Die Seite des SF | La page du FS

SF·FS

Etienne Liechti

Tech Law-Workshop: Federated Machine Learning

Federated Machine Learning erlaubt es, Erkenntnisse aus dezentral gehaltenen Datenbeständen zu gewinnen. Im Bereich der Life Sciences gibt es dafür zahlreiche potenzielle Anwendungsfelder, wie z.B. bei Rückenmarksverletzungen oder der Strahlentherapie. Eine interdisziplinäre Veranstaltung hat die Potenziale dieser Technologie aufgezeigt, dabei aber auch festgestellt, dass noch praktische und rechtliche Hürden bestehen.

Le Federated Machine Learning permet d'obtenir des informations à partir de bases de données décentralisées. Il existe de nombreux champs d'application potentiels dans le domaine des sciences de la vie, comme par exemple les lésions de la moelle épinière ou la radiothérapie. Une conférence interdisciplinaire a mis en évidence le potentiel de cette technologie, tout en constatant qu'il existe encore des obstacles pratiques et juridiques.

I. Einleitung

Der vom Zentrum für Life Sciences-Recht (ZLSR) und dem Schweizer Forum für Kommunikationsrecht (SF-FS) am 26. November 2024 in Zürich durchgeführte Tech Law-Workshop war dem Thema *Federated Machine Learning (FML)* gewidmet. Im Publikum fanden sich Vertreterinnen und Vertreter aus den Natur- und Rechtswissenschaften sowie aus der anwaltschaftlichen Praxis. Bei *FML* oder auch «föderiertem maschinellem Lernen» handelt es sich um eine Technologie, bei welcher Rechenoperationen dezentral in getrennten Datensätzen mit jeweils demselben Algorithmus durchgeführt und die berechneten Ergebnisse anschliessend an einen koordinierenden Server übermittelt werden.

Ziel des Workshops, erklärte Tagungsleiter Prof. Dr. Alfred Früh, Professor für Privatrecht an der Universität Basel, sei es, das Potenzial des Themas «föderiertes maschinelles Lernen» zu eruieren. Das bedeute, einerseits genauer zu verstehen, wie *FML* funktioniere und andererseits die Risiken und Chancen der Technologie benennen zu können. Hierfür werde das Thema aus verschiedenen Sichtweisen beleuchtet. Entsprechend stand im ersten Teil die naturwissenschaftliche Perspektive im Zentrum, mit praktischen Anwendungsfällen von *FML* aus dem Bereich der Biomedizin. Im zweiten Teil stand die rechtliche, insb. die datenschutzrechtliche und die kartellrechtliche Betrachtungsweise von *FML* im Vordergrund.

Etienne Liechti, MLaw, Universität Basel.

II. Erster Teil: Verwendung von FML in der Biomedizin

Den ersten Vortrag hielt Frau Prof. Dr. Catherine Jutzeler, Assistenzprofessorin für Biomedizinische Datenwissenschaft an der Fakultät für Gesundheitswissenschaften und Technologie der ETH Zürich zu ***Rückenmarksverletzungen***.

Verletzungen des Rückenmarks sind zwar selten, für die Betroffenen jedoch äusserst einschneidend. Mangels einheitlicher Behandlungsmöglichkeit ist dieses Forschungsgebiet von grosser Bedeutung. Jutzelers Ziel ist es, durch eine wirksamere Datenanalyse die Prognosen und Empfehlungen für die Behandlung von Rückenmarksverletzungen zu verbessern. Ein Problem dabei ist, dass die Therapie sehr unterschiedlich verlaufen kann. So kann bei einigen Patientinnen und Patienten im Verlaufe der Therapie gar keine Symptomverbesserung erzielt werden. Andere können bspw. ihre Hände wieder bewegen und Leichtverletzte können teilweise wieder vollständig gehen. Diese Variabilität des Krankheitsverlaufs sowie die niedrige Inzidenz der Krankheit führen zu einem erhöhten Bedarf an Daten bzw. an einer innovativen Nutzung der Daten. Hier kommt *FML* ins Spiel.

In ihrer Präsentation stellte Jutzeler *FML* als Alternative zur derzeitigen Datenverarbeitung dar, welche den Transfer von Daten durch mehrere Standorte voraussetzt. *FML* funktioniert ohne Datenweitergabe: In der Trainingsphase des *FML* trainieren Systeme an unterschiedlichen Standorten (z.B. in unterschiedlichen Spitälern) lokale Modelle mit lokalen Daten. Im nächsten Schritt, der Modellaktualisierung, senden die lokalen Systeme die Modelleinstellungen (Parameter) des lokal trainierten Modells an einen zentralen Server. Dieser berechnet gestützt auf die Modelleinstellungen der lokalen Modelle ein globales Mo-

dell (sog. Modellaggregation). Das aggregierte, globale Modell wird an die lokalen Systeme zurückgesendet. Diese verbessern wieder die lokalen Modelle basierend auf dem neuen, globalen Modell. Dieser Kreislauf wiederholt sich, sodass die Modelle mit der Zeit immer besser werden.

Der grosse Vorteil der *FML*-Technologie besteht darin, dass die Daten verschiedener Standorte gemeinsam genutzt werden können, dabei aber an «Ort und Stelle» bleiben. So werden die Modelleinstellungen der lokalen Modelle (Parameter) und die zugrunde liegenden Daten als solche geteilt. Damit stehe den Forscherinnen und Forschern ein Instrument zur Verfügung, welches die Zusammenarbeit unter Einhaltung der Datenschutzbestimmungen erlaube. Die Erkenntnisse aus der Anwendung von *FML* auf Rückenmarksverletzungen seien grundsätzlich auf andere seltene Krankheiten übertragbar.

In der konkreten Anwendung von *FML* zur Erforschung von Rückenmarksverletzungen sei die unterschiedliche Datenerhebung in den Spitälern ein Problem. Beispielsweise werde in einem Spital die Temperatur im Mund und in einem anderen Spital unter dem Arm gemessen. Diese Heterogenität in der Datenerhebung erschwere es dem zentralen Server, ein globales Modell zu entwickeln. Der nächste notwendige Schritt, um die Verwendung von *FML* zu ermöglichen liege daher in der Vereinheitlichung der Datenerhebung. So werde die Datenqualität homogenisiert.

Die zweite Präsentation hielt Dr. med. Dr. phil. Bram Stieltjes, Leiter von Personalized Health Basel (PHB), einer gemeinsamen Organisation der Universität Basel und der Universitätsspitäler der Region Basel, zum Einsatz von FML in der ***Strahlentherapie***.

Bei der Behandlung von Tumoren mittels Strahlentherapie muss eine Umrandung um den Tumor herum eingezeichnet werden, auf welche die Bestrahlung beschränkt wird. Diese Arbeit wird zurzeit noch von Strahlentherapeutinnen und -therapeuten vorgenommen. Das Ziel des Projekts ist es, zu ermöglichen, dass künftig die Umrandung mithilfe von *FML* eingezeichnet werden kann. Um den Algorithmus dahingehend zu trainieren, werden so viele homogene Daten wie möglich benötigt.

Wie Jutzeler kämpft auch Stieltjes mit der Heterogenität der zur Verfügung gestellten Daten. Zudem nimmt die Aufbereitung der Daten viel Zeit in Anspruch. Dabei werden die Daten zunächst von unterschiedlichen Formaten in das gleiche Format überführt. Um diese Aufgabe auszuführen, müssen die Forscherinnen und Forscher wissen, wie die Daten erhoben wurden.

Ein weiterer Grund für die Heterogenität der Daten sei, dass für die gleichen Erkrankungen teilweise unterschiedliche Behandlungen vorgesehen werden. So kann es sein, dass in einem Spital ein Medikament verabreicht wird, in einem anderen Spital in einer vergleichbaren Situation hingegen nicht. Dieses Problem kann sich sowohl beim Vergleich von Behandlungen in unterschiedlichen Spitälern als auch beim Vergleich der Behandlungen innerhalb desselben Spitals ergeben.

Erschwerend komme hinzu, dass die Qualität der Daten auch von Krankheit zu Krankheit unterschiedlich sei. So gebe es bei Rückenmarkerkrankungen ein Register, in das gewisse Daten eingetragen werden. Bei Untersuchungen im Zusammenhang bspw. mit einer Sepsis würden Daten dagegen ohne Register gesammelt. In der Tendenz seien dabei Registerdaten von besserer Qualität, da die Spitäler bei deren Erhebung einem Protokoll folgen.

Gemäss Stieltjes könnten diese Probleme gelöst werden, wenn auf der lokalen und der globalen Ebene die notwendige Infrastruktur zur Verfügung gestellt würde. Hiermit sind alle Komponenten gemeint, die den Austausch und das Training von Modellen zwischen den lokalen Geräten und dem zentralen Server unterstützen. Sie muss hinsichtlich der Übertragung von Informationen effizient, datenschutzrechtlich sicher und skalierbar sein. Hierbei sei es sinnvoll, dieses Bedürfnis zumindest national anzugehen und kantonale Alleingänge zu vermeiden. Unter den Anwesenden bestand darüber hinaus Einigkeit, dass Probleme wie die Datenaufarbeitung auch mittels intensiverer internationaler Zusammenarbeit angegangen werden sollten.

III. Zweiter Teil: Rechtliche Einordnung der Verwendung von FML

Noémi Ziegler, Rechtsanwältin, mit dem Tätigkeitsschwerpunkt Datenschutz-, Informations- und Technologierecht, präsentierte eine ***datenschutzrechtliche Einordnung*** von *FML*.

Dabei sei es entscheidend, welche Phase des Ablaufs von *FML* betrachtet werde. Ziegler führte aus, dass von Datenspenderinnen und -spendern erhobene Personendaten auf lokaler Ebene gespeichert werden. Auf dieser Ebene finde auch das Training lokaler Modelle mit den erhobenen Personendaten statt. Die Modelleinstellungen (Parameter) dieser Modelle würden dann an den zentralen Server auf der nächsten Ebene (globale Ebene) weitergegeben (Modellaktualisierung). Gestützt auf die lokalen Modelleinstellungen werde auf dieser Ebene das aggregierte, globale Modell erstellt, welches auf die lokale Ebene zurückgesendet werde.

Bemerkenswert an diesem Prozess sei, dass keine Datenweitergabe *(data sharing)* stattfinde: Die Personendaten blieben stets auf der lokalen Ebene. Lediglich die Datenparameter, also die Modelleinstellungen des lokalen Modells, würden weitergegeben. Auf der globalen Ebene finde zudem keine Datenerhebung, -bearbeitung oder -speicherung statt. Dies habe zur Konsequenz, dass die Datenbearbeitungsgrundsätze des Datenschutzgesetzes (DSG), namentlich der Grundsatz der Transparenz und der Grundsatz der Zweckbindung, nur auf der lokalen Ebene eingehalten werden müssen. Der Grundsatz der Transparenz besagt, dass Datenspenderinnen und -spender über die Datenbearbeitung, insbesondere die Weitergabe oder Weiterverarbeitung ihrer Daten, informiert werden müssen. Aus dem Grundsatz der Zweckbindung ergibt sich, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der den Datenspenderinnen und -spendern bekannt ist.

Unklar ist gemäss Ziegler indes noch, ob es auf der globalen Ebene nicht doch zu Situationen kommen kann, in denen über die erhaltenen Informationen Rückschlüsse auf eine bestimmte Person gezogen werden können. Dies würde bedeuten, dass die datenschutzrechtlichen Grundsätze nicht nur auf der lokalen Ebene eingehalten werden müssten. Ein geringes Restrisiko, dass gewisse Informationen, die Rückschlüsse auf Personen erlauben könnten, auf die globale Ebene gelangen, könne nicht vollkommen ausgeschlossen werden.

Neben anderen Punkten wurde besonders dieser Aspekt im Anschluss an das Referat unter den Anwesenden diskutiert. Hervorgehoben wurde, dass das Risiko von Verstössen gegen das Datenschutzrecht auf der globalen Ebene normativ begrenzt werden könnte. Dies liesse sich erreichen, wenn die Daten auf der globalen Ebene (mangels Erhebung oder Bearbeitung zu einem personenbezogenen Zweck) gar nicht als Personendaten gelten könnten. Ausserdem wurde argumentiert, der Zweck sei nicht personenbezogen, weil durch die Verwendung von *FML* nicht primär den Datenspenderinnen und -spendern, sondern künftigen Patientinnen und Patienten geholfen werde.

IV. Kartellrechtliche Überlegungen zu FML

Zum Schluss befasste sich Fabian Martens, Rechtsanwalt mit Schwerpunkt im Wettbewerbs- und Immaterialgüterrecht, mit der ***kartellrechtlichen Einordnung*** von *FML*.

Kartellrechtlich sei es denkbar, dass die Anwendung von *FML* zu einer marktbeherrschenden Stellung führe. Marktbeherrschung liege vor, wenn einzelne oder mehrere Unternehmen auf einem Markt als Anbieter oder Nachfrager in der Lage seien, sich von anderen Marktteilnehmern (Mitbewerbern, Anbietern oder Nachfragern) in wesentlichem Umfang unabhängig zu verhalten.

Laut Martens ist der durch die Anwendung des aggregierten Modells auf der lokalen Ebene entstehende Algorithmus das «Produkt» von *FML*, welches auf dem Markt angeboten wird. Der Preis ergebe sich aus den Inputdaten, die auf der lokalen Ebene einfliessen. Diese hätten einen finanziellen Wert, der kompensiert werden müsse. Je genauer der Algorithmus die Realität abbilde, desto werthaltiger sei er. Kriterien, die zur Beurteilung der Marktbeherrschung in einem konkreten Fall etwa beigezogen werden könnten, sind der Umsatz, die Anzahl Benutzer, die Anzahl Berechnungen sowie der Umfang bzw. die Qualität der Inputdaten. Bedient nur ein einziger Algorithmus einen Markt, hat das dahinterstehende Unternehmen eine marktbeherrschende Stellung inne. Zu einem Kartellrechtsverstoss komme es aber nur bei einem Missbrauch dieser Stellung, z.B. durch die Verweigerung von Geschäftsbeziehungen ohne sachliche Rechtfertigung.

Eine Frage, die sich aus kartellrechtlicher Perspektive ebenfalls stellt, ist, ob ein durch *FML* entwickelter Algorithmus eine Wettbewerbsabrede darstellt. Die Technologie bedingt es, gewisse Abreden zu treffen. Dies betrifft u.a. den Einbezug oder Nichteinbezug bestimmter Daten. Ein Anbieter könne durchaus ein Interesse daran haben, dass gewisse Daten ausgewertet werden und andere nicht. So könnten bspw. in einem Spital alle Operationen, die die Situation einer zu behandelnden Person nicht verschlechtert haben als Heilungserfolg bezeichnet werden. Dann wäre die Erfolgsquote höher, als wenn nur die Operationen als Erfolg gewertet werden, bei denen sich die Situation tatsächlich verbessert hat. Wenn bezüglich des Einbezugs bzw. Nichteinbezugs von Daten eine Vereinbarung getroffen wird, handelt es sich um eine Abrede.

Gemäss Martens könnte diese Form der Wettbewerbsabrede aber aus im Kartellgesetz genannten Gründen gerechtfertigt sein. Abreden sind gerechtfertigt, wenn sie zur Erhöhung der wirtschaftlichen Effizienz führen, notwendig sind, um die Produkte oder Produktionsverfahren zu verbessern oder um die Forschung oder Verbreitung von technischem oder beruflichem Wissen zu fördern.

Konkret könne eine Abrede im Rahmen von *FML* gerechtfertigt sein, wenn die Qualität eines Algorithmus aufgrund der umfangreicheren Datenlage verbessert würde. Dennoch darf auch in diesen Fällen der Wettbewerb nicht vollständig beseitigt werden.

V. Fazit

Insgesamt zeigte die Veranstaltung anhand praktischer Anwendungsbeispiele von *FML* im Gesundheitsbereich das Potenzial der Technologie. Die Hürden, die einer Verbreitung von *FML* im Weg stehen, scheinen vor allem praktischer Natur zu sein. Besonders die mangelhafte Datenqualität und die Heterogenität der zur Verfügung gestellten Daten verhindern rasche Erfolge. Diese Schwierigkeiten könnten durch die Verbesserung der Infrastruktur auf den verschiedenen Ebenen gelöst werden.

Aus rechtlicher Sicht bietet die Technologie Vorteile, weil das Datenschutzrecht – eine entsprechende Auslegung vorausgesetzt – auf der Stufe des aggregierten Modells nicht zur Anwendung kommt. Schliesslich gilt es, bei der Anwendung von *FML* kartellrechtliche Aspekte zu beachten, wobei sich im Falle von Abreden ein erheblicher Spielraum für die Rechtfertigung öffnet.

Ob *FML* auch zum willkommenen Effekt führen könnte, dass Unternehmen und Organisationen bereit sind, ihre Daten zum Zweck kooperativer Forschung zur Verfügung zu stellen, lässt sich aus heutiger Sicht noch nicht abschätzen. Dafür scheinen die praktischen Hürden noch zu hoch zu sein.