KI-Governance: Risikoübertragung an die Nutzer von maschinellen Übersetzungssystemen

Patrick Jungo, 1. September 2024

KI-Übersetzungssysteme unterliegen wie andere KI-Systeme gemäß Art. 52 des EU AI Acts der Offenlegungspflicht. Für risikoreiche Bereiche wie Recht, Finanzen oder Medizin gelten dabei strengere Vorgaben. Betreiber von Hochrisiko-KI-Systemen müssen die Trainingsdaten offenlegen. Dies könnte bei der Verarbeitung sensibler Daten, z. B. in einer Übersetzungsagentur, zu Verstößen gegen die DSGVO führen. Diese Offenlegungspflicht widerspricht den Datenschutzanforderungen der DSGVO und kann Datenschutzmaßnahmen obsolet machen.

Risikoübertragung auf die Nutzer von LLMs

KI-Übersetzungssysteme mit hoher Qualität basieren heute alle auf LLMs (Large Language Models). Andere Modelle werden zunehmend nicht mehr konkurrenzfähig sein. Die Betreiber von LLMs betreiben starkes Lobbying mit dem Ziel, sich von der Haftpflicht zu lösen und das Risiko, das durch die Nutzung von LLMs entstehen kann (Verletzung des Datenschutzes, Verletzung des Urheberrechts) auf die Anwender zu übertragen.

Wie die unten erläuterten Punkte aufzeigen, ist die Möglichkeit einer rechtlichen Übertragung des Risikos auf die Nutzer von LLMs durch den Gesetzgeber reell. Infolgedessen sollte das Risiko der beruflichen Nutzung von LLMs mit Hilfe von KI-Governance analysiert und entsprechende Maßnahmen zur Verringerung des Risikos bereits heute in Betracht gezogen werden.

Verantwortung und letztlich das Risiko liegt bei den Nutzern von LLMs

Durch den unsachgemäßen Einsatz der Modelle können Schäden verursacht werden. Da die Betreiber keine vollständige Kontrolle über die Verwendung der Modelle haben, liegt es in der Verantwortung der Nutzer, eine rechtskonforme und sichere Nutzung sicherzustellen.

Sensible Daten und Risiken

Übersetzungen sensibler Daten bergen ein hohes Risiko, da Fehler schwerwiegende Konsequenzen haben könnten. Die Betreiber von LLMs wollen nicht für solche Fehler haften und schieben daher die Verantwortung auf die Nutzer. Sie verlangen, dass die Nutzer die Datenschutzgesetze selbst einhalten, da sie spezifisches Wissen über die verarbeiteten Daten und die rechtlichen Rahmenbedingungen haben.

Druck auf die Politik

Die Betreiber üben politischen Druck aus, indem sie ihre neuesten Technologien nicht in der EU zur Verfügung stellen, z. B. Meta, das die Nutzung des LLM LLaMa 3 in der EU verweigert. Ohne Zugang zu diesen Technologien erleidet der Wirtschaftsstandort einen erheblichen Nachteil.

Die Betreiber von LLMs wollen durch Lobbying erreichen, dass das Risiko auf ihre Nutzer übergeht, da sie selbst keine vollständige Kontrolle über die Modelle haben. Gleichzeitig birgt die Offenlegungspflicht nach dem EU AI Act erhebliche Risiken für die Verarbeitung sensibler Daten, was mit den Datenschutzanforderungen der DSGVO kollidiert.