Föderales maschinelles Lernen

Themenkurzprofil Nr. 58 | Robert Peters • Benedikt Krieger | Mai 2022

Unter dem Begriff föderales Lernen (Federated Learning – FL) wird eine Alternative zu zentralen Ansätzen des maschinellen Lernens (Machine Learning – ML) verstanden. Zentrale ML-Architekturen führen Daten von Nutzer/innen zu einem großen Datenpool zusammen und trainieren auf dieser Grundlage KI-Modelle. Bei FL werden die Rohdaten der Nutzer/innen erst gar nicht an einen zentralen Server übertragen. Vielmehr wird das KI-Modell dezentral auf den jeweiligen Endgeräten der Nutzer/innen trainiert. Lediglich die Ergebnisse des lokal ausgeführten Trainingsprogramms werden anschließend zusammengeführt und für das Training eines zentralen KI-Modells verwendet. Unternehmen wie auch Datenschützer erhoffen sich davon eine höhere Akzeptanz bei Nutzer/innen, womit erhebliche gesellschaftliche und ökonomische Potenziale verbunden wären. Bei Smartphones und Sprachassistenten kommt FL bereits heute zum Einsatz. Im Zusammenhang mit industriellen Services, wie der vorausschauenden Instandhaltung (Predictive Maintenance), sind erste Anbieter am Markt. Für sensible Anwendungskontexte, wie das Gesundheitswesen und die Strafverfolgung, sind entsprechende Systeme in der Entwicklung. Jüngste Forschungsergebnisse deuten darauf hin, dass trotz zusätzlich implementierter Privacymechanismen (z.B. Differential Privacy und homomorphe Verschlüsselung) der Datenschutz durch FL nicht ohne Weiteres zu garantieren ist. Dies stellt Leistungsversprechen von Anbietern und bislang angenommene Vorteile beim Datenschutz grundsätzlich infrage. Sowohl für Unternehmen als auch für politische Entscheider/innen erwächst daraus unmittelbarer Handlungsbedarf.

Hintergrund und Entwicklung

Systeme der künstlichen Intelligenz[1] (KI) werden zunehmend für digitale Anwendungen genutzt. Insbesondere große Digitalkonzerne sind in der Lage, auf Basis von Nutzerdaten leistungsfähige und attraktive Produkte zu entwickeln (ITA 2020b) und dadurch ihre Stellung auf dem Markt immer weiter zu stärken (Winner-takes-all-Effekt) (LSE 2018). Ein Service, z.B. Suchmaschine, Empfehlungssystem bei Streaming- bzw. Verkaufsplattformen, wird für jede/n Nutzer/in umso wertvoller, je mehr Nutzungsdaten der Anbieter sammeln und verwerten kann (Netzwerkeffekt) (Haftor et al. 2021, S.199 f.). Unternehmen aggregieren auf diese Weise im Lauf der Zeit große Datenmengen. Sie verschaffen sich damit einen Vorteil beim Training ihrer KI-Modelle, z.B. gegenüber neu auf den Markt tretenden kleinen Anbietern, da neben der Qualität auch die Quantität von Daten, z.B. für das Training künstlicher tiefer neuronaler Netze, entscheidend ist (Groth/Straub 2021, S.9). Daher sammeln und speichern diese Unternehmen in der Regel die Daten ihrer Nutzer/innen zentral in Datenrepositorien – üblicherweise in einer Cloud (TAB 2015) – und trainieren mit ihnen KI-Modelle (ITA 2020b, S.1).

Zielkonflikt bei zentralen Ansätzen des maschinellen Lernens

Zentrale Ansätze des maschinellen Lernens[2] stehen einer Vielzahl von Herausforderungen gegenüber. So müs-

1 „Künstliche Intelligenz (KI) bezeichnet Systeme mit einem ‚intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwaregestützt in einer virtuellen Umgebung arbeiten (z.B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch in Hardwaresysteme eingebettet sein (z.B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des ‚Internet der Dinge')." (EK 2018)

2 Maschinelles Lernen ist ein Verfahren der künstlichen Intelligenz, bei denen Algorithmen auf Grundlage von Trainingsdaten eigene Funktions- und Analyseregeln ableiten (TAB 2020b, S.7).

sen die Daten zunächst von den Endgeräten der Nutzer/innen auf Server überführt werden. Je nach Anwendung ist dabei nur eine geringe Latenz der Datenübertragung akzeptabel, wenn Ergebnisse in Echtzeit zur Verfügung stehen sollen (ITA 2020a u. 2020b, S.1; Kar et al. 2022). Die zentrale Speicherung großer Datenmengen ist zudem aufwendig und bedeutet häufig Abhängigkeit von spezialisierten Anbietern (POST 2020b, S.3 f.). Es besteht außerdem das Risiko, dass durch einen unautorisierten Zugriff auf das Datenrepositorium eine große Menge von persönlichen Daten kompromittiert und missbräuchlich genutzt wird, etwa im Zuge von Hackerangriffen. Bei personenbezogenen Daten sind durch die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)[3] hohe Anforderungen definiert, unter welchen Umständen und zu welchem Zweck Daten überhaupt zentral zusammengeführt und ausgewertet werden dürfen. Konkret werden zentrale Ansätze des maschinellen Lernens durch die Zweckbindung, das Prinzip der Datensparsamkeit, die Speicherbegrenzung sowie Anforderungen an Integrität und Vertraulichkeit begrenzt. Sollen die Daten als Grundlage KI-basierter Technologien genutzt werden, entsteht damit ein grundsätzlicher Zielkonflikt: „Je mehr persönliche Daten eingesetzt werden, desto leistungsfähiger und präziser sind die KI-Anwendungen. Wird die Menge der Daten reduziert, um Datenschutzrisiken zu verringern, entsteht minderwertige Technologie, die das Potenzial von KI-basierten Anwendungen nicht ausschöpft." (Schallbruch et al. 2021, S.4)

Dezentrales maschinelles Lernen

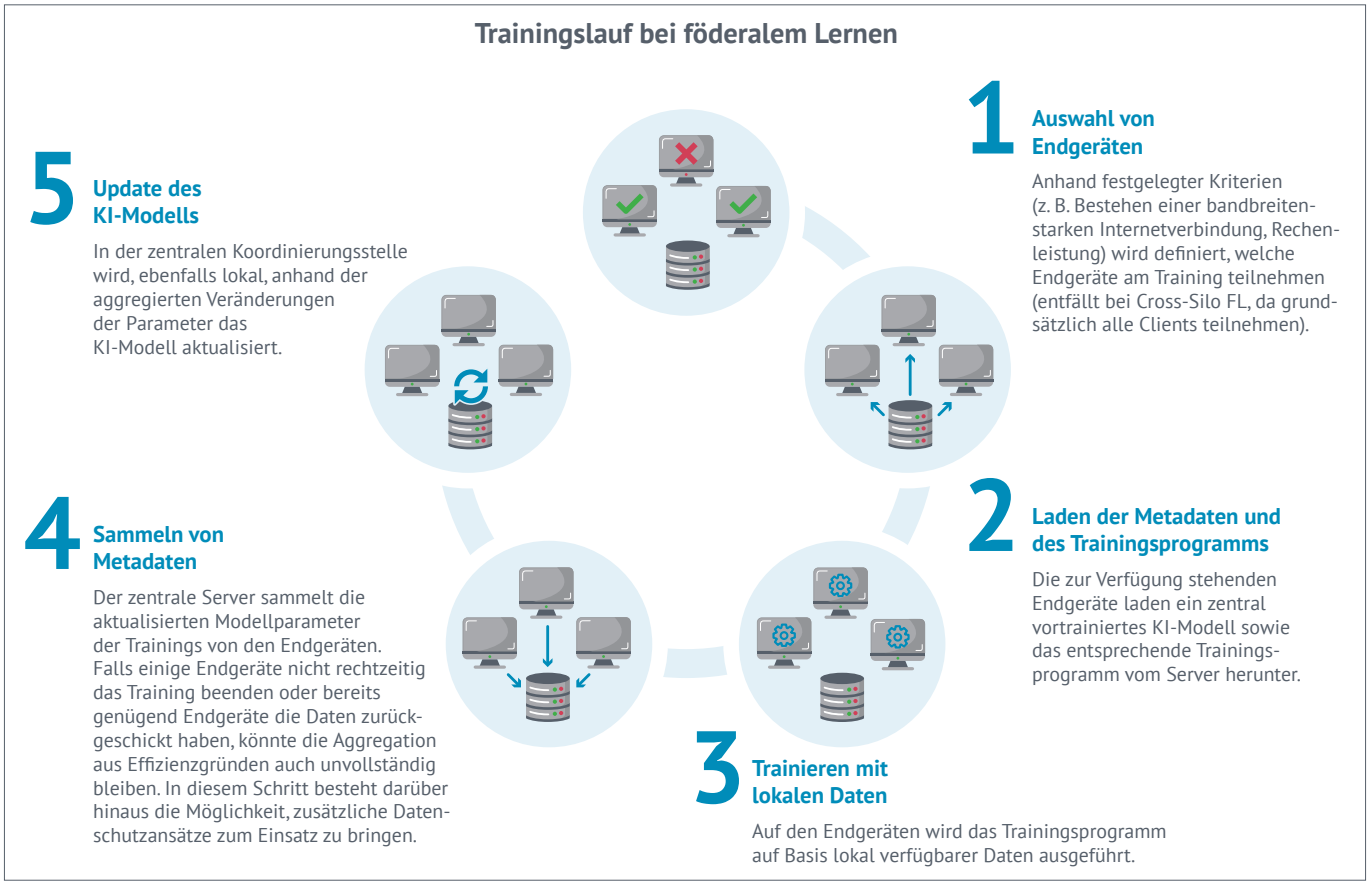
Vor diesem Hintergrund gewinnen dezentrale ML-Ansätze als alternative Architekturen in der Entwicklung und Anwendung von KI zunehmend an Bedeutung (ITA 2020b). Diese wurden u.a. von der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale des Deutschen Bundestages (2020) und vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Interview Kelber) als mögliche Privacy-by-Design-Technologien für maschinelles Lernen diskutiert. Bei dezentralen ML-Ansätzen erfolgt die Verarbeitung und zum Teil auch die Speicherung der zum Training eines KI-Modells verwendeten Daten nicht mehr in einem zentralen Datenrepositorium, sondern dezentral. Dazu wird eine Vielzahl von sogenannten Clients (z.B. Smartphones, unternehmensinterne IT-Systeme) mit einem zentralen Server vernetzt. Das Training des KI-Modells erfolgt dann zunächst beim Client (Al-Dulaimy et al. 2020; ITA 2020b, S.1).

Dezentrale ML-Ansätze lassen sich in zwei Formen unterteilen: verteiltes (distributed) und föderales Lernen. Bei verteiltem Lernen wird lediglich die Rechenleistung dezentraler Clients, z.B. lokaler Rechenzentren, genutzt. Das KI-Training erfolgt weiterhin mit einem zentral zusammengeführten und verwalteten Datenpool (Kairouz et al. 2021, S.6). Beim FL dagegen werden die Daten nicht nur dezentral verarbeitet, sie werden außerdem ausschließlich dezentral gespeichert (ITA 2020b, S.1). Bei FL sollen demnach Daten auf effektive Weise zum Zweck des maschinellen Lernens genutzt werden, ohne lokal erzeugte Daten teilen zu müssen (Zhou et al. 2021, S.2). Statt Daten der Endgeräte werden nur noch die sich mit dem Training anpassenden Parameter des zu trainierenden KI-Modells ausgetauscht (McMahan et al. 2017, S.1). Das damit verbundene Leistungsversprechen lautet: „Föderales Lernen ermöglicht es mehreren Parteien, gemeinsam ein neuronales Netz auf ihren kombinierten Daten zu trainieren, ohne dass die Privatsphäre einer der Teilnehmenden gefährdet wird." (Müller o.J.). Föderale ML-Architekturen sind ein vergleichsweise junger Ansatz, der in dieser Form erstmals von Forscher/innen des Unternehmens Google (McMahan et al. 2017) systematisch beschrieben wurde. Das Beratungsunternehmen Gartner (2021) zählt FL-Ansätze zu den Datenschutzinnovationen, die sich noch in einem frühen Entwicklungsstadium befinden.

Neben dem klassischen Ansatz, den Austausch der verschiedenen Clients über einen zentralen Server zu organisieren (Kairouz et al. 2021; Yang et al. 2019), gibt es auch komplett dezentrale Peer-to-Peer-Ansätze für FL-Architekturen (Rieke et al. 2020, S.2). In der Praxis lassen sich heute vor allem Ansätze zentral koordinierter FL-Architekturen finden, auf die sich die folgenden Betrachtungen konzentrieren. Sie können durch Cross-Device FL (Kairouz et al. 2021, S.6 ff.) oder Cross-Silo FL realisiert werden: Bei Cross-Device FL trainiert eine große Zahl von Endgeräten, etwa Smartphones oder autonome Fahrzeuge, ein KI-Modell. Bei Cross-Silo FL trainieren nicht einzelne Endgeräte, sondern ganze Organisationen (z.B. Krankenhäuser, Finanzdienstleister, Industrieunternehmen) und/oder geografisch verteilte Rechenzentren mit ihren Daten ein KI-Modell (Kairouz et al. 2021, S.6 ff, 14 ff.) In beiden Fällen handelt es sich um Systeme, bei denen die Aggregation

3 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Abb. 1 Fünf Schritte des föderalen Lernens – Iteration



Eigene Darstellung nach Kairouz et al. 2021; Rieke et al. 2020

der verschiedenen Parameterupdates eines KI-Modells zentral erfolgt und eine Vielzahl partizipierender, föderaler Endgeräte (oder Rechenzentren) mit ihren lokalen Daten ein KI-Modell trainiert. Das heißt, während bei zentralen Lernarchitekturen mit zentraler Rohdatenspeicherung die Rohdaten zum Modell gebracht werden, wird beim FL das KI-Modell dorthin gebracht, wo die Rohdaten sind (Rieke et al. 2020, S. 2). In der Regel wird beim FL ein KI-Modell zunächst mittels zentralisierter Daten vortrainiert, bevor dieses föderal weiterentwickelt wird. Abbildung 1 zeigt eine idealtypische (iterative) Lernschleife (Kairouz et al. 2021, S. 8) für das föderale Training von KI-Modellen in einer Cross-Device-Architektur.

Auch wenn FL-Ansätze häufig im Kontext von Datenschutzerwägungen genannt werden und die dabei verwendeten Rohdaten nicht das jeweilige Endgerät verlassen, gibt es noch keine Garantie dafür, dass die Nutzerdaten vor unerwünschtem Zugriff geschützt bleiben (Kaissis et al. 2020). Denn ohne weitere Maßnahmen können beispielsweise aus den Updates der Parameter des KI-Modells Rückschlüsse auf die Rohdaten der Nutzer/innen gezogen werden (Mammen 2021, S. 3). Zum Schutz personenbezogener und sonstiger schutzwürdiger Daten werden bislang vor allem bei der Übermittlung der clientsspezifischen Modellparameterupdates (Schritt 4) weitere Maßnahmen ergriffen. Dazu zählt insbesondere das Prinzip Differential Privacy (Enquete Kommission 2020, S. 68). Hier wird den auszutauschenden Daten ein künstlich erzeugtes Rauschen hinzugefügt, was dazu führt, dass die ursprünglichen Daten nicht mehr eindeutig rekonstruierbar sind. In der Aggregation der verrauschten Daten können dann ohne Rückschlüsse auf das Individuum trotzdem Erkenntnisse gewonnen werden. Dabei wird das Rauschen mit der Sensibilität der Daten skaliert. Der Abruf von sehr sensiblen Daten führt somit zu einem Hinzufügen von mehr Rauschen und vice versa (Jain et al. 2018, S. 1 ff.). Ebenfalls möglich ist die Absicherung der clientspezifischen Parameterupdates des KI-Modells über die homomorphe Verschlüsselung. Diese erlaubt die Verarbeitung von verschlüsselten Daten mit dem gleichen Ergebnis wie bei Verarbeitung der entschlüsselten Daten. Damit bleiben die Daten in der gesamten Verarbeitungskette verschlüsselt und abgesichert, ohne die Verarbeitung zu kompromittieren (Wiese et al. 2018, S. 1 ff.). Während die bisherige Forschung solchen Maßnahmen eine hohe Relevanz beimisst (Kairouz et al. 2021), zeigt eine jüngste Untersuchung, dass die bislang diskutierten Mechanismen zur Absicherung von Privacy bei FL unzureichend sind: Sie unterschätzen das Risiko einer Manipulation durch die koordinierende Zentralinstanz und können selbst durch aufwendige Absicherung nicht den Schutz sensibler Daten gewährleisten (Boenisch et al. 2021).

Föderales Lernen kommt in der Praxis an

Strategien und Ansätze, um Datenverarbeitung unter Wahrung der Privatsphäre und des Datenschutzes zu realisie-

ren, werden bereits seit Jahrzehnten erforscht. Erst seit den 2010er Jahren gelingt es jedoch zunehmend, konkrete Konzepte in die Praxis zu bringen (Apple 2017; Kairouz et al. 2021, S.5). Mittlerweile wird FL in zahlreichen digitalen Endkundenanwendungen eingesetzt: z.B. virtuelle Tastaturen für Smartphones und Tablets, Spracherkennung und Dialogsysteme. Besonderes Potenzial liegt dabei in Anwendungsfeldern, für die besonders schützenswerte Daten vorliegen, die für zentrale ML-Anwendungen nur bedingt zur Verfügung stehen, weil rechtliche Hürden (etwa Strafverfolgung und Kriminalitätsprävention) oder individuelle wie institutionelle Vorbehalte bestehen, Daten zu teilen (z.B. bei industriellen Anwendungen). Nachfolgend werden ohne Anspruch auf Vollständigkeit exemplarische Anwendungspotenziale für die genannten Felder erläutert.

Virtuelle Tastatur für Smartphones und Tablets

Alphabet setzt bei seinem „Gboard mobile Keyboard", das für Geräte mit dem Betriebssystem „Android" angeboten wird, bereits auf das FL-Prinzip. Die Anwendung berechnet das von Nutzer/innen wahrscheinlich als nächstes geschriebene Wort, um entsprechende Vorschläge anzuzeigen. Dazu wird ein zentral vortrainiertes ML-Modell an das Endgerät übertragen und dort unter Einbezug individueller Nutzerdaten dezentral weiter trainiert. Auf dem Endgerät können kontextabhängige (Wochentag und Tageszeit) sowie nutzerprofilspezifische Faktoren (z.B. Clickverhalten) und Merkmale der Nutzungshistorie (etwa Ansichten von Apps, Anzeigen, Internetseiten der vergangenen Minuten oder Stunden) zum Training genutzt werden. Das Endgerät überträgt dann lediglich ein Update des Modells und nicht die Nutzerdaten an den Server (Yang et al. 2018). Auch bei Apple-Betriebssystemen kommt FL zur Optimierung der Wortvorhersage zum Einsatz (Hao 2019).

Spracherkennung und Dialogsysteme

Alphabet und Apple setzen FL bei ihren Betriebssystemen für mobile Endgeräte ein, um die Spracherkennung und die Dialogsysteme zu optimieren. So nutzt Apple ab iOS 13 FL für die Optimierung seines Sprachassistenzsystems. Für Sprachtechnologien erscheinen föderale ML-Architekturen aus Sicht der Anbieter besonders sinnvoll, da entsprechende Systeme gerade unter Datenschutzgesichtspunkten seit Jahren in der Kritik stehen (Clauser 2019). Dabei nutzt Apple zudem das Prinzip Differential Privacy (Hao 2019). In Android-Geräten wird FL auch zur Vermeidung von Fehlaktivierungen des Google Assistant genutzt (Russel 2021).

Gesundheitswesen

Im Gesundheitswesen liegen hochgradig sensible Daten vor, deren Auswertung jedoch dabei helfen könnte, beispielsweise die Behandlung von Krankheiten zu verbessern. Mit Vorhaben wie der „Sentinel Initiative" der U.S. Food and Drug Administration wird versucht, entsprechende dezentrale Datensammlungen aufzubauen und mittels konventioneller Analyseverfahren zu erschließen (Tho 2022). Für FL besteht in diesem Bereich eine Reihe potenzieller Anwendungsszenarien (Rieke et al. 2020, S.3). So lassen sich mit FL Vorhersagemodelle über Krankheitsverläufe und damit einhergehender Interventionsbedarfe entwickeln, z.B. für den vermutlichen Sauerstoffbedarf symptomatischer Covid-19-Erkrankter (Dayan et al. 2021). Dabei gewinnen sowohl Cross-Silo- als auch Cross-Device-Ansätze an Bedeutung. Cross-Silo-Ansätze werden gegenwärtig verfolgt,

um z.B. Daten verschiedener Krankenhäuser für künftige Data-Mining- bzw. ML-Analysen zu Forschungszwecken erschließen zu können, etwa im Bereich der Krebserkennung bzw. der Wirkstoffforschung.[4] Cross-Device-Ansätze sind wiederum vor allem dann relevant, wenn, wie im Falle der App doc.ai, Angebote zur Erfassung und Auswertung gesundheitsrelevanter Daten für den Business-to-Costumer-Bereich entwickelt und angeboten werden. Hier kommt FL bereits zum Einsatz (De Brouwer 2019). Eine potenzielle Kombination von Cross-Silo- und Cross-Device-Ansätzen wurde z.B. für Systeme zur Pandemiefrüherkennung beschrieben (Schallbruch et al. 2021, S.6).

Strafverfolgung und Prävention

Seit vielen Jahren wird darüber diskutiert, wie und in welcher Form KI-Technologien zur Prävention und Verfolgung von Straftaten eingesetzt werden können. Behörden sammeln bereits heute eine Vielzahl von Daten, etwa über Anzeigen, Straftaten und deren Hergang sowie Verdächtige und Opfer von Delikten. Immer wieder wird in der Debatte die Bedeutung eines behördenübergreifenden Datenaustausches hervorgehoben. Zugleich wird das Sammeln und Auswerten von Daten zum Zweck der Strafverfolgung immer wieder diskutiert, insbesondere mit Blick auf Folgen für Freiheitsrechte. FL-Ansätze könnten hier einen möglichen Ausweg aus dem Dilemma der Gewährleistung sowohl von Freiheit als auch von Sicherheit weisen, indem Behörden untereinander künftig nicht mehr personenbezogene Daten austauschen, sondern lediglich das durch lokal trainierte KI-Modelle erfasste Erfahrungswissen (Schallbruch et al. 2021, S.8). In der Praxis spielen entsprechende Anwendungen derzeit noch keine Rolle. Strafverfolgungsbehörden aus 14 EU-Staaten untersuchen unter Beteiligung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), einer Bundesanstalt im Geschäftsbereich des deutschen Bundesministeriums des Innern und für Heimat, in einem gemeinsamen Forschungsprojekt, wie Technologien des FL zum Kampf gegen Kindesmissbrauch genutzt werden können (Global Response Against Child Exploitation o.J.).

Industrielle Anwendungen

Auch die Industrie unterliegt bei der Nutzung von ML einem grundlegenden Dilemma: Einerseits sind Unternehmen bestrebt, zum Zweck der Effizienzsteigerung und zur Etablierung neuer Services ML zu nutzen, andererseits hat auch für sie die Hoheit über sensible Unternehmensdaten (etwa über Produkte und deren Herstellung) einen hohen Wert. Daher spielt FL auch für die Realisierung von Industrie-4.0-Konzepten und konkreten Anwendungen (z.B. Predictive Maintenance) sowie in der digitalisierten Landwirtschaft potenziell eine wichtige Rolle (eoda GmbH 2020; Zhou et al. 2021). KI-Anbieter wie die Katulu GmbH[5] bieten gemeinsam mit Maschinenherstellern FL-basierte Lösungen an, die Datensouveränität wahren und zugleich leistungsfähige Services ermöglichen sollen (Interview Schlinkert). Im EU-Forschungsprojekt „Musketeer“[6] soll eine Plattform für ML mit verteilt gehaltenen Industriedaten entwickelt werden

Herausforderungen bei der Entwicklung und Adaption föderaler Architekturen

Trotz vielversprechender Anwendungsszenarien bestehen Barrieren für die Entwicklung und Einführung von FL in der Praxis. Eine Herausforderung besteht in der statistischen Uneinheitlichkeit der Trainingsdaten. Anhand der übertragenen Modellparameterupdates kann keine Aussage darüber getroffen werden, von welcher statistischen Qualität die Trainingsdaten sind, was zu Verzerrungen im KI-Modell führen und damit dessen Leistungsfähigkeit beeinflussen kann (Mammen 2021, S.3; Kairouz et al. 2021, S.75 f., 82 ff.). Eine weitere Herausforderung besteht darin, wie mobile Endgeräte privater Nutzer/innen einbezogen werden können, ohne beispielsweise Rechenkapazitäten, Datenvolumina, Akkuleistung oder die eigentliche, zeitgleich stattfindende Nutzung zu sehr zu beinträchtigen (Kairouz et al. 2021, S.81 ff.). Ein weiteres Problem für FL-basierte Architekturen ist der Umgang mit intendierter Beeinflussung des KI-Modells, z.B. um dem jeweiligen Anbieter einen wirtschaftlichen Schaden zuzufügen. So besteht potenziell die Gefahr, dass Trainingsdaten auf fremden Endgeräten manipuliert oder kompromittierte Endgeräte bewusst eingeschleust werden (Kairouz et al. 2021, S.62 ff.). Für diese Herausforderungen zeichnen sich jedoch Lösungen ab, insbesondere informatische Ansätze, wie beispielsweise das statistische Einpreisen heterogener Qualität der Rohdaten

4 Mit der „Joint Imaging Platform“ des Deutschen Konsortiums für Translationale Krebsforschung wird beispielsweise ein FL-Ansatz verfolgt (https://jip.dktk.dkfz.de/jiphomepage/; 11.5.2022). Verschiedene Pharmaunternehmen arbeiten im EU-Projekt „MELLODDY“ gemeinsam an Ansätzen zur Entdeckung neuer pharmazeutischer Wirkstoffe mittels FL. Einige deutsche Kliniken sind zudem in der internationalen „Federated Tumor Segmentation (FeTS) initiative“ involviert (University of Pennsylvania o.J.).

5 katulu.io/de (1.6.2022)

6 https://musketeer.eu (1.6.2022)

in die von Clients übermittelten Modellparameterupdates, um Verzerrungen des aggregierten Modells zu reduzieren (Kairouz et al. 2021, S.79; Li et al. 2019). Dennoch müssen bei der Konstruktion einer FL-Anwendung mögliche systembedingte Schwächen hinsichtlich Datenschutz und Sicherheit in den Phasen der Datensammlung bzw.-auswahl, des Trainings sowie der Verwendung des Modells einbezogen werden (Liu et al. 2022, S.15). Dies gilt insbesondere, wenn die Anwendung sensible Bereiche betrifft, wie etwa Gesundheitsdaten (Pfitzner et al. 2021, S.24). Nicht zuletzt erfordert das FL – wie alle datenbasierten Ansätze – die Bereitschaft derjenigen, die über die Daten verfügen, andere an den Lernergebnissen aus den Daten teilhaben zu lassen, zumal sie mit ihrer lokalen Rechenkapazität auch einen Teil der Ressourcen beisteuern müssen.

Gesellschaftliche und politische Relevanz

Soziale und ethische Aspekte

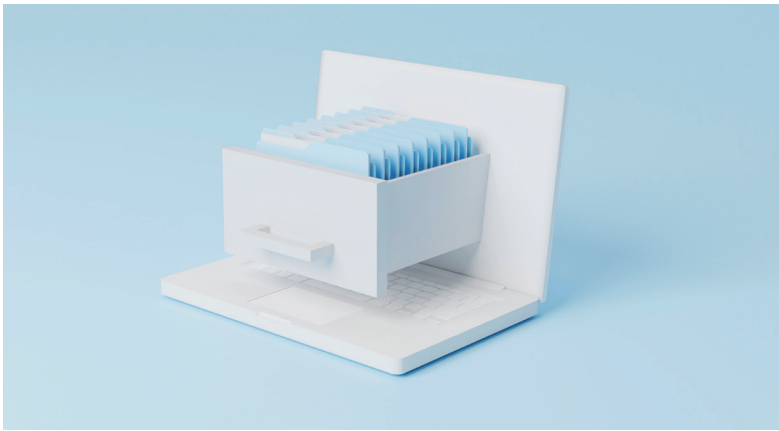
Personenbezogene und andere sensible Daten mit Methoden der künstlichen Intelligenz auszuwerten, birgt gesellschaftlich erhebliche Chancen, etwa im Gesundheitswesen oder in der Strafverfolgung. Daher besteht auch in solchen sensiblen Anwendungskontexten das Bedürfnis, große Mengen von Daten für das Training von KI-Modellen zu nutzen (Aledhari et al. 2020, S.1; Schallbruch et al. 2021, S.4). Während hier bislang vor allem auf zentrale Datenspeicher und KI-Architekturen zurückgegriffen wurde, ermöglichen leistungsfähige Endgeräte und die Verfügbarkeit bandbreitenstarker Internetverbindungen heute ein Umdenken: weg von zentralen Architekturen hin zu föderalen Strukturen (Interview Kelber). Als weiteres Anwendungsszenario wird die Nutzung von FL-Architekturen im Kontext von Trusted-Rechenzentren diskutiert, die als Datentreuhänder fungieren und als dezentrale Datenpools eingerichtet werden könnten. Trusted-Rechenzentren wurden von der Enquete-Kommission (2020, S.177) angeregt und sind nicht einheitlich definiert. Sie könnten insbesondere dort, wo bislang eine Zusammenführung sensibler Daten nicht realisiert wurde (z.B. im Gesundheitssektor), als Clients in Cross-Silo-FL-Architekturen eingesetzt werden (Interview Zweig).

Bisherige Erkenntnisse deuten darauf hin, dass FL systemische Risiken traditioneller ML-Ansätze reduziert (Kairouz et al. 2021, S.1). Föderale Ansätze versprechen daher, Potenziale des ML voll ausschöpfen zu können, die aufgrund der geschilderten Risiken nicht genutzt werden konnten: „Aus sozioinformatischer Betrachtung sind Menschen vermutlich eher dazu bereit, ihre Daten zur Verfügung zu stellen, wenn sie wissen, dass diese ihr Endgerät nicht verlassen. Dann würden Ansätze des föderalen Lernens potenziell zu besseren Ergebnissen führen als zentrale KI-Architekturen“, so Katharina Zweig von der Technischen Universität Kaiserslautern (Interview Zweig). Auch der Bundesdatenschutzbeauftragte Ulrich Kelber geht davon aus, dass mittels FL eine breitere Datengrundlage erzeugt und KI-Modelle und darauf aufbauende Angebote qualitativ verbessert werden können (Interview Kelber). Durch jüngste Forschungsergebnisse wird das mit FL zuweilen verbundene Versprechen eines systemimmanenten Datenschutzes und darüber hinausgehende Erwartungen jedoch infrage gestellt. Daten von Boenisch et al. (2021) deuten darauf hin, dass auch derzeit angewendete und diskutierte zusätzliche Mechanismen, wie Differential Privacy und homomorphe Verschlüsselung, anders als bislang angenommen, die koordinierende Instanz einer FL-Architektur (z.B. den Anbieter eines FL-basierten digitalen Services) nicht davon abhalten, Rohdaten der Nutzer/innen zumindest teilweise zu rekonstruieren. FL würde demnach weitaus aufwendigere als die bislang implementierten Privacymechanismen erfordern, die einen erhöhten Kommunikationsaufwand zwischen Zentralinstanz und Clients mit sich bringen und damit einen Vorteil von FL-Architekturen zunichtemachen würden (Boenisch et al. 2021, S.14). Bis entsprechende alternative kryptografische Ansätze für FL entwickelt sind, bleibt den Nutzer/innen in der Praxis lediglich die Option, nur an solchen FL-Protokollen teilzunehmen, bei denen sie der zentralen Instanz vorbehaltlos vertrauen (Interview Boenisch). Entsprechende Risiken sind auch deshalb sehr ernst zu nehmen, weil FL-Ansätze dafür genutzt werden können, auf weit größere Datenbestände zuzugreifen, als dies bisher mit Big-Data- und cloudbasierten Ansätzen möglich und akzeptiert war (Kaspersen 2022).

Zu berücksichtigen ist auch, dass FL anfällig ist für Verzerrungen, die aufgrund der Auswahl von Clients entstehen. So wählen Digitalkonzerne, die bereits auf FL setzen, in der Regel nur Clients mit hohen Systemvoraussetzungen für das Training ihrer Modelle aus (z.B. Akkuleistung, verfügbare Rechenkapazitäten). Dadurch können Daten von Nutzer/innen mit älteren oder leistungsschwächeren Endgeräten häufig nicht am Training teilnehmen. Dies verzerrt die Trainingsdaten zugunsten von Nutzer/innen mit hochwertigen Premiumendgeräten (Interview Boenisch).

Ökonomische Aspekte

Relevante Potenziale und Chancen bestehen auch in ökonomischer Hinsicht. Unmittelbar profitiert zunächst die



zentrale Instanz, z.B. Alphabet und Apple, die zum Training ihrer KI-Modelle föderale Ansätze nutzt. So reduzieren sich deren Kosten für den Betrieb von Serverinfrastrukturen, wenn erhebliche Teile des Trainings bei den Clients erfolgen. Darüber hinaus lassen sich mit dem Versprechen hohen Datenschutzes neue Anwendungspotenziale erschließen. So könnten auch sensible Unternehmensdaten für die Anwendung von ML-Verfahren unproblematischer zur Verfügung gestellt werden, wenn Unternehmen diese auf ihren eigenen Servern bereitstellen und eine Kompromittierung ausgeschlossen werden kann. Wenn Produktionsdaten das Training von Predictive-Maintenance-Systemen oder die Inline-Qualitätskontrolle (Echtzeitüberwachung von Produktionsprozessen zum Zweck der Qualitätssicherung) verbessern, reduziert dies für das produzierende Gewerbe Kosten (z.B. durch die Vermeidung von Totzeiten) und hat auch ökologisch positive Effekte, etwa durch die Minimierung von Ausschussmengen. Dabei könnten auch kleine und mittlere Unternehmen von FL profitieren. Sie erzeugen zwar bei ihrer Produktion zu wenig Daten, um allein für ihre Produktion KI-Modelle sinnvoll einsetzen zu können. Mittels FL können sie aber ohne Weitergabe eigener Produktionsdaten an den Erfahrungen anderer Unternehmen teilhaben: „Federated Learning versetzt Unternehmen in die Lage, miteinander zu lernen, ohne etwas übereinander zu lernen." (Interview Schlinkert) Damit könnten auch solche Unternehmen ML effektiv und effizient einsetzen, die bislang aufgrund der geringen Größe ihres Datenbestands nur sehr begrenzt von den Potenzialen datenbasierter Optimierung profitieren können (TAB 2019).

Auch bei digitalen B2C-Anwendungen könnten solche Anbieter wirtschaftliche Vorteile im Wettbewerb erlangen, die ihren Nutzer/innen mit FL eine höhere Kontrolle über die eigenen Daten und somit höheren Datenschutz zusichern (Interview Korneeva). Mit Blick auf die internationale Konkurrenzfähigkeit deutscher und europäischer Technologieanbieter könnte FL damit die Entwicklung datenschutzkonformer, hoch innovativer digitaler Dienste voranbringen. Um die dazu notwendige Glaubwürdigkeit zu erlangen, müssen Systemanbieter jüngste Erkenntnisse zu Defiziten bisher implementierter Privacymechanismen bei FL ernst nehmen, gegenüber ihren Nutzer/innen die daraus resultierenden Konsequenzen kommunizieren und ihre Leistungsversprechen dahingehend anpassen.

Ökologische Aspekte

Zentrale KI-Architekturen und insbesondere bestimmte Deep-Learning-Ansätze erfordern den Einsatz erheblicher Energieressourcen für ihre Entwicklung und das Training (Strubell et al. 2019). Zugleich erlaubt die Konzentrierung der Datenhaltung und Rechenleistung in modernen Cloudsystemen auch den Einsatz besonders effizienter und energiesparender Technologien (Masanet et al. 2020; Strubell et al. 2019). Bislang ist jedoch unklar, ob und unter welchen Umständen FL einen geringeren CO_2-Fußabdruck als zentrale KI-Architekturen aufweist und bis zu welchem Grad dieser minimiert werden kann (Guler/Yener 2021; Qiu et al. 2020). Einerseits bestehen Einsparmöglichkeiten, etwa aufgrund des geringeren Kommunikationsaufwands, andererseits lassen sich die sehr unterschiedlichen Geräte nicht ähnlich effizient zum Einsatz bringen wie ein zentrales System (POST 2020a). Hier besteht offenbar weiterer Forschungsbedarf (Qiu et al. 2020).[7] Darauf müssen KI-Anbieter, die bereits FL verwenden, dringend reagieren, um ökologische wie ökonomische Nachteile zu vermeiden.

Politische Relevanz

Politisch stellt sich vor allem die Frage, ob es gelingt, die bislang von Systemanbietern postulierten Vorzüge von FL als Privacy-by-Design-Ansatz tatsächlich zu realisieren. Das Potenzial dazu wird grundsätzlich als erheblich eingeschätzt. So erhofft sich Ulrich Kelber (Interview Kelber), dass FL einen Beitrag leisten kann, um vermeintliche Gegensätze von Datenschutz und Innovationsfähigkeit zu überwinden: „Richtig eingesetzt, können wir mit föderalem Lernen mehr Innovation erreichen und zugleich dem Datenschutz besser gerecht werden, als es sich heute in der Praxis zeigt."

Anpassungen scheinen vor allem in solchen Bereichen sinnvoll bzw. notwendig zu sein, in denen digitale Dienste nicht mit europäischem Datenschutzrecht konform sind. Dies gilt z.B. für Sprachtechnologien, die mittels großer Sprachmodelle arbeiten und dazu Daten europäischer Bürger/innen via Programmierschnittstellen an Server in den USA übermitteln (Peters 2022; TAB 2022). Hier gilt es, die schon bestehenden Rechtsnormen auch anzuwenden, um damit die Marktchancen für Technologien mit hohen Datenschutzstandards zu verbessern (Interview Kelber). Die jüngst aufgedeckten Defizite bei bislang im-

7 Erste Schritte zur Berechnung des CO_2-Fußabdrucks wurden 2021 von einem Team europäischer Forschungseinrichtungen vorgestellt (Qiu et al. 2021).

plementierten Privacymechanismen für FL zeigen aber auch eine mögliche Lücke in der Anwendung im bisherigen Datenschutzrecht auf: So sollten etwa auch die clientspezifischen Updates von Modellparametern, die von natürlichen Personen genutzt werden, wie personenbezogene (Roh-)Daten behandelt werden (Interview Boenisch). Wenn, wie Boenisch et al. (2021) zeigen, die von Clients übermittelten Modellparameterupdates eine Rekonstruktion personenbezogener Rohdaten ermöglichen, sind diese Daten – anders als bislang angenommen – personenbeziehbar, womit Anbieter hier die Vorgaben der Datenschutz-Grundverordnung einhalten und z.B. die Zustimmung der am FL-Protokoll teilnehmenden Nutzer/innen von Clients einholen müssen: „Personenbeziehbare Metadaten sind personenbezogene Daten und damit ist die DSGVO anzuwenden. Es kommt jetzt darauf an, auch die Metadaten in einer Form zu behandeln, dass die datenschutzrechtlichen Vorteile von FL voll zum Tragen kommen (Interview Kelber). Die angesprochenen jüngsten Forschungsergebnisse wären darüber hinaus auch auf ihre Konsequenz für bestehende Angebote am Markt und laufende Forschungsprojekte zu prüfen, insbesondere dann, wenn diese mit öffentlichen Geldern unterstützt werden. Es scheint förderpolitisch zudem sinnvoll, neue Untersuchungen anzustrengen, die alternative oder ergänzende Privacymechanismen für FL entwickeln. Neben vertieften Forschungsanstrengungen wären zukünftig Standards für FL (Yang et al. 2019, S.15) sowohl auf die Privacyziele als auch auf Effektivität und (u.a. ökologische) Effizienz zu entwickeln.

Mögliche vertiefte Bearbeitung des Themas

Die aufgezeigten Potenziale und Herausforderungen, die mit FL-Anwendungen verbunden sind, hängen wesentlich von den technisch-informatischen Entwicklungen beim ML und verteilten Rechnen ab. Anwendungen der KI und des ML wurden und werden bereits intensiv auf ihre gesellschaftlichen, ethischen, rechtlichen sowie ökonomischen und ökologischen Auswirkungen sowohl durch wissenschaftliche als auch politische Institutionen, u.a. die Enquete-Komission des Deutschen Bundestages und die Datenethikkommission der Bundesregierung, hin untersucht. Aspekte, die die hier diskutierten FL-Ansätze betreffen, wurden zuletzt in Untersuchungen des TAB zu den Themen Energieverbrauch der IKT-Infrastruktur sowie Data Mining (beide Berichte im Erscheinen), Digitalisierung der Landwirtschaft (TAB 2021a u. 2021b) und Autonome Waffensysteme (TAB 2020b) behandelt ebenso wie in den Themenkurzprofilen zu KI-basierten Dialogsystemen (TAB 2022) und zum ML jenseits von Big Data (TAB 2019). Eine Bearbeitung des Themas aus einer umfassenden TA-Perspektive heraus stünde vor der Herausforderung, den möglichen Implikationen in den vielen Anwendungsfeldern gerecht zu werden und gleichzeitig mit dem Tempo der sehr dynamischen Entwicklung Schritt zu halten. Anstelle einer solchen sehr aufwendigen Herangehensweise bietet es sich an, Aspekte und Perspektiven des föderalen ML jeweils im Rahmen passender anwendungsbezogener Studien aufzugreifen.

Literatur

- Al-Dulaimy, A.; Sharma, Y.; Gokan Khan, M.; Taheri, J. (2020): Introduction to edge computing. In: Taheri, J.; Deng, S. (Hg.): Edge computing. Models, technologies and applications. London, S.3–25
- Aledhari, M.; Razzak, R.; Parizi, R.; Saeed, F. (2020): Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. In: IEEE access 8, S. 140699–140725
- Apple (2017): Learning with Privacy at Scale. https://machinelearning.apple.com/research/learning-with-privacy-at-scale (11.5.2022)
- Boenisch, F.; Dziedzic, A.; Schuster, R.; Shamsabadi, A. S.; Shumailov, I.; Papernot, N. (2021): When the Curious Abandon Honesty: Federated Learning Is Not Private. https://arxiv.org/pdf/2112.02918
- Clauser, G. (2019): Amazon's Alexa Never Stops Listening to You. Should You Worry? https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/ (11.5.2022)
- Dayan, I.; Roth, H. R.; Zhong, A.; Harouni, A.; Gentili, A.; Abidin, A.; Liu, A.; Costa, A.; Wood, B.; Tsai, C.-S.; Wang, C.-H. et al. (2021): Federated learning for predicting clinical outcomes in patients with COVID-19. In: Nature medicine 27(10), S.1735–1743
- De Brouwer, W. (2019): The Federated Future is ready for shipping. Medium, 11.3.2019, https://medium.com/@_doc_ai/the-federated-future-is-ready-for-shipping-d17ff40f43e3 (11.5.2022)
- Enquete-Kommission (Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale) (2020): Bericht der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale. Unterrichtung, Deutscher Bundestag, Drucksache 19/23700, Berlin
- Eoda GmbH (2020): Federated Learning. Mit Federated Learning zu erfolgreichen KI- und Data-Science-Projekten. Whitepaper. https://www.eoda.de/wp-content/uploads/2020/11/Whitepaper-Federated-Learning-eodaGmbH_YUNA_elements.pdf (11.5.2022)
- Europäische Kommission (2018): Künstliche intelligenz in Europa. Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. (EU-Kommission 2018 S.1, https://www.kowi.de/Portaldata/2/Resources/fp/2018-COM-Artificial-Intelligence-de.pdf) (29.11.2021)
- Gartner Inc. (2021): Gartner Says Digital Ethics is at the Peak of Inflated Expectations in the 2021 Gartner Hype Cy-

cle for Privacy. https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate (11.5.2022)
- German Cancer Consortium (o.J.): Joint Imaging Platform. https://jip.dktk.dkfz.de/jiphomepage/ (11.5.2022)
- Global Response Against Child Exploitation (o.J.): GRACE - Global Response Against Child Exploitation. https://www.grace-fct.eu/ (11.5.2022)
- Groth, O.; Straub, T. (2021): Analyse aktueller globaler Entwicklungen im Bereich KI mit einem Fokus auf Europa. Konrad-Adenauer-Stiftung e.V.
- Guler, B.; Yener, A. (2021): Sustainable Federated Learning. https://arxiv.org/pdf/2102.11274 (1.6.2022)
- Haftor, D.; Costa Climent, R.; Eriksson Lundström, J. (2021): How machine learning activates data network effects in business models: Theory advancement through an industrial case of promoting ecological sustainability. In: Journal of Business Research 131, S.196–205
- Hao, K. (2019): How Apple personalizes Siri without hoovering up your data. https://www.technologyreview.com/2019/12/11/131629/apple-ai-personalizes-siri-federated-learning/ (11.5.2022)
- ITA (Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften) (2020a): Cloud Computing als politische Herausforderung. Wien
- ITA (2020b): Dezentrales KI-Lernen: Gesellschaft als Reallabor? Wien
- Jain, P.; Gyanchandani, M.; Khare, N. (2018): Differential privacy: its technological prescriptive using big data. In: Journal of Big Data 5(1)
- Kairouz, P.; McMahan, H.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; D'Oliveira, R. et al. (2021): Advances and Open Problems in Federated Learning. In: Foundations and Trends in Machine Learning (Vol 4 Issue 1, revised version 3)
- Kaissis, G.; Makowski, M.; Rückert, D.; Braren, R. (2020): Secure, privacy-preserving and federated machine learning in medical imaging. In: Nat Mach Intell 2(6), S.305–311
- Kar, B.; Yahya, W.; Lin, Y.-D.; Ali, A. (2022): A Survey on Offloading in Federated Cloud-Edge-Fog Systems with Traditional Optimization and Machine Learning. arXiv, https://arxiv.org/pdf/2202.10628.pdf (10.5.2022)
- Kaspersen, A. (2022): AI, Movable Type, & Federated Learning, with Blaise Aguera y Arcas. https://www.carnegiecouncil.org/studio/multimedia/20220119-ai-movable-type-federated-learning-blaise-aguera-y-arcas (11.5.2022)
- Li, T.; Sahu, A.; Talwalkar, A.; Smith, V. (2019): Federated Learning: Challenges, Methods, and Future Directions. Nr. 3, https://arxiv.org/pdf/1908.07873 (1.6.2022)
- Liu, P.; Xu, X.; Wang, W. (2022): Threats, attacks and defenses to federated learning: issues, taxonomy and perspectiveS. In: Cybersecurity 5(1)
- LSE (ondon School of Economics and Political Science) (2018): Why Tech Markets Are Winner-Take-All. https://blogs.lse.ac.uk/medialse/2018/06/14/why-tech-markets-are-winner-take-all/ (10.5.2022)
- Mammen, P. M. (2021): Federated Learning: Opportunities and Challenges. https://arxiv.org/pdf/2101.05428.pdf (1.6.2022)
- Masanet, E.; Shehabi, A.; Lei, N.; Smith, S.; Koomey, J. (2020): Recalibrating global data center energy-use estimates. In: Science. New York, 367(6481), S.984–986
- McMahan, H.; Moore, E.; Ramage, D.; Hampson, S.; Aguera y Arcas, B. (2017): Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International, S.1273–1282, http://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf (28.3.2022)
- Müller, K. (o.J.): Federated Learning. Fraunhofer HHI, https://www.hhi.fraunhofer.de/en/departments/ai/research-groups/efficient-deep-learning/research-topics/federated-learning.html (10.5.2022)
- Peters, R. (2022): Europäische Sprachmodelle und die Rolle des Staates im Innovationsökosystem. Tagesspiegel Backround, 4.4.2022, https://background.tagesspiegel.de/digitalisierung/europaeische-sprachmodelle-und-die-rolle-des-staates-im-innovationsoekosystem (11.5.2022)
- Pfitzner, B.; Steckhan, N.; Arnrich, B. (2021): Federated Learning in a Medical Context: A Systematic Literature Review. In: ACM Trans. Internet Technol. 21(2), S.1–31
- POST (Parliamentary Office of Science and Technology – UK Parliament (2020a): Edge computing. POSTNOTE Nr. 631, https://researchbriefings.files.parliament.uk/documents/POST-PN-0631/POST-PN-0631.pdf (11.5.2022)
- POST (2020b): Remote sensing and machine learning. POSTNOTE Nr. 628, https://researchbriefings.files.parliament.uk/documents/POST-PN-0628/POST-PN-0628.pdf (10.5.2022)
- Qiu, X.; Parcollet, T.; Beutel, D.; Topal, T.; Mathur, A.; Lane, N. (2020): Can Federated Learning Save The Planet? https://arxiv.org/pdf/2010.06537 (1.6.2022)
- Qiu, X.; Parcollet, T.; Fernandez-Marques, J.; de Gusmao, P.; Beutel, D.; Topal, T.; Mathur, A.; Lane, N. (2021): A first look into the carbon footprint of federated learning. https://arxiv.org/pdf/2102.07627 (1.6.2022)
- Rieke, N.; Hancox, J.; Li, W.; Milletarì, F.; Roth, H.; Albarqouni, S.; Bakas, S.; Galtier, M.; Landman, B.; Maier-Hein, K.; Ourselin, S. et al. (2020): The future of digital health with federated learning. In: NPJ digital medicine 3
- Russel, B. (2021): Google is using federated learning to improve Assistant's "Hey Google" accuracy. https://www.xda-developers.com/google-federated-learning-hey-google-accuracy/ (11.5.2022)
- Schallbruch, M.; Huth, M.; Lundbæk, L.-N.; Herdenau, C.; Attenberger, L. (2021): Künstliche Intelligenz für den öffentlichen Sektor: Masked Federated Learning als datenschutzfreundliche Lösung. Positionspapier. Xayn AG
- Strubell, E.; Ganesh, A.; McCallum, A. (2019): Energy and Policy Considerations for Deep Learning in NLP. https://arxiv.org/pdf/1906.02243 (1.6.2022)

- TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2015): Big Data in der Cloud. (Leimbach, T.; Bachlechner, D.) TA-Vorstudie, TAB-Hintergrundpapier Nr. 19, Berlin
- TAB (2019): Beyond Big Data (Autorin: Ehrenberg-Silies, S.). TAB-Themenkurzprofil Nr. 34, Berlin
- TAB (2020a): Autonome Waffensysteme (Autoren: Grünwald, R.; Kehl, C.). TAB-Arbeitsbericht Nr. 187, Berlin
- TAB (2020b): Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen – ein Überblick. (Autor/in: Kolleck, A.; Orwat, C.) Hintergrundpapier Nr. 24, Berlin
- TAB (2021a): Digitalisierung der Landwirtschaft: technologischer Stand und Perspektiven (Autoren: Kehl, C.; Meyer, R.; Steiger, S.). TAB-Arbeitsbericht Nr. 193, Berlin
- TAB (2021b): Digitalisierung der Landwirtschaft: gesellschaftliche Voraussetzungen, Rahmenbedingungen und Effekte (Autoren: Kehl, C.; Meyer, R.; Steiger, S.). TAB-Arbeitsbericht Nr. 194, Berlin
- TAB (2022): Sprich mit mir! Perspektiven für den Einsatz KI-basierter Dialogsysteme (Autor: Peters, R.). TAB-Themenkurzprofil Nr. 52, Berlin
- Tho, D. (2022): Real-world data. Data networks, standardization, and federated analysis. https://www.sentinelinitiative.org/sites/default/files/documents/Real-World%20Data%20Data%20networks%2C%20standardization%2C%20and%20federated%20analysis.pdf (11.5.2022)
- University of Pennsylvania (o.J.): The Federated Tumor Segmentation (FeTS) initiative. https://www.med.upenn.edu/cbica/fets/ (11.5.2022)
- Wiese, L.; Homann, D.; Waage, T.; Brenner, M. (2018): Homomorphe Verschlüsselung für Cloud-Datenbanken: Übersicht und Anforderungsanalyse. In: Sicherheit 2018, Lecture Notes in Informatics, Gesellschaft für Informatik, S. 222 – 234
- Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. (2019): Federated Machine Learning: Concept and Applications. In: ACM Transactions on Intelligent Systems and Technology 10(2), No. 12
- Yang, T.; Andrew, G.; Eichner, H.; Sun, H.; Li, W.; Kong, N.; Ramage, D.; Beaufays, F. (2018): Applied Federated Learning: Improving Google Keyboard Query Suggestions. https://arxiv.org/pdf/1812.02903 (1.6.2022)
- Zhou, J.; Zhang, S.; Lu, Q.; Dai, W.; Chen, M.; Liu, X.; Pirttikangas, S.; Shi, Y.; Zhang, W.; Herrera-Viedma, E. (2021): A Survey on Federated Learning and its Applications for Accelerating Industrial Internet of Things. https://arxiv.org/pdf/2104.10501 (1.6.2022)

Im Rahmen der Recherche zu diesem Beitrag wurden Interviews mit mehren Expert/innen durchgeführt. Die Autoren danken Franziska Bönisch, Ulrich Kelber, Ekaterina Korneeva, Anne Mareike Schlinkert und Katharina Zweig für die zur Verfügung gestellten Informationen und ihr Mitwirken an diesem Beitrag.

Das Horizon-Scanning ist Teil des methodischen Spektrums der Technikfolgenabschätzung im TAB.

Horizon SCANNING

Mittels Horizon-Scanning werden neue technologische Entwicklungen beobachtet und diese systematisch auf ihre Chancen und Risiken bewertet. So werden technologische, ökonomische, ökologische, soziale und politische Veränderungspotenziale möglichst früh erfasst und beschrieben. Ziel des Horizon-Scannings ist es, einen Beitrag zur forschungs- und innovationspolitischen Orientierung und Meinungsbildung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung zu leisten.

In der praktischen Umsetzung werden im Horizon-Scanning softwaregestützte Such- und Analyseschritte mit expert/innenbasierten Validierungs- und Bewertungsprozessen kombiniert.

Herausgeber: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)

Gestaltung und Redaktion: VDI/VDE Innovation + Technik GmbH

Bildnachweise: © bymuratdeniz/iStock (S.1); © NicoElNino/iStock (S.2, S.4); © ipopba/iStock (S.5); © marchmeena29/iStock (S.6); © PeopleImages/iStock (S.7)

ISSN-Internet: 2629-2874