The Need of AI Governance

By Patrick Jungo

AI Governance: Risk Transfer to Users of Machine Translation

Systems AI translation systems, like other AI systems, are subject to disclosure requirements according to Article 52 of the EU AI Act. For high-risk areas such as law, finance, or medicine, stricter regulations apply. Operators of high-risk AI systems are required to disclose their training data. This could lead to violations of the GDPR when processing sensitive data, for example, in a translation agency. This disclosure requirement conflicts with the data protection requirements of the GDPR and may render data protection measures obsolete.

Risk Transfer to Users of LLMs

Today's high-quality AI translation systems are all based on LLMs (Large Language Models). Other models are increasingly becoming less competitive. LLM operators are engaging in strong lobbying efforts to relieve themselves from liability and shift the risks that may arise from the use of LLMs (e.g., data protection violations, copyright infringements) onto users. As the points discussed below show, the legal possibility of transferring risk to users of LLMs by lawmakers is a real concern. Consequently, the professional use of LLMs should be analyzed through AI governance, and appropriate measures to mitigate risk should be considered today.

Responsibility and Ultimately the Risk Lie with the Users of LLMs

The risks arising from the improper use of their models lie with the users. Since the operators do not have full control over how the models are used, it is the users' responsibility to ensure legal compliance and secure usage.

Sensitive Data and Risks

Translations of sensitive data carry a high risk, as errors could have serious consequences. LLM operators do not want to be liable for such errors and therefore shift the responsibility onto the users. They require users to comply with data protection laws themselves, as the users have specific knowledge of the processed data and the legal frameworks involved.