Dezentrales KI-Lernen: Gesellschaft als Reallabor?

Die Erforschung Künstlicher Intelligenz (KI) prägt bereits unseren Alltag: die Eingabehilfe einer Handytastatur, Algorithmen zur Spracherkennung und für Musikempfehlungen, Fotoauswahl und Gesichtserkennung sind Beispiele für KI-Anwendungen, die ständig weiterentwickelt und praktisch getestet werden. Künstliche Intelligenz hat wesentlich zum Erfolg großer IT-Unternehmen beigetragen, da diese in der Lage sind, große Mengen an Nutzungsdaten zu sammeln und zentral zu verarbeiten. In der bisherigen Erfahrung führte die KI-Entwicklung zu einer Winner-takes-it-all-Dynamik: umso umfangreicher die Trainingsdaten einer KI, desto treffender die Prognosen, desto effektiver die angebotene KI-Dienstleistung.[1] Prinzipiell braucht KI-Lernen große Rechenkapazitäten, weshalb schon bisher Cloud-Lösungen für KI-Lernen genutzt wurden (AWS, Microsoft, Google).[2] Diese Cloud-Lösungen bauen auf einer zentralisierten Architektur auf: Nutzungsdaten werden zentral in der Cloud gespeichert und dann zum Training von Algorithmen genutzt. Die Nachteile einer zentralen Datenspeicherung bestehen darin, dass große Datenmengen transferiert werden müssen, was Kosten verursacht; Latenzprobleme verhindern oft die erforderliche Echtzeit-Inferenz; Verschwiegenheitsanforderungen in Bereichen mit sensibler Datenverarbeitung verhindern die Cloud-Speicherung; Datenübertragung zu entlegenen Cloud-Servern bietet Einfallstore für Hacker-Angriffe (siehe Thema Cloud Computing).

Dezentrale Ansätze im Maschinenlernen versuchen diesen Nachteilen entgegenzuwirken und werden in Anbetracht der zunehmenden Vernetzung von Geräten (siehe Thema Netz der bewegten Dinge) und damit steigender, dezentraler Rechnerleistung immer attraktiver. Einer dieser Ansätze ist „Edge Computing“. Die Idee ist, dass Informationsverarbeitung am Rand des Netzwerks („Edge“), d. h. z. B. direkt am Endgerät stattfindet, um einerseits von den Vorteilen einer Cloud zu profitieren und andererseits Verzögerungen bei der Datenübertragung zu vermeiden. Einen anderen Fokus legt „Federated Learning“, eine neue Trainingsmethode für KI, die auf kooperatives Lernen anhand eines geteilten Vorhersagemodells abzielt (Peters und Krieger 2022). Anders als bisher ist dazu kein zentraler Datensatz notwendig, sondern die Verbesserungen und Lernprozesse der einzelnen, mobilen Geräte werden als Update verschlüsselt an eine Cloud geschickt. In der Cloud werden die gesammelten Updates aller NutzerInnen zusammengeführt und helfen, das zentrale Trainingsmodell zu verbessern. Das verbesserte Modell wird dann wiederrum auf die mobilen Geräte zurückgespielt und kann gleich genutzt werden. Die Vorteile dieser Verarbeitungsweise liegen im reduzierten Datenvolumen der Updates im Vergleich zur Übertragung der gesamten Nutzungsdaten und damit ge-

[1] mattturck.com/the-power-of-data-network-effects/.

[2] hackernoon.com/federated-learning-a-step-closer-towards-confidential-ai-7ac4afa9b437.

ringeren Kosten. Zudem bietet Federated Learning einen höheren Datenschutz, da alle persönlichen Daten am mobilen Gerät verbleiben und lediglich die Updates des Modells verschlüsselt an die Cloud übermittelt werden.

Gerade für Bereiche, in denen es aufgrund von sektoralen Geheimhaltungsbestimmungen oder Geschäfts- und Sicherheitsinteressen nicht gewünscht ist, Daten an Dritte weiterzugeben (Bankenwesen, Gesundheitsbereich, Versicherungen, Militär), eröffnet dezentrales Maschinenlernen neue Zukunftsoptionen. Die Dezentralisierung von digitaler Infrastruktur für KI-Lernen wird auch in Zukunft die umfassende Marktmacht großer Technologiekonzerne nicht mindern. Die Möglichkeiten von Federated Learning könnten aber zum vermehrten Eintritt neuer Akteure in den Markt für KI-Lernen führen, z .B. Start-ups in Nischenbereichen, wie z. B. Krebsforschung.[3] Durch einen offeneren Zugang zur KI-Infrastruktur und durch dezentrale KI-Lernmethoden könnten die Nutzung und Verbesserung von KI zu Effizienzgewinnen in prognostischen Anwendungen führen und damit gesellschaftliche Vorteile realisieren. Trotz vielversprechender Visionen, bestehen auch Zweifel an der neuen Technologie: KritikerInnen argumentieren, dass das geteilte, globale Prognosemodell durch jedeN TeilnehmerIn von Federated Learning manipuliert werden kann (Bagdasaryan et al. 2019).

Gerade bei der KI-Entwicklung wird deutlich, dass Forschungsprozesse und die mit ihnen verbundenen Risiken über institutionalisierte Grenzen der Wissenschaft hinaus- und in die Gesellschaft hineingetragen werden, d. h. Gesellschaft als Reallabor für experimentelle Forschung genutzt wird (Krohn/Weyer 1989). Ob dezentrale KI-Technologien begrenzen können, dass die Gesellschaft wie bisher als Experimentierfeld von Facebook, Amazon und Google dient, bleibt offen. Welche sozialen, ethischen und politischen Implikationen die Anwendung von Federated Learning für die Verarbeitung personenbezogener Daten hat, könnte weiterführend erarbeitet werden.

Zitierte Quellen

Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D. und Shmatikov, V., 2019, How To Backdoor Federated Learning, arxiv.org/pdf/1807.00459.pdf.

Krohn, W. und Weyer, J., 1989, Gesellschaft als Labor: Die Erzeugung sozialer Risiken durch experimentelle Forschung, *Soziale Welt* 40(3), 349-373.

Peters, R. und Krieger, B., 2022, Föderales Maschinelles Lernen. http://dx.doi.org/10.5445/IR/1000150233.

[3] owkin.com.