploited to influence political campaigns. This case highlighted how AI systems, when not properly regulated, can be used to manipulate public opinion and infringe on individual privacy.[76]

Similarly, AI tools in sectors such as healthcare, finance, and retail routinely collect and analyze vast quantities of personal data to offer personalized services or optimize decision-making. In healthcare, AI systems like IBM Watson for Oncology have been criticized for processing sensitive patient data without proper safeguards. While AI can improve diagnostic accuracy and treatment, it raises concerns about data breaches and unauthorized sharing of highly sensitive health information.

The extensive use of AI in credit scoring systems has also sparked debates about transparency, fairness, and bias, especially when financial decisions are made using opaque algorithms that process personal financial data.

### Non-State Actors and Malicious Use of AI

AI technologies have also been exploited by non-state actors, including terrorist organizations and criminal groups, to infringe on privacy and pose security threats. Terrorist groups have adopted AI-driven cyberattacks and hacking tools to infiltrate personal data, breach secure systems, and conduct espionage operations. These groups utilize AI to automate phishing attacks, crack encrypted communications, and harvest personal information for ransom or ideological purposes. The rise of deepfake technologies, which leverage AI to create realistic but false digital content, has also given malicious actors the ability to manipulate images and videos, compromising the privacy and security of targeted individuals.

[75] *Human Rights Watch, Mass Surveillance Fuels Oppression of Uyghurs and Palestinians, 2021. Available at: https://www.hrw.org/news/2021/11/24/mass-surveillance-fuels-oppression-uyghurs-and-palestinians.*

[76] *The Guardian, Cambridge Analytica and Facebook: The Scandal That Rocked the 2016 US Election, 2018. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.*

In addition, corporate espionage has increasingly involved the use of AI to steal trade secrets, manipulate markets, or disrupt competitors' operations. By exploiting AI tools to gain unauthorized access to private information, these actors infringe on both personal privacy and corporate confidentiality. The intersection of AI with cybersecurity creates new vulnerabilities, making both individuals and organizations more susceptible to privacy breaches.

### Data Protection and Privacy in Kosovo

As Kosovo moves forward in its digital transformation, privacy and data protection are becoming critical concerns. While the country is gradually adopting technologies that enhance efficiency and connectivity, the integration of AI in public and private sectors is still in its early stages. This has somewhat limited the number of cases where AI systems have been directly linked to human rights violations.

Despite fewer reported incidents involving AI-driven privacy infringements, Kosovo faces a range of pressing privacy challenges that could be exacerbated by AI systems if not properly addressed. Some of the key issues include:

- Widespread use of CCTV without oversight
- Data leaks, particularly from government agencies
- Uncontrolled sharing of personal data
- Processing of biometric data without clear justification
- Absence of a “once-only” principle for data submission

Kosovo has seen a rise in the deployment of CCTV systems, which are increasingly used for public safety and crime prevention. While these systems are not yet integrated with AI-driven facial recognition, the potential for such integration raises concerns about mass surveillance and privacy violations. Without adequate legal frameworks, the use of CCTV could infringe on the privacy of citizens, particularly in public spaces, where constant monitoring could become the norm.[77][78]

Data leaks, especially from government agencies, are a recurring issue in Kosovo. The country is undergoing a digitization process, with platforms like e-Kosova becoming essential for accessing public services. However, these platforms have been criticized for not adhering to high privacy standards, putting citizens' data at risk. A lack of secure protocols means that personal information, including sensitive data, is vulnerable to breaches.

The practice of sharing personal data across multiple platforms without proper user consent is a significant privacy issue in Kosovo. As digital services expand, both public and private sectors often share personal data between institutions or third parties without proper oversight, increasing

[77] *Agency for Information and Privacy of Kosovo. (2024). Raporti Gjashtemujor AIP 2024 [Mid-Year Report]. Retrieved from https://aip.rks-gov.net/download/raporti-gjashtemujor-aip-2024/.*

[78] *Bellaadem, I. (2023). Balancing Cybersecurity, Artificial Intelligence, and Human Rights: Opportunities and Challenges in Kosovo. Kosovo Foundation for Open Society (KFOS). Retrieved from https://kfos.org/en/publications/132/balancimi-i-sigurise-kibernetike-inteligjences-artificiale-dhe-te-drejtave-te-njeriut-mundesite-dhe-sfidat-ne-kosove.*

the risk of data misuse. AI systems used for data analytics or customer profiling could exacerbate this problem by making it easier to exploit or commodify personal information.[79]

The processing of biometric data, such as fingerprints or facial recognition, is becoming more common in various sectors. However, there is often no clear legal or procedural justification for the use of such data, which opens up significant risks for misuse. AI systems that rely on biometric data for identification or verification could further infringe on citizens' rights if these technologies are deployed without consent or accountability.

Kosovo citizens are often required to submit the same personal data across multiple platforms, increasing the likelihood of data duplication and security breaches. The absence of a “once-only” principle, where citizens' data would be stored securely and only submitted once for all public services, is a major gap in the country’s digital infrastructure. AI could help streamline and secure these processes, but only if privacy standards are enforced.[80]

Deepfakes and AI-generated disinformation have emerged as growing concerns in Kosovo, particularly in the context of media manipulation and misinformation. While deepfakes are not yet a widespread issue, they pose a future risk as AI tools become more accessible and sophisticated. Deepfakes can be used to create misleading content, which undermines trust in public discourse and poses significant privacy risks for individuals targeted by such technologies.[81]

In Kosovo, public institutions are increasingly using digital tools and systems for internal management, many of which process personal and sensitive data. These tools, while essential for efficiency, present significant privacy and cybersecurity challenges. Tools like SMIL (Information System for Case Management) used by the judiciary, ASYCUDA, a digital management system employed by Kosovo Customs, and the Tax Administration of Kosovo (TAK)’s algorithm for risk analysis and case selection, automate various processes and help streamline operations. [82]However, the issue arises when these systems are not regularly updated or adequately maintained due to the lack of institutional capacity and insufficient financial resources. This leaves them vulnerable to data breaches and cyber incidents. Public institutions often lack the technical expertise or budget to continuously improve these systems, ensure their security, or address emerging privacy concerns.

Kosovo citizens, like those in other parts of the world, are also subject to privacy risks posed by international actors, such as large technology companies. Platforms like Meta (formerly Facebook), Google, and others collect vast amounts of personal data, often using AI-driven algorithms to analyze behavior and target users with personalized ads or content. While these

[79] *Bellaadem, I. (2023). Balancing Cybersecurity, Artificial Intelligence, and Human Rights: Opportunities and Challenges in Kosovo. Kosovo Foundation for Open Society (KFOS). Retrieved from https://kfos.org/en/publications/132/balancimi-i-sigurise-kibernetike-inteligjences-artificiale-dhe-te-drejtave-te-njeriut-mundesite-dhe-sfidat-ne-kosove.*

[80] *Open Data Kosovo. (2022). Digital Rights in Kosovo. Retrieved from https://opendatakosovo.org/portfolio/country-situation-report-digital-rights-in-kosovo/.*

[81] *Bami, X. (2024). Kosovo Press Council Updates Code of Ethics to Combat AI Risks. Prishtina Insight. Retrieved from https://prishtinainsight.com/kosovo-press-council-updates-code-of-ethics-to-combat-ai-risks/.*

[82] *Škop, M., Vincze, O., Alishani, A., Arsovski, G., & Izdebski, K. (2021). alGOVrithms 2.0: The State of Play. Open Data Kosovo. Retrieved from https://opendatakosovo.org.*

companies are subject to regulations like the EU's GDPR, Kosovo citizens face additional barriers when it comes to protecting their data.

A significant challenge for Kosovo citizens is that, unlike their counterparts in the EU, they have limited recourse for filing complaints or taking action against these companies. While an EU citizen can leverage the GDPR to file a complaint and have their data rights protected, a Kosovo citizen may find it difficult to do the same, given Kosovo's non-membership in the EU. This places them at a disadvantage when trying to assert their privacy rights against international corporations or state actors.

## 3.2. Freedom of Expression

As we discussed, AI-driven systems, particularly those used for content moderation and filtering, can inadvertently suppress free speech, limit access to information, and stifle public discourse. These issues stem from AI's ability to automate decisions without fully understanding the context of speech, leading to concerns about over-censorship, bias, and the manipulation of online narrative

AI-driven content moderation tools are widely deployed by social media platforms and online forums to detect and remove offensive or harmful content. While this is essential for combating hate speech, cyberbullying, and misinformation, these systems often fail to understand the context behind posts, leading to over-censorship. AI algorithms may inadvertently suppress legitimate speech, especially in situations where subtle language or cultural differences are at play. For example, discussions around political dissent or protests may be wrongly flagged and removed because AI systems misinterpret them as incitements to violence.

AI systems used in content moderation often rely on datasets that reflect existing biases in society. When these algorithms are trained on biased data, they can reproduce or even exacerbate discrimination against certain groups. For instance, AI has been shown to disproportionately target content from minority communities or political activists. This can restrict these groups' ability to participate in public discourse and voice their opinions, thus stifling free expression. In some cases, marginalized groups' content is more frequently flagged for removal, further silencing already underrepresented voices.

AI is not only used to remove harmful content but also plays a central role in generating disinformation. Deepfakes—videos or images manipulated using AI to create convincing yet false depictions of individuals—are a growing concern for the future of free expression. These AI-generated images and videos can be used to undermine trust in the media, discredit political opponents, or spread false narratives, all of which distort the information landscape. The proliferation of AI-driven disinformation campaigns has made it more difficult for individuals to discern fact from fiction, reducing the overall quality of public debate.

Many online platforms have turned to AI moderation as a cost-effective solution for handling the vast amounts of content shared daily. However, this over-reliance on automation can lead to errors that limit free expression. Human moderators are often bypassed in favor of quicker but less nuanced AI systems, which can result in unfair content removal and leave little room for appeal.

Platforms that do not adequately combine AI with human oversight risk creating a system that prioritizes efficiency over fairness(

A significant concern with AI systems is the lack of transparency in their decision-making processes. Content moderation algorithms often operate as "black boxes," where users are unaware of why their posts were removed or flagged. This lack of clarity makes it difficult for individuals to understand the rules governing their online expression and undermines trust in the platforms. Furthermore, the accountability of these AI systems is often unclear, with many companies failing to provide clear processes for users to contest decisions made by algorithms.

### AI and Freedom of Expression in Kosovo

In Kosovo, the increasing role of AI in managing digital content raises concerns about freedom of expression, especially in the context of content moderation and disinformation. While AI tools are becoming integral in filtering and removing harmful content on platforms like Facebook, TikTok, and Twitter, they often operate without understanding the nuanced political and cultural environment in Kosovo. This can result in the over-censorship of legitimate political speech or protest, especially when content is flagged or removed by algorithms without proper human oversight.

Kosovo faces unique challenges when it comes to freedom of expression. Platforms like Facebook and TikTok, which are widely used in the country, often rely on AI-driven algorithms to moderate content. These algorithms, however, struggle with the complexity of Kosovo’s political landscape, where discussions on interethnic tensions, protests, or even criticism of the government may be mistakenly flagged as harmful or inciting violence. This has been especially problematic during high-tension periods, such as the 2023 elections boycotted by Kosovo Serbs or clashes between Kosovo police and protesters.

The National Democratic Institute (NDI) has documented that AI tools have been weaponized in Kosovo to spread disinformation, manipulate public opinion, and exacerbate political tensions. The use of deepfakes and AI-generated content has been particularly alarming, as these tools are being employed to mislead the public, further undermining the quality of public discourse and freedom of expression. In 2023, incidents of AI-driven disinformation surged during times of political instability, heightening interethnic tensions and creating distrust among communities. [83]

Foreign media, particularly from Russia and China, have played a significant role in shaping malign narratives surrounding Kosovo’s political landscape. According to a report by the National Democratic Institute (NDI), Russian state media has actively promoted Serbian nationalism by drawing misleading parallels between Kosovo and Crimea, thus undermining Kosovo's independence. In contrast, Chinese media has primarily focused on criticizing NATO and Western involvement in Kosovo, portraying them as destabilizing influences and questioning the legitimacy of Western-led peacebuilding efforts in the region. These disinformation campaigns are part of

[83] *National Democratic Institute. (2023). Information Disorders in Kosovo. Retrieved from https://www.ndi.org/publications/information-disorders-kosovo-2023-report.*

broader efforts to erode public trust in democratic institutions and weaken support for Kosovo’s sovereignty.[84]

AI-generated disinformation has become an increasingly serious threat to freedom of expression in Kosovo, particularly concerning political and ethnic tensions, such as those between Kosovo and Serbia. Disinformation and propaganda campaigns often target sensitive political issues, including internal conflicts in the north of Kosovo, the ongoing Kosovo-Serbia relations, and discussions surrounding Kosovo's integration into the EU. In recent years, AI tools have been leveraged to amplify false narratives that inflame these tensions, creating challenges for both public discourse and social cohesion. [85]

In response to these challenges, the Kosovo Press Council updated its Code of Ethics in 2024 to address the growing risks posed by AI-driven disinformation and deepfakes. The updated guidelines emphasize the need for transparency in AI use within media, reinforcing the importance of safeguarding freedom of expression while combating disinformation. [86]

Kosovo's media and citizens are subject to the content moderation policies of international platforms like Meta and YouTube, which use AI systems designed for global use. These platforms, while complying with local laws in larger markets, often fail to consider the unique socio-political dynamics of smaller regions like Kosovo. The result is that content relevant to Kosovo’s internal issues may be censored or geo-blocked without sufficient context or consideration of local laws.

One major issue for Kosovo citizens is their limited ability to seek recourse against international tech companies when their content is wrongfully removed. Unlike EU citizens, who are protected by regulations such as the DSA, Kosovo lacks strong legal frameworks that would allow its citizens to challenge content moderation decisions made by global tech giants.

## 3.3. Equality and Non-Discrimination

The increasing use of AI in decision-making processes across various sectors raises significant concerns about equality and non-discrimination. AI systems, while often designed to streamline processes and increase efficiency, can inadvertently reinforce societal biases and discrimination if not properly regulated and audited. These concerns are particularly pressing in sectors such as employment, law enforcement, and public services, where AI algorithms may influence key decisions about individuals’ lives.

A major challenge with AI systems is the potential for algorithmic bias, which can occur when AI models are trained on datasets that reflect existing societal inequalities. When these biases are embedded into AI systems, they can result in discriminatory outcomes, disproportionately affecting marginalized groups. For example, AI-driven hiring systems have been found to favor

[84] *Ibid.*

[85] *TechSoup Global Network, Hive Mind, & Metamorphosis Foundation. (2024). Disinformation and Civil Society Mapping Report - Western Balkans Region. Retrieved from https://metamorphosis.org.mk/wp-content/uploads/2024/09/western-balkans-region_disinformation-and-civil-society-mapping-report-1.pdf.*

[86] *Bami, X. (2024). Kosovo Press Council Updates Code of Ethics to Combat AI Risks. Prishtina Insight. Retrieved from https://prishtinainsight.com/kosovo-press-council-updates-code-of-ethics-to-combat-ai-risks/.*

certain demographic groups over others due to biased training data, leading to discrimination in employment. Similarly, AI used in criminal justice systems, such as predictive policing, has been criticized for disproportionately targeting minority communities.

AI is increasingly being used in public administration and service delivery, but it can have unintended discriminatory effects if the underlying data and algorithms are not properly designed or audited. For instance, AI systems that manage access to social services or determine eligibility for benefits can inadvertently exclude vulnerable populations, such as ethnic minorities or economically disadvantaged groups, based on flawed assumptions embedded in the algorithms. Without regular audits for fairness and transparency, these systems risk perpetuating inequality and deepening social divides.

In law enforcement, the use of AI tools such as facial recognition technology has been shown to have higher error rates for people of color, raising concerns about racial bias and discrimination. These technologies, when applied in contexts like policing or border control, can disproportionately target certain groups, leading to heightened surveillance and unjust treatment. The potential for AI-driven systems to reinforce existing racial and ethnic inequalities is a critical issue that needs to be addressed through strong regulatory frameworks.

AI's role in automated decision-making processes can also lead to the exclusion of certain groups from vital services or opportunities. For instance, in credit scoring or loan approvals, AI systems that rely on historical financial data may disproportionately deny loans to individuals from disadvantaged backgrounds. These systems may perpetuate discriminatory outcomes based on biased data rather than an individual's current circumstances, exacerbating existing inequalities.

To combat these challenges, robust legal protections are essential to ensure that AI systems do not perpetuate discrimination. Many countries, particularly within the EU, have started to address these issues through regulations like the GDPR and the proposed AI Act, which aim to ensure fairness and transparency in AI applications. However, for non-EU countries such as Kosovo, there is still much work to be done to develop comprehensive legal frameworks that can effectively address these concerns and protect against discriminatory AI applications.

As AI becomes more prevalent in decision-making, the risk of embedding societal biases into automated systems grows. It is critical for both governments and private sector actors to adopt ethical AI practices, including regular audits of AI systems, ensuring diversity in training data, and implementing transparency measures to mitigate discriminatory outcomes.

### Equality and Non-Discrimination in Kosovo

While Kosovo has yet to document specific cases of AI-driven discrimination, the increasing adoption of AI systems—particularly under the country's Digital Agenda and E-Government Strategy—suggests that these risks will become more prominent as AI technologies are deployed in public services. As AI starts to play a larger role in decision-making processes within public administration, there are concerns that algorithmic bias could exacerbate existing inequalities, particularly in areas like social services, law enforcement, and public benefits distribution.

In the public sector, AI systems could soon be used for automating decision-making processes, managing public records, or allocating resources. However, these systems, if not designed carefully with fairness and transparency in mind, could disproportionately affect vulnerable populations, leading to discriminatory outcomes. For instance, as more AI tools are integrated into sectors like healthcare and education, there is a risk that these technologies might unintentionally exclude individuals from minority or economically disadvantaged backgrounds due to the biases inherent in training data.

In the private sector, we already see the presence of AI in product recommendations and marketing strategies. Large companies operating in Kosovo, particularly in e-commerce and telecommunications, use AI to propose products or services to customers based on automated data analysis. While this can improve efficiency, it also introduces risks of discriminatory outcomes, such as biased consumer profiling, where certain groups may receive fewer opportunities or access to products due to their demographics or economic status.

Additionally, international companies operating in Kosovo, like Meta or Google, continue to refine their AI-driven systems to enhance services. However, the use of AI by these global platforms presents a potential risk for equality and non-discrimination, particularly as these systems may not be tailored to the local context or Kosovo’s regulatory frameworks. Given the increasing role of these platforms in shaping online content and services, there is a pressing need for Kosovo to ensure that global AI systems comply with local standards on fairness and equality.

# Chapter IV: AI Landscape and Stakeholder Preparedness in Kosovo

The AI landscape in Kosovo is evolving, driven by both public and private sector initiatives aimed at fostering digital transformation. The government has made strides in modernizing its services through strategies like the Digital Agenda of Kosovo 2030 and the E-Government Strategy 2023-2027, which prioritize the integration of AI technologies into key sectors such as healthcare, education, and public administration. These efforts are still in the early stages, but they signal a commitment to leveraging AI to enhance governance and public service delivery.

The private sector has been quicker to adopt AI tools, especially in industries like telecommunications, e-commerce, and finance. Companies are increasingly using AI-driven systems for customer service automation, data analysis, and personalized marketing, reflecting the growing role of AI in business operations. Despite these advancements, many businesses in Kosovo face challenges related to infrastructure, technical expertise, and regulatory support, limiting the widespread use of AI.

Civil society organizations and international donors have also played a significant role in advancing AI development in Kosovo. NGOs like Open Data Kosovo are working to raise awareness of AI's potential and promote ethical AI usage. International donors, including USAID, the EU, and UNDP, have supported various digital transformation projects, funding initiatives aimed at building AI capacities and ensuring that Kosovo aligns with European and global standards in technology governance.

The general public in Kosovo, particularly the youth, has shown an increasing interest in AI tools, especially popular applications like GPT models and AI-based chatbots. Young people, tech enthusiasts, and startups are experimenting with AI in creative ways, but overall public understanding of AI's capabilities and risks remains limited.

In this chapter, we will explore the current state of AI adoption in Kosovo, including the role of key stakeholders such as the government, private sector, civil society, and international donors. We will also examine the findings of two surveys: one with key players in Kosovo's AI ecosystem and another with the general public, focusing on their preparedness for the challenges and opportunities presented by AI. The chapter will highlight key gaps and opportunities in Kosovo's AI landscape and offer recommendations for improving stakeholder preparedness and fostering responsible AI adoption.

## 4.1. Key Stakeholders in Kosovo's AI Ecosystem

Defining Kosovo's AI ecosystem is challenging due to the lack of comprehensive research and the fact that AI adoption is still in its early stages. The ecosystem is not fully established, and much of the activity surrounding AI remains unstructured, leaving significant gaps in understanding who the primary actors are and how AI is being integrated into the country's broader digital landscape. Nevertheless, as AI technologies gradually take hold, it is crucial to identify and analyze the key stakeholders who are currently, or will soon be, influencing AI development in Kosovo.

In this section, we will divide these stakeholders into four categories: public institutions, the private sector, civil society and international organizations, and the general public. By examining these groups, we aim to better understand who is shaping Kosovo's AI environment and how prepared they are to handle the opportunities and risks that AI presents.

### Public Institutions

The role of public institutions in shaping Kosovo’s AI landscape is essential, as they provide the legal, regulatory, and infrastructural support necessary for AI adoption and innovation. While AI development in Kosovo is still in its early stages, several key public institutions are already engaging with digital transformation initiatives, laying the groundwork for future AI integration. These institutions will be crucial in establishing the ethical, legal, and operational frameworks needed for AI to be responsibly adopted across both public and private sectors.

The Ministry of Economy is one of the primary institutions responsible for driving AI development in Kosovo, particularly through its role in promoting digital infrastructure and fostering innovation in telecommunications and information technology. The Ministry works to create policies that encourage technological advancement while ensuring that AI systems align with national economic goals. It is instrumental in facilitating the integration of AI into business sectors and public services.

The Agency for Information Society (AIS) oversees the implementation of ICT policies across Kosovo's public institutions. Its role in managing the country's e-governance strategy is critical, as many of the digital transformation initiatives, including potential AI-driven public services, will be under its jurisdiction. As the executive agency responsible for IT project oversight, the AIS is central to ensuring that AI tools are integrated into government systems in a way that aligns with Kosovo’s digital strategy.

The Agency for Information and Privacy (AIP) is responsible for overseeing the implementation of data protection and privacy laws in Kosovo, particularly those related to personal data processing. As AI-driven systems that process large datasets become more prevalent, the AIP will play a critical role in ensuring that AI applications respect citizens' privacy and adhere to transparent and accountable data processing practices. By regulating the use of personal data in both public and private sectors, AIP will help safeguard individuals' rights in the digital age. Furthermore, AIP’s mandate to ensure access to public information will align with broader efforts to maintain transparency and trust in AI systems as they are integrated into national infrastructure.

The Cybersecurity Agency (CSA) is responsible for implementing cybersecurity measures across Kosovo, ensuring the protection of both public and private digital infrastructures. As AI systems become more widely adopted in various sectors, the CSA will help protect these technologies from cyber threats such as data breaches and hacking. By developing and enforcing robust cybersecurity protocols, the CSA will ensure that AI-driven technologies are secure and resilient, supporting Kosovo's ongoing digital transformation. This will be essential in fostering public trust and safeguarding national digital assets as AI becomes an integral part of the country’s technological landscape.

The Digital Transformation Commission (DTC) is a high-level governmental body established to oversee and coordinate Kosovo's digital transformation efforts across public institutions. Chaired by the Prime Minister, the DTC ensures that the country's digitalization strategies, including the integration of AI technologies, are implemented effectively. As Kosovo continues its path toward e-governance and AI-driven services, the DTC will help provide strategic direction and ensure that these initiatives align with broader national goals for modernization and efficiency. By centralizing digital oversight, the DTC plays a critical role in promoting collaboration across ministries and institutions, driving innovation, and ensuring that digital technologies, including AI, are integrated into public services in a coordinated and secure manner.

The Independent Media Commission (IMC) is responsible for regulating the broadcasting and media sectors in Kosovo, ensuring compliance with laws governing media content and broadcast frequencies. As AI technologies become more involved in media production, distribution, and content moderation, the IMC will help regulate AI-generated content, ensuring that it adheres to ethical standards and combats issues such as disinformation and deepfakes. The IMC should propose guidelines for the responsible use of AI in media, which will play a pivotal role in maintaining transparency and accountability in Kosovo’s digital media landscape.

In addition to the key institutions already discussed, several others, though playing a lesser role, ought to contribute to Kosovo’s AI landscape. The Kosovo Parliament should develop the legislative framework necessary to regulate AI technologies, while the Ministry of Justice should oversee the ethical and legal use of AI, particularly regarding privacy and discrimination.

The Police, Judiciary, and Prosecution should adopt AI tools for crime prevention and case management, addressing concerns around privacy and fairness. The Ministry of Industry, Entrepreneurship, and Trade, through its Consumer Protection division, should regulate AI’s role in digital markets, ensuring fair practices in e-commerce.

The Ombudsperson should protect citizens from AI-related rights violations, such as discrimination, while public universities should lead AI research and capacity-building, cultivating the expertise needed for Kosovo’s digital transformation. Together, these institutions should play crucial roles in building Kosovo’s ethical and legal AI ecosystem.

### Non-Public Institutions

In addition to public institutions, various nonpublic institutions such as non-governmental organizations (NGOs), media outlets, international organizations, private companies and universities are actively contributing to Kosovo's evolving AI landscape. While their direct influence on AI regulation may be more limited, these stakeholders play crucial roles in shaping the country's AI adoption and innovation.

NGOs such as the Innovation Center Kosovo (ICK), STIKK (Kosovo ICT Association), Open Data Kosovo (ODK), and the Jakova Innovation Center (JIC) are at the forefront of promoting tech-driven innovation and raising awareness about the ethical use of AI. Organizations like Balkan Investigative Reporting Network (BIRN), Institute for Technology and Society (ITS), Kosovo Journalists Association (KJA), and the Kosovo Foundation for Open Society (KFOS) are essential in advocating for digital rights, transparency, and the responsible use of AI in media and public services.

The media sector, represented by outlets like Kosovo 2.0, Sbunker, and Hibrid, is also engaging with AI, particularly in discussions surrounding disinformation and AI-driven content moderation. These platforms have an important role in educating the public about the societal impacts of AI and holding institutions accountable for their use of such technologies.

International organizations are pivotal in supporting Kosovo's digital transformation and AI adoption through funding and capacity-building initiatives. Key players include UNMIK, HELVETAS, Open Society Western Balkans, USAID, GIZ, NDI, the EU, and UNDP, all of which help align Kosovo’s AI policies with international standards. These organizations offer expertise, technical assistance, and financial resources to ensure that AI is implemented in a way that respects human rights and ethical standards.

Universities such as RIT Kosovo, UBT, and AAB play a crucial role in fostering AI research and developing talent. By offering AI-related courses and supporting research initiatives, these institutions are preparing the next generation of AI professionals who will contribute to Kosovo’s digital economy.

The private sector in Kosovo is also expanding its engagement with AI, with telecom companies, technology firms, and startups increasingly adopting AI tools for data analytics, customer service automation, and business process optimization. Companies involved in AI innovation are likely to expand their AI capabilities, contributing to the growth of Kosovo’s tech ecosystem and driving economic development.

AI usage among Kosovo's general public is steadily increasing, particularly among younger generations who are embracing technologies like ChatGPT and other AI-driven apps. Many citizens are using these tools for everyday tasks such as language translation, content generation, and personalized assistance, reflecting a growing awareness of AI’s practical benefits. The proliferation of smartphones and improved internet access have made AI tools more accessible to a broad audience. However, while the adoption rate is rising, especially in urban areas and among tech-savvy youth, there remains a gap in AI literacy among the wider population, highlighting the need for public awareness initiatives to ensure responsible and informed usage of these technologies in Kosovo.

Together, these stakeholders form a collaborative network that supports Kosovo’s AI adoption, advocating for innovation, ethical practices, and alignment with global standards.

## 4.2. Stakeholder Preparedness in Kosovo

In order to gauge the level of preparedness for AI adoption in Kosovo, two surveys were conducted. The first survey involved 25 key stakeholders representing various public and non-public institutions, including government bodies, private companies, civil society organizations, and academic institutions. This survey aimed to assess how prepared these entities are to integrate and manage AI technologies, focusing on their technical capacity, regulatory frameworks, and perceived challenges.

Additionally, an online survey was conducted with 230 respondents from the general public. The goal of this survey was to measure public awareness of AI technologies, their understanding of the benefits and risks associated with AI, and their readiness to engage with AI-driven services.

However, it is important to acknowledge some limitations of these findings. The relatively small sample size of key stakeholders and the limited scope of the online survey restrict the generalizability of the results. With only 230 respondents in the public survey, and given that it was conducted online, the sample may not fully represent the broader population.

**Key Stakeholders**

The survey included 25 key stakeholders from various sectors. The largest group was civil society, representing 28% of respondents, followed by the private sector with 24%. Academia accounted for 16%, while the executive branch made up 12%. Both media and the judiciary contributed 8% each, international organizations accounted for 4% however we did not receive any answers from the legislative branch. This breakdown provides a balanced view across multiple sectors involved in AI-related activities in Kosovo.

From the survey responses to the question, "*How informed are you about Artificial Intelligence (AI) and its global developments?*" the data shows that 32% reported being very well-informed, and an additional 28% stated they were well-informed. This indicates that 60% of the surveyed stakeholders have a solid understanding of AI and its global trends. Meanwhile, 36% considered themselves moderately informed, reflecting a reasonable awareness but room for growth in knowledge. Only 4% of stakeholders said they were minimally informed, and no one selected "not informed at all."

The results demonstrate that a majority of respondents, approximately 96%, possess at least a moderate level of knowledge about AI and its global developments. This suggests that most key stakeholders are relatively aware of AI's potential and its current trajectory. However, there remains a need to ensure that those with more limited understanding, though a small group, receive further education and capacity-building, especially as AI becomes more integral to various sectors in Kosovo.

In the survey question about the main AI applications used in the workplace, respondents were able to choose multiple options to reflect the variety of AI tools utilized in their organizations. The results show that 64% of stakeholders use AI for data processing, and 56% rely on AI for data analytics, indicating a strong emphasis on managing and interpreting large datasets.

Process automation was selected by 44%, highlighting its role in improving efficiency by automating routine tasks. Other applications, such as natural language processing (NLP) and recommender systems, were less commonly used, with 24% and 20% of stakeholders selecting these options, respectively. Facial recognition and biometric tools were the least used, cited by 16%, reflecting the more niche use of AI for security and identification purposes.

The ability for respondents to select multiple AI applications indicates that many stakeholders are integrating AI in several areas of their operations. The heavy reliance on data processing and analytics suggests that most organizations are leveraging AI for data-centric tasks, while more advanced applications like NLP and facial recognition are less widespread but could see increased adoption as AI infrastructure and understanding grow in Kosovo.

In response to the question about the perceived impact of AI on specific human rights areas in Kosovo, the results showed a mix of positive and negative perceptions across different rights. Here's a breakdown of the responses:

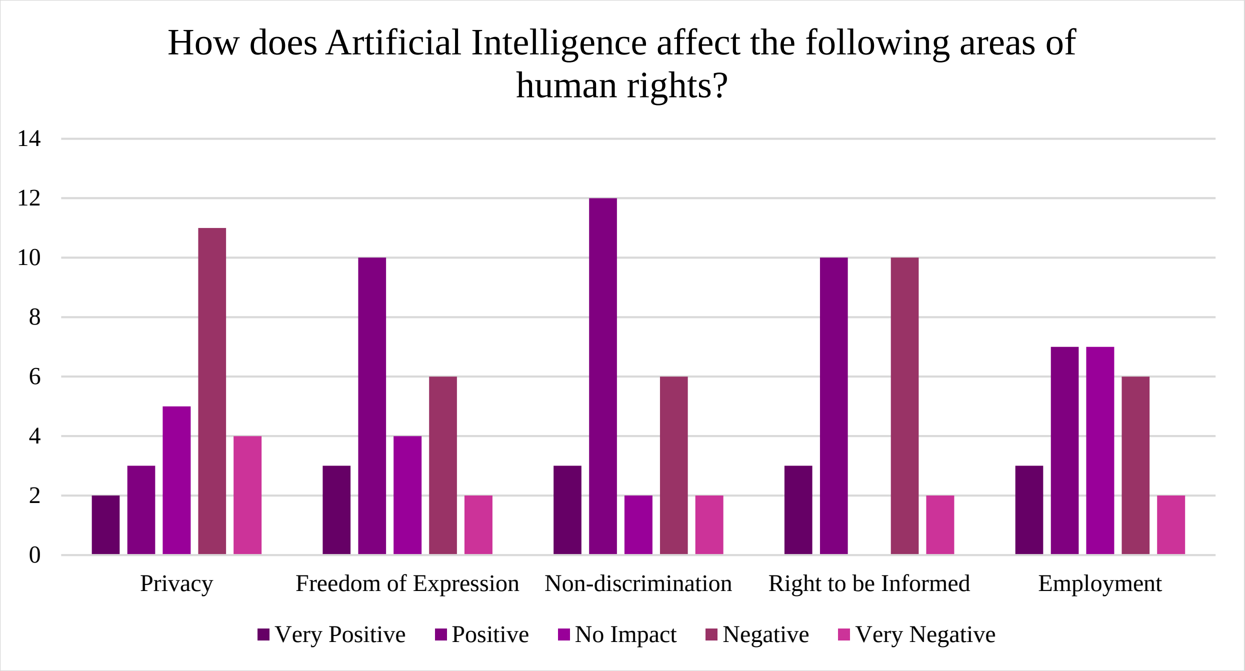
Of the respondents, 8% felt AI had a very positive impact on privacy, while 12% saw a positive impact. However, concerns about privacy were more prevalent, with 28% identifying a negative impact and 32% perceiving a very negative impact. Additionally, 20% believed AI had no significant impact on privacy.

For freedom of expression, 8% believed AI had a very positive impact, and 32% identified a positive impact. On the other hand, 24% felt AI had a negative impact, and 16% saw a very negative impact. 20% felt AI had no impact in this area.

In the area of non-discrimination, 16% believed AI had a very positive impact, while 28% felt it had a positive impact. However, concerns about AI's potential to perpetuate biases were still evident, with 28% identifying a negative impact, and 8% seeing a very negative impact. 12% saw no impact.

When it came to the right to information, 4% felt AI had a very positive impact, and 12% noted a positive impact. However, concerns about disinformation and the manipulation of information were significant, with 32% seeing a negative impact and 40% perceiving a very negative impact. 12% saw no impact.

In the area of labor rights, 12% believed AI had a very positive impact, while 28% saw a positive impact. However, 24% identified a negative impact, and 20% saw a very negative impact. 16% felt AI had no impact on labor rights.



In response to the question regarding the existence of specific laws or policies in Kosovo that regulate the use of Artificial Intelligence (AI) and the protection of human rights, 12% of respondents indicated that they were aware of such regulations. However, a majority, 56%, responded that they believed there were no AI-specific laws or policies currently in place. Additionally, 32% expressed uncertainty, indicating they were not sure whether any regulations existed.

This result highlights a significant lack of awareness or clarity regarding AI legislation in Kosovo. The fact that more than half of the respondents believe there are no such laws, combined with a large portion expressing uncertainty, suggests either a gap in the regulatory framework or a failure to effectively communicate existing legal provisions. This underscores the importance of raising public awareness and providing legal clarity about AI governance and its impact on human rights in Kosovo. As we have already stated, there is no current law that specifically regulated AI.

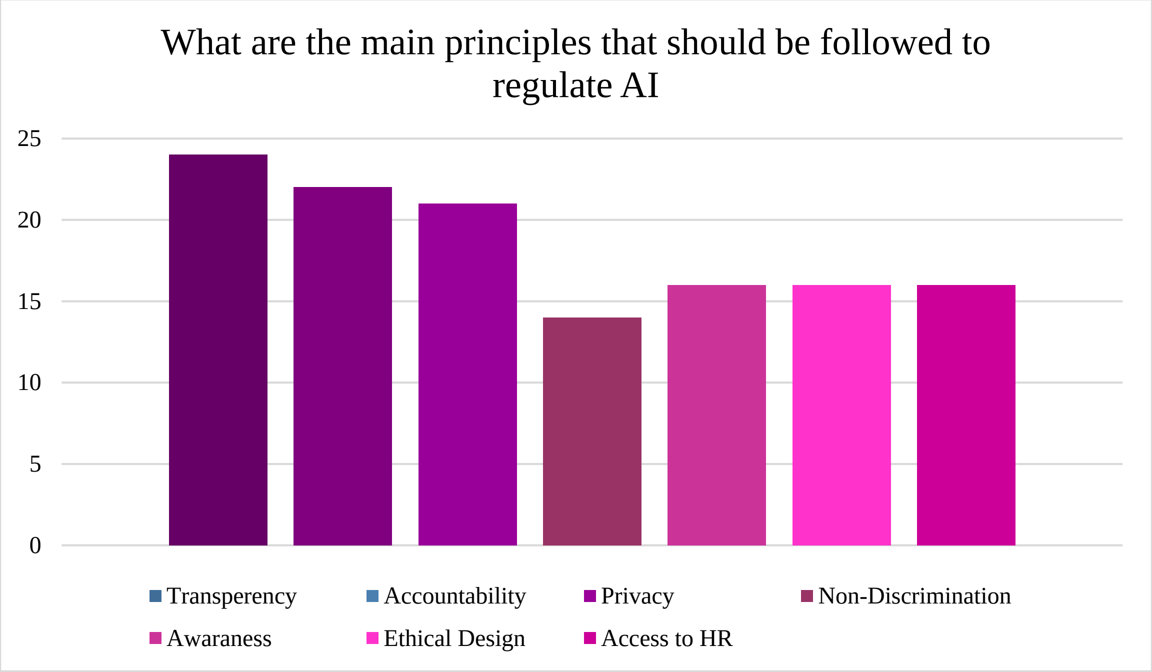
When asked how effective the current national laws and policies in Kosovo are in addressing concerns related to human rights in the context of AI, the responses showed a clear lack of confidence in their effectiveness. Only 8% considered the laws to be very effective, and another 8% deemed them effective. In contrast, 52% felt that the laws were not very effective, while 32% considered them moderately effective.

These results indicate that a majority of stakeholders believe the current legal and policy framework is insufficient in addressing the potential human rights issues that AI may present. This lack of confidence underscores the need for more robust legal measures and improved implementation to better safeguard human rights as AI becomes increasingly prevalent in Kosovo.

In the question regarding the key principles that should be followed to keep AI under control and protect human rights, respondents were allowed to choose more than one option. The overwhelming majority, 96%, selected transparency, indicating a strong belief that AI systems must be transparent in their operations. 88% emphasized the importance of accountability, suggesting that mechanisms to hold AI systems and their operators responsible are crucial.

Privacy and security were also significant concerns, with 84% highlighting the need for stringent data protection measures. Non-discrimination was chosen by 56%, reflecting concerns about the risk of AI systems perpetuating biases. Additionally, 64% selected principles such as awareness, access to human rights, and ethical design, underscoring the need for AI systems to be developed with ethical considerations and human rights at their core.

These results reflect a broad consensus that transparency, accountability, and privacy are the most important principles to be upheld when deploying AI systems to ensure human rights protections in Kosovo.



In response to the question of whether the government should regulate the use of AI to protect human rights, 60% strongly agreed, indicating that they believe it is absolutely necessary for the government to implement AI regulations. An additional 20% felt that the government should regulate AI to a large extent, while 16% agreed that regulation was needed but only to a limited extent. Only 4% believed that regulation was unnecessary, and no respondents selected the option for having no opinion.

These results clearly show a strong demand among stakeholders for the government to take an active role in regulating AI to ensure the protection of human rights, with the majority favoring comprehensive or substantial regulation.

In response to the question of how prepared the organization or institution is to address the ethical issues related to AI, 12% felt their organization was very prepared, and 20% indicated they were prepared. However, a larger portion, 32%, rated their organization as moderately prepared, suggesting that there is some groundwork in place, but more progress is needed. Additionally, 24% felt their organization was not well-prepared, and 12% believed they were not at all prepared to handle ethical concerns surrounding AI.

These results indicate that while some organizations in Kosovo are beginning to address the ethical implications of AI, there remains a significant portion that feels unprepared, highlighting the need for capacity building and increased focus on AI ethics.

The responses to the question, *"What resources or support would help improve your organization's capacity to manage human rights issues related to AI?*" revealed several recurring themes and insights.

One of the most common responses emphasized the need for training. Multiple participants explicitly mentioned the importance of workshops, video tutorials, and informative sessions focused on AI and its implications for human rights. There were also specific calls for training tailored for journalists and staff education to better understand AI's potential risks and ethical considerations. This points to a broad recognition that capacity-building through structured educational programs is critical for organizations in Kosovo to manage AI-related challenges effectively.

Several respondents mentioned awareness initiatives, particularly around privacy and security issues, indicating that there is a gap in understanding the ethical implications of AI technologies. Additionally, participants called for the development of internal ethical codes within institutions and for raising awareness among public officials regarding AI's impact. The focus on ethics underscores the need for comprehensive frameworks that promote responsible AI use.

A few responses highlighted the need for institution-specific regulations, such as drafting internal policies to manage AI and standard operating procedures (SOPs). This shows that beyond education, stakeholders recognize the necessity of having structured guidelines within organizations to manage AI responsibly.

There was also a call for more expert support, with participants noting the need for legal expertise and technical consultation. These responses reflect a need for external specialists to guide organizations in navigating AI's complexities, particularly in human rights and legal contexts. Partnering with international organizations or civil society to gain access to AI expertise was also seen as a beneficial strategy for improving organizational capacity.

Some respondents mentioned the need for advanced tools that can help monitor and assess AI systems to ensure they adhere to ethical standards. This demonstrates that organizations not only require educational support but also technological resources to evaluate the real-world applications of AI in relation to human rights.

There was a strong emphasis on collaborative efforts with international organizations and civil society groups. These partnerships are seen as essential for sharing knowledge, resources, and developing joint policies on AI and human rights.

Some respondents highlighted the need to improve legislation related to AI and to gain insights from international case law regarding how AI-related issues have been treated in other countries. This reflects an awareness of the need for legal clarity and comparative legal analysis to manage the challenges posed by AI.

In conclusion, the common themes in the responses suggest a clear need for training, awareness programs, and policy development to better manage AI-related human rights issues. Moreover, organizations are seeking external expertise, monitoring tools, and international collaboration to enhance their capacity in this field. The feedback indicates that while there is growing concern about AI, organizations feel they are underprepared and need significant support to address these challenges effectively.

The responses to the question *"What steps should be taken at the national level to ensure that AI technologies are used ethically and in line with human rights?"* focused heavily on the need for legal regulation and public awareness.

A significant portion of the respondents called for the drafting and implementation of specific laws to regulate AI. These laws should focus on preventing the misuse of AI and ensuring that it aligns with human rights standards, particularly regarding privacy, data protection, and non-discrimination. Additionally, there were suggestions for establishing a dedicated authority or institution to oversee AI usage and ensure compliance with these laws.

Alongside regulation, respondents emphasized the importance of public awareness campaigns and training programs to educate both the general public and professionals about the ethical implications of AI. There was also recognition that while legal frameworks are essential, technical solutions should also play a role in managing AI issues without creating excessive bureaucratic layers.

Another recurring theme was the call for collaboration with international organizations and foreign states, acknowledging that Kosovo cannot tackle all AI-related challenges on its own, particularly regarding international companies and cross-border AI issues.

In summary, the key themes were legal reform, awareness efforts, and international cooperation, all aimed at ensuring the ethical use of AI in Kosovo.

The responses to the question *"Do you have specific suggestions for improving the legal framework, awareness, and ethical practices related to AI in Kosovo?"* highlight three main areas of focus: the need for specific legislation, harmonization with EU regulations, and increasing public awareness.

Many respondents emphasized the lack of specific AI legislation in Kosovo and called for the creation of dedicated laws. Some suggested that existing laws on data protection and consumer rights could be adapted to include AI, while others advocated for drafting new laws that would reflect the complexities of AI technologies. There was also support for aligning with the EU's new AI Act, ensuring that Kosovo's regulations are in line with European standards. Additionally, there were suggestions for the establishment of a dedicated institution or office to oversee AI and emerging technologies, which would monitor compliance with ethical standards.

In terms of awareness, several respondents highlighted the importance of educating both developers and users of AI. This would involve creating a clear legal system to ensure that AI is developed and used responsibly. Others mentioned the need for public campaigns, particularly targeting older generations, to raise awareness about AI's impact on human rights. These campaigns could be carried out through media outlets such as television, where older audiences are more likely to engage.

Finally, there was a recurring suggestion to establish ethical guidelines within public and private institutions, ensuring that AI technologies are developed and applied in an ethical manner. Respondents also proposed forming a commission of experts from diverse fields—technology, law, and human rights—to develop policies and oversee the ethical use of AI, in alignment with international best practices.

In summary, the suggestions centered on creating AI-specific legislation, harmonizing regulations with EU standards, and enhancing public awareness through targeted campaigns. Additionally, there was a strong call for establishing ethical frameworks and expert bodies to ensure that AI is implemented responsibly in Kosovo.

### General Public

In response to the question, *"Have you ever heard of Artificial Intelligence?"* 78.4% indicated that they had heard a lot about AI, while 19.8% mentioned that they had heard a little. A small minority, 1.8%, stated that they had never heard of AI, and 0.9% were unsure.

When asked *"How informed are you about Artificial Intelligence technologies?"* the results revealed a lower level of knowledge. Only 14.4% considered themselves to be well-informed, while 27.9% felt moderately informed. The largest group, 35.1%, stated they were somewhat informed, and 19.8% admitted they were poorly informed. Additionally, 2.7% acknowledged being not informed at all.

These findings show that while awareness of AI is high, with nearly all respondents having heard of it, detailed knowledge of AI technologies is significantly lower. However, we remain somewhat skeptical of the responses, as the level of self-reported knowledge, though lower than awareness, still seems relatively high. It is possible that many respondents may have overestimated their understanding of AI, suggesting that further efforts to improve public education and understanding on the topic are still crucial.

In response to the question, *"Do you think Artificial Intelligence has an impact on your daily life?"* 27% felt that AI has a significant impact on their daily lives, while the majority, 54.1%, indicated that AI has a moderate impact. 9.9% stated that AI has a small impact, and 3.6% believed that AI has no impact on their lives. Additionally, 5.4% were unsure about the impact of AI on their day-to-day activities.

When asked, *"In which area do you think Artificial Intelligence will impact your life the most?"* the responses were more varied. The largest group, 37.8%, believed that AI would have the greatest influence on their career and work life. This was followed by 25.2%, who felt AI would most significantly affect education and learning. Other key areas mentioned were personal life (11.7%), public services and administration (8.1%), business and economy (5.4%), and healthcare (5.4%). A small portion of respondents, 7.2%, thought AI would impact all areas of life.

These results suggest that while many people perceive AI as having a moderate impact on their daily lives, the awareness of AI's potential influence is focused largely on professional and educational domains. The majority believe that AI will impact their work and career, reflecting growing awareness of AI’s role in job markets and automation. At the same time, significant attention is also given to AI's role in education, personal life, and public administration, indicating a broad expectation that AI will reshape multiple aspects of both personal and professional life.

The next set of questions directly addresses public perceptions of AI's impact on three key human rights: privacy, freedom of information, and non-discrimination.

In response to the question, *"Are you concerned about the protection of your privacy due to the use of Artificial Intelligence?"* 25.2% indicated they are very concerned, and 49.5% reported being somewhat concerned. A smaller percentage, 17.1%, stated they were not very concerned, and 5.4% were not concerned at all. Additionally, 2.7% were unsure.

When asked, *"Do you believe that Artificial Intelligence technologies can spread inaccurate or false information that could influence public opinion?"* 36% strongly believed that AI could do so very often, and 46.8% felt it could sometimes. Meanwhile, 9.9% thought this could happen rarely, 1.8% believed it would never occur, and 5.4% were unsure.

The third question asked, *"Do you think Artificial Intelligence can cause discrimination in society (e.g., in employment, services, etc.)?"*. Here, the majority of respondents (52.3%) agreed that AI could sometimes cause discrimination, and 18% believed AI could cause discrimination often. 12.6% thought it would happen rarely, and 9.9% did not believe AI would cause discrimination, while 7.2% were unsure.

These results indicate a high level of concern about AI’s potential to infringe on privacy rights, with the majority of respondents expressing worry about the impact of AI on their personal privacy. Similarly, there is significant concern that AI could spread misinformation, with many respondents perceiving this as a real threat to freedom of information. Lastly, public awareness of AI’s potential to cause discrimination in areas such as employment and services is notable, as over half of respondents believed AI could contribute to discriminatory practices, either often or occasionally. Together, these findings highlight the public's awareness of AI’s potential risks to fundamental human rights.

In response to the question, *"What do you think is the most important issue to consider when regulating Artificial Intelligence?"* the majority of respondents, 54.1%, prioritized the protection of privacy and personal data as the most important issue. 23.4% believed that ensuring security and protection against technology abuse was the most critical factor. Another 10.8% highlighted the need for transparency in how AI functions, and 7.2% stressed the importance of preventing discrimination and ensuring equal treatment. Finally, 4.5% emphasized the accountability of those who develop and use AI systems.

These findings are consistent with the concerns expressed in the previous questions about privacy, misinformation, and discrimination. In particular, the overwhelming emphasis on privacy protection aligns with the earlier finding that a significant portion of respondents are concerned about how AI might affect their personal privacy. The second most important issue, security and protection against abuse, also echoes the public's worry about the spread of misinformation and AI misuse. Meanwhile, the relatively smaller focus on discrimination prevention and accountability reflects the moderate level of concern about AI causing societal discrimination observed in the previous questions.

Overall, these responses suggest that when it comes to regulating AI, the public is most concerned with privacy and security, followed by transparency and discrimination, reinforcing the need for a comprehensive and well-balanced approach to AI regulation.

In response to the question, *"Are you aware of any specific law or policy in Kosovo that regulates the use of Artificial Intelligence?"* 64.5% answered no, indicating that the majority of the public is unaware of any AI-specific legislation in Kosovo. Meanwhile, 27.3% stated they were unsure, and only 8.2% claimed to know of a law or policy regulating AI.

For the question, *"Do you think the government should regulate the use of Artificial Intelligence to protect your rights?"* an overwhelming majority, 83.8%, believed that the government should regulate AI to ensure the protection of their rights. 9.9% disagreed, stating that government regulation was not necessary, while 6.3% had no opinion on the matter.

These results clearly highlight the lack of awareness regarding AI-specific legislation in Kosovo. Most respondents are either unaware or unsure about any legal frameworks regulating AI. At the same time, there is a strong demand for government intervention to regulate AI, with nearly 84% of respondents agreeing that regulation is necessary to protect their rights. This indicates a clear public expectation for government action in the AI space, even if current awareness of existing laws is low. The gap between legislative awareness and desire for regulation suggests an opportunity for both public education and the development of clear AI policies.

In response to the question, "*Do you believe that Artificial Intelligence technologies will improve the quality of life for people in Kosovo in the future?*" the majority of respondents, 60.9%, felt that AI would have a positive impact and believed it would improve the quality of life. 20% were even more optimistic, predicting that AI would have a very positive impact.

Meanwhile, 9.1% believed that AI would have no impact on the quality of life. A smaller portion, 6.4%, felt that AI would have a negative effect, and 3.6% believed it would have a very negative effect.

The majority of the public holds a positive outlook regarding AI's future impact on quality of life in Kosovo, with over 80% expecting improvements to some degree. This optimism is tempered by a small but notable group who are either skeptical about AI's impact or even anticipate negative consequences. These findings suggest a generally favorable perception of AI's potential, although the presence of skepticism indicates that public trust and regulatory measures will play a key role in shaping how AI is received and implemented in the future.

## 4.3. Stakeholder Preparedness Gaps

Stakeholder preparedness refers to the readiness of key actors—such as public institutions, private sector companies, civil society, and the general public—to understand, regulate, and effectively engage with AI technologies. In the context of AI, preparedness involves having the necessary legal frameworks, ethical guidelines, technical capacity, and public awareness to ensure AI's responsible and beneficial implementation.

This section assesses the gaps in preparedness among various stakeholders in Kosovo, based on survey results and the current AI landscape in the country. The findings reveal significant gaps in both legal infrastructure and institutional capacities, while also identifying areas where improvements can be made. We will explore these gaps in public sector regulation, private sector integration, and public awareness.

### Stakeholder Gaps

Public institutions in Kosovo are not yet adequately prepared to handle the ethical, legal, and regulatory challenges posed by AI. Despite growing awareness of AI's importance and potential, there is a significant lack of concrete action in terms of developing AI-specific policies or a comprehensive national strategy. While the government has expressed intentions to develop an AI strategy[87], as of now, no formal plans are in place, nor is there any clear timeline for such a strategy to be implemented before 2025. As a result, the development of AI-specific legislation or the establishment of a dedicated AI agency appears to be on a distant horizon.

Discussions and interviews with public officials reveal a fundamental lack of understanding regarding how AI functions, its technical complexities, and its full potential. Although 64.5% of survey respondents indicated they were unaware of any laws regulating AI in Kosovo, it's not just the absence of legislation that is concerning. The challenge extends to the institutional capacity within public bodies to comprehend and effectively manage AI-related issues. For instance, public officials, while having heard of AI, primarily associate it with generative AI tools like ChatGPT, which are widely discussed in media and tech circles. However, their understanding of more advanced and diverse applications of AI—such as predictive analytics, automated decision-making, and biometric recognition—is limited.

This lack of depth in understanding poses significant risks, especially in sectors like the judiciary and prosecution. As AI begins to play a larger role in legal and investigative processes, institutions like the judiciary and prosecutor's office will struggle to handle cases involving AI-related issues. Complex cases involving algorithmic decision-making, AI-driven surveillance, or even discrimination arising from biased AI models are beyond the current expertise of many legal professionals. Based on interviews with officials, it is evident that there is no structured training or preparedness within these institutions to address the growing intersection of AI and the law.

[87] *Ministry of Economy, Republic of Kosovo, Digital Agenda of Kosovo 2030, p.24. Available at: Digital Agenda of Kosovo 2030*

Moreover, while 83.8% expressed that the government should regulate AI to protect individual rights, public institutions themselves are ill-equipped to meet this demand. Beyond the absence of a legal framework, the administrative structure to enforce such regulations, once they exist, is also lacking. Without significant capacity-building efforts, it is unlikely that public institutions will be able to create or enforce policies that adequately address the ethical concerns surrounding AI technologies.

The private sector in Kosovo is beginning to integrate AI into business models, particularly in larger companies such as telecoms and tech startups. However, the overall level of preparedness remains limited. AI tools currently in use are focused on basic functions like data processing and process automation, with more advanced uses, such as AI-driven analytics and natural language processing, being adopted slowly, mainly by larger enterprises. Despite this progress, very few companies have established ethical frameworks for AI use. The absence of comprehensive policies surrounding privacy protection, discrimination, and AI transparency could expose businesses to legal and ethical risks as AI usage grows.

Additionally, the private sector seems unprepared for future AI regulations. Many companies lack the internal expertise required to comply with potential AI laws, especially around data protection and accountability for AI-driven decisions. This gap could leave businesses vulnerable to regulatory challenges as Kosovo aligns itself with the AI standards set by the EU. Moreover, most small and medium-sized enterprises (SMEs) do not have the financial resources to invest in AI technologies or capacity-building programs for their employees. Without government incentives or funding programs to support AI adoption, many businesses could fall behind in the global AI race.

Civil society organizations (CSOs) in Kosovo are becoming more aware of AI's ethical implications, particularly concerning human rights. However, their capacity to engage with AI governance and advocacy remains underdeveloped. Even among the few CSOs that do discuss AI, very few focus on its impact on society or human rights. International organizations and donors are increasingly focusing on e-governance and digitization in Kosovo, and this will likely extend to AI in the near future, but for now, these efforts are still at a relatively low level. Furthermore, civil society organizations lack the technical expertise required to monitor AI systems or contribute to policy discussions meaningfully. Most organizations are still focused on traditional human rights issues, and while there is a growing interest in digital rights, few are equipped to address AI-specific challenges. Despite these limitations, civil society holds significant potential to raise awareness about AI risks, such as discrimination, privacy violations, and bias. CSOs could play a crucial role in public education campaigns and advocate for more ethical AI practices across public and private sectors.

Kosovo's academic institutions are still in the early stages of integrating AI into their curriculum. Few universities offer AI-related programs, and there is little research being conducted on the societal impacts of AI. This represents a significant gap in developing local expertise and thought leadership on AI. Academia has the potential to drive the development of AI expertise in Kosovo by expanding its educational offerings, fostering research collaborations, and providing training for both public and private sectors on the responsible use of AI technologies.

The general public in Kosovo demonstrates high awareness of AI, but their understanding of the technology and its broader implications remains limited. As indicated by the survey, most people are familiar with AI, but their knowledge is often confined to generative AI tools like ChatGPT. There is less awareness of AI's broader applications in fields such as employment, healthcare, or public services. Many respondents believe they are well-informed about AI, but this may be an overestimation. The gap between perceived knowledge and actual understanding could lead to misinformed public debates about AI and its role in society.

## 4.4. Benchmarks for AI Regulation

As previously discussed, Kosovo is at a nascent stage in its AI development, with limited regulatory frameworks and institutional capacities. In contrast, other countries have made significant strides in establishing comprehensive AI governance models. For instance, the European Union (EU) has developed a robust approach to AI regulation, emphasizing risk-based frameworks, ethical considerations, stakeholder inclusivity, and ethical oversight. [88]

Countries like Germany and the Netherlands have been recognized for their advancements in AI. The Netherlands, for example, has been identified as a rising star in the Global AI Index, ranking ahead of Germany, France, and Australia.[89] This progress reflects strong investments in AI research and multi-stakeholder collaboration. Similarly, Germany has consistently ranked among the top countries in AI innovation, focusing on ethical AI adoption and integrating AI into various industries.[90] These nations exemplify more advanced AI strategies and regulation, from which Kosovo's government could study to inform its own AI governance framework.

While Chapter II has already analyzed the EU's legal framework, this section will focus on the EU's institutional and supervisory structures.

### The EU's AI Governance Approach

The EU has established a sophisticated oversight and implementation framework under the AI Act to operationalize its regulatory mechanisms for AI. The AI Act introduces several new bodies specifically tasked with ensuring compliance, monitoring, and coordination across member states. These include the AI Board[91] and the AI Office[92], both created to strengthen the governance structure for AI in the EU. Together, these institutions form the core of the EU's regulatory oversight framework, working to ensure that AI development aligns with the Act's principles of

[88] European Commission, "Artificial Intelligence Board: Coordinating EU AI Policy," accessed November 17, 2024, https://digital-strategy.ec.europa.eu/en/policies/ai-board.

[89] Data Science District, "In the Global AI Index, the Netherlands appears as a rising star, ranking ahead of Germany, France, and Australia," Link: https://datasciencedistrict.nl/in-the-global-ai-index-the-netherlands-appears-as-a-rising-star-ranking-ahead-of-germany-france-and-australia/.

[90] Tortoise Media, "The Global Artificial Intelligence Index 2024," Link: https://www.tortoisemedia.com/2024/09/19/the-global-artificial-intelligence-index-2024/.

[91] For more information, please visit: https://digital-strategy.ec.europa.eu/en/policies/ai-board

[92] For more information, please visit: https://digital-strategy.ec.europa.eu/en/policies/ai-office

safety, transparency, and ethical responsibility, however it's important to note that these are not the sole actors responsible for ensuring effective oversight.

In addition to these central bodies, the framework relies heavily on national supervisory authorities, which implement and enforce AI regulations at the member state level. These authorities play a critical role in conducting audits, assessing compliance, and addressing non-compliance.[93] Moreover, the governance structure is complemented by the involvement of existing institutions and sector-specific regulators. For example, the European Data Protection Board (EDPB) addresses data privacy concerns linked to AI systems, ensuring compliance with the GDPR, namely data protection.[94] This integrated approach allows the EU to address the multidisciplinary challenges posed by AI technologies.

The EU's governance framework also emphasizes the importance of multi-stakeholder collaboration, engaging actors from academia, industry, civil society, and international organizations to provide input on AI policy and implementation. [95] These stakeholders contribute to ensuring that AI systems align with ethical principles and societal values while addressing emerging risks effectively, as exemplified by the AI Office's consultation on trustworthy general-purpose AI models, which invites input from academia, industry, civil society, and public authorities to inform the development of the first General-Purpose AI Code of Practice.[96]

The AI Board, the AI Office and the national supervisory authorities operationalize the EU's regulatory principles, transforming high-level oversight into actionable governance. By examining their mandates and functions in detail, we can better understand how the EU's sophisticated governance model is implemented in practice. The AI Board is a key institution established under Article 65 of the AI Act. Its primary role is to oversee the consistent application of AI regulations across the European Union. The AI Board is composed of representatives from each EU Member State's national supervisory authority, a representative from the European Commission, and other relevant stakeholders, ensuring broad and coordinated governance.[97][98]

Article 66 of the AI Act further details the Board's extensive responsibilities, which include providing guidance, facilitating cooperation, and supporting the development of regulatory practices. Among its key tasks are:

[93] European Union, "Artificial Intelligence Act," Article 70: National Supervisory Authorities. Link: https://artificialintelligenceact.eu/article/70/.

[94] European Data Protection Board, "About the EDPB. Link: https://edpb.europa.eu.

[95] European Union, "Introduction to Codes of Practice." Link: https://artificialintelligenceact.eu/introduction-to-codes-of-practice/.

[96] European Commission, "AI Act: Have Your Say on Trustworthy General-Purpose AI". Link: https://digital-strategy.ec.europa.eu/en/consultations/ai-act-have-your-say-trustworthy-general-purpose-ai.

[97] European Union, "Artificial Intelligence Act," Article 65: European Artificial Intelligence Board. Link: https://artificialintelligenceact.eu/article/65/.

[98] European Commission, "European Artificial Intelligence Board. Link: https://digital-strategy.ec.europa.eu/en/policies/ai-board.

- Facilitating cooperation between national supervisory authorities and promoting consistent administrative practices across member states, including those related to regulatory sandboxes and real-world testing of AI systems.
- Advising the European Commission and member states on the implementation of the AI Act, including updates to the regulatory framework, development of codes of conduct, and evaluation of emerging technological trends.
- Collecting and sharing technical and regulatory expertise, developing benchmarks, and contributing to public awareness and AI literacy.
- Collaborating with other EU bodies, agencies, and international organizations to align efforts on product safety, cybersecurity, consumer protection, and fundamental rights.
- Assisting national authorities in developing the technical and organizational expertise needed to implement the AI Act and contributing to the assessment of training needs.[99]

The AI Office, established within the European Commission, is a cornerstone of the EU's governance framework for AI. It plays a critical role in implementing the AI Act and advancing the EU's commitment to trustworthy AI. [100]As an operational body, the AI Office supports the work of the AI Board, facilitates cooperation among national authorities, and ensures the consistent application of AI regulations across the EU.

The AI Office is structured to act as the secretariat of the AI Board, handling technical and administrative responsibilities. It supports the development of standards and guidelines, aids Member States in harmonizing enforcement practices, and provides expertise on emerging issues in AI regulation. This coordination helps maintain a consistent approach across the EU, ensuring that national authorities implement the AI Act in a manner aligned with the Union's broader objectives.[101][102]

One of the AI Office's key initiatives is the AI Pact, a voluntary agreement that encourages stakeholders to commit to principles of trustworthy AI even before the full implementation of the AI Act. This initiative demonstrates the proactive nature of the AI Office, emphasizing collaboration with private companies, civil society, and academic institutions to foster ethical AI innovation and deployment.

The AI Office also plays a vital role in public engagement and capacity building. It provides training resources for national authorities, raises awareness about the risks and opportunities of

[99] European Union, "Artificial Intelligence Act," Article 66: European Artificial Intelligence Board. Link: https://artificialintelligenceact.eu/article/66/

[100] European Commission, "European Artificial Intelligence Office," Link: https://digital-strategy.ec.europa.eu/en/policies/ai-office

[101] European Union, "Artificial Intelligence Act," Articles 56 and 64. Links:
https://artificialintelligenceact.eu/article/56/
https://artificialintelligenceact.eu/article/64/

[102] European Commission, "European Artificial Intelligence Office," Link: https://digital-strategy.ec.europa.eu/en/policies/ai-office

AI, and promotes human-centric AI development. Its efforts aim to build public trust in AI technologies while ensuring that they are developed and deployed in line with EU values.

Collaboration is a central aspect of the AI Office's operations. It works closely with the AI Board, offering operational support to ensure the Board's smooth functioning. It also liaises with national supervisory authorities, assisting them in addressing enforcement challenges and aligning practices across Member States. Additionally, the AI Office engages with other EU bodies, such as the EDPB, on data privacy issues and collaborates with other sectoral regulators.

Through its work, the AI Office bridges gaps between technical, administrative, and regulatory aspects of AI governance. It also strengthens the EU's position in global AI discussions by fostering international cooperation and aligning with global standards. By integrating these various responsibilities, the AI Office ensures that AI technologies in the EU are developed and deployed safely, ethically, and in a way that reflects European values.

The implementation and enforcement of AI regulations at the national level are carried out by national supervisory authorities, as mandated under Article 70 of the AI Act. These authorities are designated by each member state to oversee the application of the regulation, reflecting the EU's commitment to a decentralized but harmonized governance model.

Responsibilities of national supervisory authorities include:

- Conducting audits and investigations into non-compliance with AI regulations.
- Addressing violations of the AI Act through fines or operational restrictions on AI systems.
- Working with the AI Board to ensure consistent enforcement, particularly for AI systems deployed across multiple member states[103].

The EU's governance framework for AI also includes other key bodies that provide specialized insights and guidance, such as the Advisory Forum and the Scientific Panel of Independent Experts.

The Advisory Forum brings together representatives from national supervisory authorities, relevant EU institutions, and stakeholders to facilitate dialogue and share expertise on the implementation and application of the AI Act. This forum plays a critical role in fostering cooperation and ensuring the continuous improvement of AI governance across the Union.[104] The Scientific Panel is composed of independent experts with technical, ethical, and regulatory expertise in AI. It advises the AI Board and the European Commission on scientific developments, emerging risks, and technological trends to ensure that EU policies remain aligned with the latest advancements and challenges in AI.[105]

[103] European Union, "Artificial Intelligence Act," Article 70: National Supervisory Authorities. Link: https://artificialintelligenceact.eu/article/70/.

[104] European Union, "Artificial Intelligence Act," Article 67: Advisory Forum: Link: https://artificialintelligenceact.eu/article/67/.

[105] European Union, "Artificial Intelligence Act," Article 68: Scientific Panel of Independent Experts. Link: https://artificialintelligenceact.eu/article/68/

### Proposed Solutions for Kosovo

As discussed earlier, Kosovo is still at the early stages of AI development, with limited institutional capacity and no framework specifically designed to address the challenges and opportunities of artificial intelligence. This gap is particularly concerning as Kosovo moves through a digitization process. While these advancements hold great promise, the absence of regulation leaves Kosovo vulnerable to risks such as unfair practices, breaches of privacy, and even potential human rights violations if AI systems are misused or poorly implemented in sensitive areas like healthcare, education, or the justice system.

Ensuring that AI systems are developed and used responsibly is not just a question of technological progress—it is also about safeguarding the rights and dignity of individuals. Chapter II highlighted that Kosovo's existing laws do not specifically address AI. There is no dedicated AI law, no policy document, and no strategy that outlines how AI should be governed or how its risks should be managed. This lack of clarity creates a legal vacuum, leaving businesses, public institutions, and citizens without guidance on how to navigate the complexities of AI technologies.

The creation of a comprehensive AI law in Kosovo is critical to ensuring that artificial intelligence is developed and used in ways that protect human rights, foster innovation, and promote public trust. Without clear legal frameworks, the deployment of AI technologies could result in harmful consequences, such as biased decision-making, violations of privacy, or the misuse of AI in ways that undermine equality and justice. An AI law would serve as a foundation for addressing these risks, providing rules and safeguards that hold developers, deployers, and users of AI accountable for their systems' impacts on individuals and society.

Without adequate legal protections, there is a significant risk that vulnerable groups could be disproportionately affected by poorly regulated AI systems. The law would also signal Kosovo's commitment to aligning with international best practices, such as those seen in the EU's AI Act, while adapting these frameworks to local needs. As Kosovo aspires to deepen its partnership with the EU, creating a legal framework that mirrors European standards would also prepare its institutions for integration into broader regional governance structures.

In addition to the legal framework, the Digital Agenda of Kosovo 20230 already emphasizes the importance of creating an AI strategy. The strategy would serve as a roadmap for implementing the law, prioritizing areas such as public awareness, capacity building, and multi-stakeholder collaboration. By integrating governance into the broader digitization agenda, Kosovo can ensure that AI adoption supports societal well-being while fostering economic growth.

Governance should be a central feature of the law. A multi-stakeholder approach, involving government institutions, private sector actors, academia, and civil society, would promote inclusivity and ensure that diverse perspectives inform the regulation of AI. The law should also establish clear roles for oversight bodies, with responsibilities for monitoring compliance, assessing risks, and enforcing standards. Public engagement and consultation must remain key elements, as they are essential to building trust and ensuring that the law reflects societal values.

It is evident that drafting a comprehensive AI strategy, passing an AI law, and creating the necessary governance bodies are all essential steps for ensuring the ethical and human-centered development of artificial intelligence in Kosovo. However, the process of achieving these milestones is both complex and time-consuming. In practice, it often takes 2–3 years to draft, consult, and pass a new law, followed by another 1–2 years to establish and fully operationalize the institutions required to implement and enforce it. Given the rapid pace of AI development globally, this timeline poses significant challenges for Kosovo. Without any interim measures, the country risks falling behind or, worse, allowing unregulated AI systems to proliferate, potentially causing harm to individuals and undermining trust in public institutions.

To address this gap, it would be prudent for Kosovo's institutions to establish a temporary AI oversight body. This body would not necessarily require formal regulatory or enforcement powers but could act in an advisory capacity to ensure that AI technologies are developed and deployed in a way that aligns with ethical principles and human rights. Such a body could provide guidance to public institutions, particularly in the context of Kosovo's ongoing digitization efforts.

This advisory body could be composed of representatives from key existing institutions, such as the IPA and the Ombudsperson Institution. The IPA is particularly relevant given its role in overseeing data protection, a critical aspect of AI governance. Similarly, the Ombudsperson Institution brings expertise in safeguarding human rights, which is essential for ensuring that AI systems do not perpetuate discrimination, bias, or other rights violations. Together, these institutions could provide a multidisciplinary perspective on the ethical and societal implications of AI, offering public institutions the guidance needed to navigate this complex and rapidly evolving field.

The temporary oversight body could also include representatives from academia, civil society organizations, and the private sector to ensure a diverse range of perspectives. Its functions might include advising on the procurement and deployment of AI systems, conducting assessments of high-risk applications, and recommending best practices for ensuring transparency and accountability.

This interim solution would allow Kosovo to address immediate challenges while the longer-term frameworks, such as the AI law and governance bodies, are developed and operationalized. By prioritizing ethical and human-centered AI during this transitional period, Kosovo can lay the groundwork for a more comprehensive governance framework while minimizing the risks associated with unregulated AI. Moreover, establishing such a body would demonstrate a commitment to proactive governance, ensuring that the country remains aligned with global trends and ready to embrace AI in a way that benefits all citizens.

# Chapter V: Recommendations

Based on the research findings, it is clear that Kosovo must take significant steps to address the challenges posed by the increasing integration of AI into society. To ensure that AI is deployed in a manner that upholds human rights, several key actions are recommended across various sectors.

Developing an AI governance framework should be a priority for Kosovo. This framework should include the drafting of AI-specific legislation that addresses privacy, freedom of expression, non-discrimination, and access to information. The AI framework should be aligned with emerging European regulations, particularly the EU's AI Act and DSA. Kosovo should develop a comprehensive AI strategy that outlines clear responsibilities for regulatory oversight, including ensuring transparency, ethical use of AI technologies, and protection of fundamental rights. AI-driven applications, especially in sectors like healthcare and law enforcement, should undergo regular audits to ensure they comply with these new regulations.

The capacity of public institutions must be significantly improved to effectively manage and regulate AI technologies. Government officials, members of the judiciary, and law enforcement agencies should undergo specialized training programs on AI-related issues, particularly concerning data protection, privacy rights, and algorithmic bias. Public institutions also need to strengthen their digital infrastructure and cybersecurity frameworks to ensure they can handle the growing presence of AI technologies responsibly. More specifically, public bodies should be required to carry out AI impact assessments before implementing AI-based systems. This would help prevent potential misuse of AI.

In the private sector, companies must adopt clear ethical guidelines for the use of AI technologies. Larger companies, particularly in sectors such as telecommunications and finance, should be encouraged to implement AI with a focus on transparency and accountability. These guidelines should address potential risks such as biased algorithms, discriminatory outcomes, and the improper handling of personal data. Smaller businesses, meanwhile, will need support—both financial and technical—to integrate AI technologies responsibly. The government could consider offering tax incentives or grants to SMEs that adhere to human rights standards in their use of AI.

Academia needs to take a more active role in AI development in Kosovo. Universities should expand their course offerings to include AI ethics, law, and governance alongside technical AI training. Research on the societal impacts of AI needs to be supported through increased funding, particularly in areas related to human rights, privacy, and equality. Partnerships between academia and the private sector should be encouraged, with the aim of fostering responsible AI innovation that aligns with societal needs.

Civil society and the general public also play a vital role in the ethical use of AI. Non-governmental organizations need to be more involved in policy discussions and AI governance efforts, particularly by monitoring AI use and holding public institutions and businesses accountable. International organizations and donors, such as the UNDP and EU agencies, should continue to provide support for capacity-building initiatives in this area. Public awareness campaigns are also essential to help citizens understand the risks and benefits of AI technologies, particularly in relation to data privacy and algorithmic bias. Civil society groups can lead efforts to educate the public and advocate for their rights in the digital age.

Kosovo should actively engage with international partners to align its AI regulations with global standards. In particular, collaboration with the EU is crucial to ensure that Kosovo's AI governance keeps pace with evolving EU regulations like the AI Act and DSA. Partnerships with neighboring countries can also help Kosovo learn from their experiences and share best practices in AI regulation. International donors can play a key role by providing funding for research, capacity-building, and infrastructure development related to AI.

Finally, Kosovo must look beyond immediate needs and develop a long-term AI strategy. This strategy should focus on ensuring that AI technologies contribute to sustainable development and economic growth, while also safeguarding human rights. Public institutions and businesses should be encouraged to adopt AI technologies that promote fairness and inclusivity, ensuring that the benefits of AI are shared broadly across society. Continuous monitoring and evaluation of AI's impact on society will be critical to ensure that new challenges are identified and addressed in a timely manner.

Kosovo should also adopt a cross-sectorial, collective, and participatory approach to developing and implementing AI governance. The involvement of multiple stakeholders—across government institutions, the private sector, civil society, academia, and international organizations—will ensure that AI policies are more representative, inclusive, and responsive to the needs of all citizens. This process should be transparent, with open discussions and consultations that allow for public input and accountability.

Given the time required to pass AI legislation and establish governance bodies, Kosovo should create a temporary AI oversight body as an interim solution. This advisory body would guide public institutions on ethical AI use, particularly during the digitization process, and help address immediate challenges. Comprising representatives from existing institutions like the Information and Privacy Agency (IPA) and the Ombudsperson Institution, it would ensure AI aligns with human rights and ethical standards while laying the groundwork for long-term governance.

In addition, Kosovo's AI strategy should be grounded in digital rights and principles, aligning with the EU's Digital Agenda. This includes placing people at the center of AI development, ensuring freedom of choice for users, promoting safety and security in AI applications, fostering solidarity and inclusion to prevent discrimination, encouraging public participation in AI-related decision-making, and ensuring sustainability in AI deployment. These principles should guide all AI policies and regulations, ensuring that human rights are safeguarded in the digital age.

In summary, the recommendations focus on building a strong AI governance framework, enhancing the capacity of public institutions, encouraging ethical AI use in the private sector, supporting AI research in academia, and engaging civil society and the public in meaningful ways. By taking these steps, Kosovo can ensure that AI technologies are developed and implemented in a way that protects human rights and promotes responsible innovation.

# Chapter VI: Conclusion

As AI technologies continue to expand globally, their influence on human rights is becoming increasingly significant. This study has sought to explore the unique challenges Kosovo faces in this context, given its developing digital infrastructure and limited regulatory framework for AI. While AI holds great promise for economic and societal development, it also presents considerable risks, particularly in relation to fundamental rights such as privacy, freedom of expression, and non-discrimination.

Kosovo, like many other countries, is at a pivotal moment in its digital transformation. AI technologies are beginning to penetrate key sectors, yet the country lacks the legislative and institutional capacity to manage the ethical, legal, and societal implications of these technologies. The absence of AI-specific governance mechanisms leaves Kosovo vulnerable to potential abuses, including unchecked surveillance, algorithmic bias, and the erosion of civil liberties.

To better understand these challenges, this paper examined four key research questions, providing insights into the current state of AI in Kosovo and highlighting areas that require urgent attention. The research findings shed light on the gaps in AI regulation, stakeholder preparedness, and the broader AI ecosystem in the country.

**1. How does AI impact human rights in Kosovo, particularly in terms of privacy, freedom of expression, and non-discrimination?**

AI technologies present significant risks to human rights in Kosovo, especially in areas such as privacy and surveillance. Without proper safeguards, AI-driven data collection systems could infringe upon individuals' privacy by enabling mass surveillance or unauthorized data use. Similarly, AI's growing role in content moderation has the potential to restrict freedom of expression, particularly in a politically sensitive environment like Kosovo, where political discourse is often contentious. AI systems could also exacerbate existing inequalities or introduce new forms of discrimination, particularly in sectors such as employment and healthcare, where biased algorithms could disproportionately affect vulnerable populations.

**2. What measures and policies are currently in place in Kosovo to protect human rights in the context of AI?**

Currently, Kosovo has no specific AI-related laws or comprehensive regulatory frameworks that address the human rights implications of AI. While Law No. 06/L-082 on Protection of Personal Data provides some protection in the area of data privacy, it does not fully address the broader ethical concerns associated with AI technologies. Although freedom of expression and equality in relation to AI are not directly regulated, there are existing laws that establish some general ground rules. Other laws, such as those related to equality and non-discrimination, lay down basic protections that may become increasingly relevant as AI systems are deployed in sectors like employment and public services.

There is a pressing need for AI-specific legislation that aligns with emerging international standards, such as the EU's AI Act and the DSA.

**3. What is the current AI landscape in Kosovo, including key technologies, players, and sectors utilizing AI?**

The AI landscape in Kosovo is still in its infancy. While AI technologies are being adopted by some larger companies and public sector institutions, the level of AI integration remains limited. Key sectors, such as telecommunications, finance, and public administration, are starting to explore AI-driven solutions, but the majority of stakeholders lack the technical expertise and resources needed to fully engage with AI. Key players include government bodies, private companies, civil society organizations, and international donors. However, coordination between these groups is limited, and the AI ecosystem remains underdeveloped compared to neighboring countries and global standards.

**4. How informed and prepared are various stakeholders in Kosovo (government, private sector, civil society) regarding the ethical implications of AI?**

The findings indicate that while many stakeholders are aware of AI technologies, there is a significant lack of preparedness when it comes to managing their ethical and human rights implications. Government institutions, in particular, are not adequately equipped to regulate or monitor AI applications, leaving gaps in oversight that could lead to potential abuses. The private sector is beginning to adopt AI technologies, but ethical guidelines are largely absent, raising concerns about transparency, accountability, and bias. Civil society organizations, though increasingly engaged in AI-related discussions, lack the technical capacity to fully participate in governance efforts. There is a clear need for cross-sectoral collaboration and capacity-building to improve AI governance across all stakeholders.

Kosovo faces both challenges and opportunities as it navigates the growing influence of AI. While the country’s AI landscape is still developing, the risks associated with AI technologies, particularly in relation to human rights, are substantial. The recommendations provided in this paper aim to address these challenges by calling for the development of an AI governance framework, improved institutional capacity, and greater public awareness.

By adopting AI-specific legislation, fostering collaboration between public and private sectors, and aligning with international standards, Kosovo can ensure that the benefits of AI are realized in a manner that respects and protects human rights. The process of developing an ethical AI framework should be transparent, inclusive, and grounded in the principles of the EU Digital Agenda—emphasizing the central role of people, freedom of choice, safety, inclusion, participation, and sustainability.

Looking forward, Kosovo’s ability to manage AI technologies will depend on its commitment to a rights-centered, participatory, and cross-sectoral approach. By addressing the regulatory gaps identified in this research and ensuring that stakeholders are prepared to manage AI’s ethical implications, Kosovo can position itself as a leader in responsible AI governance within the region. Ultimately, the protection of human rights in the age of AI will require not only strong legal frameworks but also continuous engagement and vigilance across all sectors of society.

ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY