Open Source AI
Open Source Prinzipien angewendet auf künstliche Intelligenz

Zahlreiche grosse und kleine Technologie-Unternehmen veröffentlichen KI-Modelle unter dem Begriff «Open Source AI». Gleichzeitig wird in der Fach-Community heftig über die Definition diskutiert. Dieser Beitrag erläutert die wesentlichen Aspekte der Thematik und zeigt praktische Anwendungen von offen zugänglichen KI-Modellen.

Es scheint so, also ob sich die Geschichte wiederholt: Vor rund 30 Jahren, als der Internet-Boom und die Software-Entwicklung so richtig Fahrt aufnahmen, stellte sich die Frage, wer nun konkret unter welchen Umständen die Möglichkeit hat, Software-Produkte zu nutzen, zu analysieren, zu verändern und weiterzuverbreiten. Im Jahr 1998 wurde dazu die Open Source Initiative (OSI) gegründet, die den Begriff «Open Source Software» mit der «Open Source Definition» prägte und seither über 100 Open Source Lizenzen verabschiedet hat (vgl. «Open Source Software», S. 52). Heute, mit dem Hype um die neusten Entwicklungen der künstlichen Intelligenz (engl. «Artificial Intelligence», kurz AI), ist erneut die Diskussion entbrannt, was Offenheit, Transparenz und Wiederverwendung für diese neuartigen Digitaltechnologie bedeuten. Wiederum hat sich die OSI in die globale Diskussion eingeschaltet. Seit 2022 koordiniert sie einen öffentlichen Prozess mit Hunderten von Technologie- und Rechtsfachleuten um eine klare Definition zu erarbeiten, wann von «Open Source AI» gesprochen werden kann und wann nicht.

Tech-Firmen und die Gefahr des «Open-Washing»

Warum ist diese Definition von «Open Source AI» überhaupt von Bedeutung? Weil sich immer wieder Unternehmen mit dem Begriff «Open» schmücken, um Aufmerksamkeit und Wohlwollen der Öffentlichkeit zu erlangen, obwohl eigentlich kaum etwas transparent und frei zugänglich ist. Bestes Beispiel ist die bekannte Firma OpenAI, die mit ChatGPT ein innovatives und erfolgreiches Produkt lanciert hat, das jedoch nichts mit der technologischen Offenheit von Open Source Software zu tun hat: Weder kann ChatGPT uneingeschränkt kostenlos genutzt werden, noch ist nachvollziehbar, wie die neuen GPT-Modelle funktionieren und mit welchen Daten sie trainiert wurden. Andere Herausforderungen stellen sich, wenn grosse Firmen wie Meta, Microsoft und Google mächtige KI-Modelle (im Gegensatz zu OpenAI) tatsächlich veröffentlichen und diese frei genutzt werden können. Damit sind solche Modelle mehr «open» als ChatGPT, denn sie ermöglichen den Betrieb auf eigenständigen Servern oder sogar auf persönlichen Laptops (siehe beispielsweise GPT4All). Dies gewährleistet den Datenschutz und erhöht die Kontrolle über die Technologie (vgl. «Digitale Souveränität», S. 46). Allerdings bieten auch solche sogenannten «Open Weights»-Modelle nicht zwingendermassen eine vollständige Transparenz, welche Daten etwa für deren Erstellung genutzt wurden. Dies ist eine wichtige Voraussetzung der «Open Source AI»-Definition der

OSI, dass neben dem KI-Modell auch der Quellcode und das Trainingsverfahren veröffentlicht werden. Allerdings heisst jedoch «Open Source AI» nicht notwendigerweise, dass auch alle zum Training verwendeten Daten zugänglich sein müssen. Oftmals kann es aus Gründen der Privatsphäre oder des Urheberrechts heikel sein, die vollständigen Rohdaten mitzuveröffentlichen.

Datenschutz, digitale Souveränität, Innovation und Kostenvorteile mit «Open Source AI»

Um den hohen Datenschutzanforderungen im öffentlichen Sektor Rechnung zu tragen und die digitale Souveränität zu gewährleisten, nutzt das Institut Public Sector Transformation der BFH «Open Source AI» für die Entwicklung von KI-Lösungen für die Verwaltung (vgl. «KI im öffentlichen Sektor», S. 56). Dabei können auf über eine Million auf Hugging Face veröffentlichte KI-Modelle zugegriffen werden, welche Texte (vgl. «Natural Language Processing», S. 58), Quellcode, Bilder, Musik, Video etc. verarbeiten und auch generieren. Von Vorteil ist ausserdem die finanziell attraktive Skalierung von eigenständig betriebenen KI-Systemen, weil diese nicht wie bei ChatGPT nach Anzahl Abrufen über die Schnittstelle verrechnet werden, sondern wie bei herkömmlichen «On-Premise» Lösungen ausschliesslich die Serverkosten anfallen (vgl. «Cloud Computing», S. 48). Gleichzeitig hat das Institut Public Sector Transformation auch Erfahrung im Anpassen von bestehenden und im Generieren von neuen KI-Modellen. So konnten beispielsweise im Auftrag des Bundesgerichts spezifische «Legal Language Models» basierend auf grossen Mengen von Rechtsdaten entwickelt werden.

Unsere Empfehlungen

1. Daten-, Technologie- und Kostentransparenz einfordern

Bei IT-Lösungen mit Einsatz von KI sollte geprüft werden, wo die Nutzungsdaten beim Betrieb hinfliessen, welche Technologien konkret eingesetzt werden und welche Kostenfolgen bei der Skalierung entstehen.

2. Aktuelle Entwicklungen von «Open Source AI» beobachten

Täglich werden neue KI-Modelle und Datensets auf Hugging Face veröffentlicht und geprüft, sodass eine laufende Beobachtung des «Open Source AI» Trends über neuste Entwicklungen informiert hält.

3. Das Potenzial von «Open Source AI» nutzen

Mittels Proof-of-Concepts (PoCs) und Pilotprojekten können öffentliche Stellen das Potenzial von «Open Source AI» testen und die Qualität von KI-generierten Ergebnissen konkret prüfen.

Mehr Informationen

Kontaktmöglichkeiten
und weitere Informationen
zu Open Source AI:
bfh.ch/ipst/public-sector-ai

Kontakt

Prof. Dr. Matthias Stürmer
Institutsleiter

matthias.stuermer@bfh.ch
T +41 31 848 41 68

Prof. Dr. Marcel Gygli
Professur KI im öffentlichen Sektor

marcel.gygli@bfh.ch
T +41 31 848 64 90