## AI security in the EU under the framework of the EU AI Act:

---

# 1. Introduction

- **Overview of AI in the EU**: Summarising what is the EU's goals for AI, advantages (economic growth, new technologies) and disadvantages (security threats, ethical issues)
- **Importance of AI Security**: Emphasising why a strong regulatory approach to AI security is critical for the EU, particularly in sectors where AI poses high security risks.
- **EU AI Act as a Milestone**: Introducing the EU AI Act, positioning it as a regulatory framework that addresses AI risks with a focus on security, ethics, and human rights.

# 2. Research Problem

- **Security Concerns in AI Development and Deployment**: Listing the principal risks associated with AI and which include data security issues, algorithmic control, cyber security and misuse of artificial intelligence systems.
- **Limitations of Current Security Measures**: mentioning some of the weaknesses of the EU AI Act, such as the enforcement, the considerations of the latest AI technologies, and cross-sectoral cohesiveness.

# 3. Literature Review and Background

- **AI Security Risks**: Summarising studies on AI-specific security risks in high-stakes fields like healthcare, finance, law enforcement, and autonomous vehicles.
- **Overview of the EU AI Act**: Providing a concise explanation of the Act's provisions, including its classification of AI applications based on risk and its requirements for high-risk AI systems in areas like transparency, data quality, risk management, and cybersecurity.

- **Comparative Regulatory Approaches**: Comparing the EU's approach to that of other regions like the U.S. and China, highlighting the EU's unique focus on security and ethics.

## 4. Research Objectives

- **Objective 1**: Evaluating the effectiveness of the AI Act's security measures and risk categorization, particularly in high-risk applications.
- **Objective 2**: Identifying potential gaps in the Act's approach to security, especially for AI applications that may be at risk for rapid technological advances.
- **Objective 3**: Exploring opportunities to enhance the EU's AI security framework, suggesting policy adaptations that account for emerging security threats.

## 5. Methodology

- **Policy Analysis**: Conducting a detailed examination of the AI Act, specifically its provisions on AI security, transparency, and risk management.
- **Case Studies**: Analysing real-life AI security incidents in the EU (e.g., cyberattacks on AI systems or ethical controversies) to assess how the Act's regulations might address or fall short in preventing these issues.
- **Expert opinions**: Interview AI policy experts and cybersecurity professionals to gain insights into the practical challenges and potential solutions for implementing the Act's security measures.
- **Comparative Framework**: Compare the EU AI Act's security policies with international standards, identifying unique strengths and areas where the EU can learn from other regions.

## 6. Expected Contributions

- **Recommendations for Policy Enhancements**: In light of the presented research, provide recommendations for the changes in the current state of the AI Act, for instance, including modes for updating the AI Act or secondary legislative acts and policies that will reflect the high-risk AI applications.
- **Implications for EU Policymakers and Businesses**: Explaining in this research how policymakers and companies in the EU can improve AI security, and why this is essential for the EU's confidence in AI.

## 7. Conclusion

- **Summary of Importance**: Reinforcing the significance of a strong AI security framework within the EU, particularly given the Act's global influence.
- **Long-Term Vision**: Stating the potential for the EU to lead in global AI security policy and to set a standard for responsible AI governance.

---