Source: istockphoto.com

INFORMATION, COMMUNICATION & COMPUTING

Fields of Expertise TU Graz

Kay Uwe Römer
Source: Lunghammer – TU Graz

At first glance, the European AI Act which has been in force since February 2025 has little impact on research on AI models and systems at universities as the AI Act expressly does not apply to AI systems or models developed solely for the purpose of scientific research and development, as long as they are not placed on the market or put into service.

However, applied research on AI in collaboration with industry with the purpose of developing AI models and systems or prototypes thereof that will later be used by the industry partner obviously affects university researchers, who have to ensure that the research results meet AI Act regulations when further developed and put into service by the company partner. Already, low-risk AI systems have to meet requirements on transparency (users must be clearly informed about the use of AI), security (AI applications must not pose any risks to individuals or data), and data protection (GDPR also applies to AI applications if they are trained or used with personal data). For high-risk AI applications the demands are even higher: risk management (to identify and minimize potential risks at an early stage), data quality and fairness (to ensure that training and test data are of high quality and do not promote bias or discrimination), human supervision (critical decisions must not be made entirely automatically, i.e., humans can intervene in the decision-making process), robustness and security (AI systems must be protected against external attacks and manipulation, and regular security checks are required), and documentation (detailed records of how AI systems work and make decisions must be kept in order to demonstrate transparency in the event of regulatory audits). Given these complex requirements it seems mandatory that university researchers – from PhD students and postdocs to professors – are systematically trained in the AI Act regulations. This applies not just to computer science or information technology, but increasingly also to other engineering disciplines using AI techniques. However, currently there seems to be a lack of such training and also of qualified trainers at the university.

In this edition of TU Graz research, Lorenzo Cicardo, gives us some insights on his research. Enjoy reading!

**Information,
Communication
& Computing**