NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

DFN infobrief recht

2 / 2023
Februar 2023

Datenschutz auf Rezept

DSK veröffentlicht Hinweise zur datenschutzkonformen Forschung mit Gesundheitsdaten

Auf die Schremse treten?

EU-Kommission entwirft Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA

Musk? Oh no! Mastodon!

Immer mehr öffentliche Stellen nutzen Mastodon statt Twitter

Kurzbeitrag: Google brings light into the dark (pattern)

Google hat seine Cookie-Banner angepasst

Datenschutz auf Rezept

DSK veröffentlicht Hinweise zur datenschutzkonformen Forschung mit Gesundheitsdaten

von Johannes Müller

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung veröffentlicht.[1] Hierbei hat sie konkrete Empfehlungen gegeben, die bei der Verarbeitung von Gesundheitsdaten zu Forschungszwecken zu beachten sind und nannte weitere Hinweise zur Erfüllung der gesetzlichen Anforderungen aus der Datenschutzgrundverordnung (DSGVO).

I. Der datenschutzrechtliche Schutz von Gesundheitsdaten für Forschungszwecke

Die DSGVO regelt die Anforderungen an den Schutz von personenbezogenen Daten im Rahmen einer Datenverarbeitung. Hierbei werden besondere Datenkategorien als besonders sensibel und daher schützenswert erachtet. Für deren Verarbeitung gelten folglich höhere Anforderungen. Eine dieser Kategorien stellt auch diejenige der Gesundheitsdaten dar.[2] Diese werden in Art. 4 Nr. 15 DSGVO als personenbezogene Daten definiert, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die höheren Anforderungen, die für die Verarbeitung von Gesundheitsdaten gelten sollen, werden in Art. 9 DSGVO zum Ausdruck gebracht. Gemäß Art. 9 Abs. 1 DGVO ist eine Datenverarbeitung von Gesundheitsdaten grundsätzlich verboten. Ausnahmsweise soll eine Datenverarbeitung erlaubt sein, sofern eine der in Art. 9 Abs. 2 DSGVO normierten Ausnahmen vorliegt. Diese sind strenger als die Voraussetzungen, die gemäß Art. 6 DSGVO für die generelle Verarbeitung von personenbezogenen Daten gelten sollen. Art. 9 DSGVO erlaubt etwa die Verarbeitung von Gesundheitsdaten, sofern eine ausdrückliche Einwilligung von der betroffenen Person erteilt wurde (Art. 9 Abs. 2 lit. a DSGVO) oder sofern die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person durchgeführt wurde (Art. 9 Abs. 2 lit. c DSGVO).

II. Privilegierung von Datenverarbeitungen zu Forschungszwecken

Erfolgt die Datenverarbeitung zu wissenschaftlichen Zwecken ist darüber hinaus jedoch auch zu beachten, dass die DSGVO solche Verarbeitungen grundsätzlich privilegiert. Die grundsätzliche Besserstellung von Datenverarbeitungen zu Forschungszwecken bringt die DSGVO an verschiedenen Stellen zum Ausdruck. Gemäß Art. 14 Abs. 5 lit. b DSGVO kann etwa unter anderem für Forschungsarbeiten die Informationspflicht bezüglich der betroffenen Person bei Datenverarbeitungen entfallen. Auch sieht Art. 89 Abs. 2 DSGVO eine Öffnungsklausel vor, die es den Mitgliedstaaten erlaubt, die datenschutzrechtlichen Betroffenenrechte einzuschränken, sofern durch diese die Forschung ernsthaft beeinträchtigt wird. Sofern bei der datenschutzrechtlichen Bewertung einer Datenverarbeitung keine konkrete Privilegierung aus der DSGVO greift, kann im Rahmen einer Interessensabwägung dennoch zu beachten sein, dass Datenverarbeitungen zu Forschungszwecken durch die DSGVO grundsätzlich privilegiert

1 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/104DSK-Petersberger-Erklaerung.pdf;jsessionid=767CAA5A244C12FBAF2D09268FC67D1F.intranet241?__blob=publicationFile&v=1 (zuletzt abgerufen am 18.01.2023).

2 Vgl. hierzu Mc Grath, Zu Risiken und Nebenwirkungen fragen Sie Ihren Arzt oder Verantwortlichen, DFN-Infobrief Recht 04/2020.

werden und daher im konkreten Fall das Interesse des wissenschaftlichen Datenverarbeiters besonders schwer wiegt.

III. Die Empfehlungen der DSK

Dieser gegensätzlichen Gesichtspunkte, die im Rahmen der Forschung mit Gesundheitsdaten zu beachten sind, war sich die DSK bei der Formulierung der Petersberger Erklärung bewusst. So weist sie einerseits einleitend darauf hin, dass die Forschung einen hohen medizinischen Erkenntnisgewinn bringen könne, der im Interesse der Allgemeinheit liege. Andererseits erkennt sie auch, dass die DSGVO Gesundheitsdaten als besonders sensibel erachtet. Die Empfehlungen der DSK können daher dabei helfen, im konkreten Fall die Interessen in Einklang miteinander zu bringen.

Hierzu formuliert die DSK sieben Empfehlungen zur Verarbeitung von Gesundheitsdaten in der Forschung. Diese Empfehlungen werden durch anschließende Erläuterungen ergänzt. Teilweise weisen diese Empfehlungen Elemente grundlegender Natur auf. So weist Empfehlung 1 darauf hin, dass die Menschen im Mittelpunkt der Datenverarbeitung stehen und nicht zum bloßen Gegenstand der Forschung gemacht werden sollen. Hierzu soll die betroffene Person auch über den rechtlichen Rahmen hinaus in die Verarbeitung eingebunden werden. Die Einbindung könne durch digitale Managementsysteme erfolgen. In den weiteren Ausführungen weist die DSK darauf hin, dass es betroffenen Personen grundsätzlich möglich sein muss, der Datenverarbeitung voraussetzungslos zu widersprechen. Allgemeine Natur hat auch die zweite Empfehlung Sie gibt den Grundsatz wieder, dass Daten umso umfangreicher genutzt werden können, je höher der Schutz durch geeignete Garantien und Maßnahmen ist. Die dritte Empfehlung nennt als solche konkreten Maßnahmen: die Verschlüsselung, Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung. Anonyme Datensätze könnten umfassend durch die Forschung genutzt werden.[3] Mit dieser Empfehlung gibt die DSK lediglich Anforderungen wieder, die sich bereits unmittelbar aus Art. 32 DSGVO ergeben. In den weiteren Erläuterungen konkretisiert die DSK noch die Angaben zur Anonymisierung: Könne der Zweck der Forschung auch mit anonymisierten Daten erreicht werden, so dürfen lediglich solche genutzt werden.

Die vierte Empfehlung beschäftigt sich mit Datenverarbeitungen, bei denen die Datensätze aus unterschiedlichen Quellen stammen und beim Datenverarbeiter verknüpft werden. Durch eine Verknüpfung der Daten sei es einfacher möglich, die betroffene Person zu identifizieren. Nach Einschätzung der DSK liege deshalb ein besonders schwerwiegender Eingriff in die Rechte der betroffenen Person vor, sodass höhere Schutzanforderungen gelten sollen. Durch geeignete Verfahren gilt es sicherzustellen, dass betroffenen Personen der Zugang zu ihren Daten gewährt wird. Durch die Einrichtung besonderer Verfahren müsse garantiert werden, dass die Zusammenführung nur anlassbezogen und temporär erfolge. Durch ein Einwilligungsmanagementsystem erhalten betroffene Personen die Möglichkeit, bei Kenntnis der Risiken der Zusammenführung aktiv zuzustimmen. Besonders konkret ist die Petersberger Erklärung in ihrer fünften Empfehlung. In dieser fordert sie die Einrichtung eines zentralen Registerverzeichnisses durch die Verantwortlichen.[4] Diese sollen hierfür auch verbindliche Qualitätsanforderungen vorgeben. Durch ein solches sollen mehrfache Datensammlungen vermieden werden, auch wenn die Gesundheitsdaten in verschiedenen Registern gespeichert sind. Hierdurch soll auch die Datensammlung transparenter gestaltet sein. Parallel zum Registerverzeichnis wird auch die Schaffung einer zentralen koordinierenden Stelle gefordert. Diese soll Anträge (durch Dritte) zur Nutzung der Gesundheitsdaten veröffentlichen und die Nutzenden dazu verpflichten, die Forschungsergebnisse in anonymer Form zu veröffentlichen. Die letzten beiden Empfehlungen richten sich nicht an Datenverarbeiter selbst. In der 6. Empfehlung regt die DSK eine gesetzliche Regelung des Forschungsgeheimnisses an, durch das der Umgang mit Forschungsdaten auch aus strafrechtlicher und prozessualer Sicht klargestellt werden soll. Die siebte Empfehlung befasst

3 Vgl. hierzu Haserück/Kurz, Gesundheitsdaten: Wie man datenschutzkonform und effektiv forschen kann, Deutsches Ärzteblatt 48/2022, abrufbar unter https://www.aerzteblatt.de/archiv/228698/Gesundheitsdaten-Wie-man-datenschutzkonform-und-effektiv-forschen-kann (zuletzt abgerufen am 18.01.2023).

4 Das Führen von medizinischen Registerverzeichnissen ist bereits üblich, so existiert etwa das Deutsche Register Klinischer Studien als anerkanntes Primärregister für die Registrierung von in Deutschland durchgeführten patientenorientierten klinischen Studien. Auch betreibt das RKI beispielsweise ein Zentrum für Krebsregisterdaten, in dem die anonymisierten Daten der Landeskrebsregister auf Bundesebene zusammengeführt werden; vgl. zur datenschutzkonformen Verarbeitung von Gesundheitsdaten durch ein Krebsregister auch das Urteil des VG Hamburg vom 28.7.2022 (AZ 21 K 1802/21).

sich mit der Kontrolle durch die Datenschutzbehörden. Diese sollten standardisierte Anforderungen, insbesondere an die Dokumentation der Verarbeitungsprozesse festlegen.

IV. Relevanz für Hochschulen

Da sich die Erklärung des DSK unmittelbar mit Datenverarbeitungen zu Forschungszwecken beschäftigt, weist sie eine hohe Relevanz für Hochschulen und andere wissenschaftliche Einrichtungen auf, die Gesundheitsdaten verarbeiten. Im Rahmen der aufgezeigten gegensätzlichen Interessenlage kann die Petersberger Erklärung die datenschutzrechtliche Bewertung der Forschung von Gesundheitsdaten erleichtern. Die Erklärung weist keine verbindliche Natur auf. Da die DSK sich aber aus allen Datenschutzbeauftragten der Länder und dem Bundesdatenschutzbeauftragten zusammensetzt, kommt der Erklärung ein hohes Gewicht zu. Besondere Hilfestellung gibt die Erklärung, sofern sie konkrete Hinweise gibt, die nicht lediglich eine Wiedergabe gesetzlich normierter Pflichten darstellen. Insbesondere sind die Ausführungen zu erhöhten Schutzanforderungen bei der Verknüpfung unterschiedlicher Datensätze zu beachten. Hohe Relevanz weist auch die Forderung auf, ein zentrales Registerverzeichnis zu schaffen, um Datennutzung transparent zu gestalten und mehrfache Datensammlungen zu verhindern. Konkret in der Praxis lässt sich auch die Forderung umsetzen, eine zentrale Stelle für Datennutzungsanträge zu schaffen.

Auf die Schremse treten?

EU-Kommission entwirft Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA

von Klaus Palenberg

Nach der Vereinbarung über den Datenschutzrahmen EU-USA zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, haben die USA zwischenzeitlich Regelungen erlassen, diesen umzusetzen. Nun hat die Europäische Kommission erklärt, sie halte die US-Regelungen für ausreichend. Die Vereinigten Staaten gewährleisteten damit ein angemessenes Datenschutzniveau. Zugleich veröffentlichte die Europäische Kommission einen Entwurf für die Entscheidung eines Angemessenheitsbeschlusses. Ob mit dieser Entscheidung nun endlich Rechtssicherheit bei der Übermittlung von Daten in die Vereinigten Staaten eintritt, versucht dieser Beitrag zu beleuchten. Dabei soll auch auf Details der Regelungen und der Kritik hieran eingegangen werden.

I. Der Hintergrund

Die europäische Datenschutz-Grundverordnung (DSGVO) fordert bei einer Datenübertragung in einen Staat, der nicht im Geltungsbereich der DSGVO liegt (Drittstaat), gewisse Garantien, dass auch dort ein dem europäischen Datenschutzrecht vergleichbarer Schutz gewährleistet wird. Zu diesem Zweck sieht sie beispielsweise in Art. 45 DSGVO einen sogenannten Angemessenheitsbeschluss durch die Kommission vor. Mit einem solchen stellt diese dann fest, dass in dem betreffenden Drittstaat ein angemessenes Schutzniveau für personenbezogene Daten europäischer Bürger:innen besteht. Von dieser Möglichkeit – eine entsprechende Regelung sah bereits die RL 95/46/EG (Datenschutzrichtlinie) vor - hatte die Kommission auf Grundlage von Abkommen mit den Vereinigten Staaten Gebrauch gemacht. Den Safe-Harbour-Beschluss (Entscheidung 2000/520/EG) aus dem Jahre 2000 erklärte der Europäische Gerichtshof (EuGH, Urteil vom 06.10.2015 – C-362/14) jedoch mit der Schrems-I-Entscheidung[1] für ungültig. Ebenso erging es dem Nachfolge-Beschluss aus dem Jahre 2016 (Durchführungsbeschluss (EU) 2016/1250), dem EU-US Privacy Shield, durch das Schrems-II-Urteil[2] (EuGH, Urteil vom 16.07.2020 – C-311/18). Auch dessen Vorgaben erfüllten nicht die europarechtlichen Anforderungen.

Seitdem liegt kein gültiger Angemessenheitsbeschluss für eine Datenübermittlung in die USA vor.
Eine solche ist daher derzeit in der Regel auf Standardvertragsklauseln[3] zu stützen. Angesichts der damit einhergehenden tatsächlichen und rechtlichen Unsicherheiten, haben die EU und die USA im März 2022 einen dritten Versuch unternommen und einen neuen Transatlantischen Datenschutzrahmen (inzwischen heißt er Datenschutzrahmen EU-USA) auf den Weg gebracht.[4]

Die USA haben daraufhin per Durchführungsverordnung durch den Präsidenten (Executive Order on Enhancing Safeguards for

1 Siehe hierzu Sydow, Kein sicherer Hafen für die Daten?, DFN-Infobrief Recht 12/2015.

2 Siehe hierzu Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 08/2020.

3 Siehe hierzu Wellmann, O ihr gnadenbringende Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

4 Für weitere Informationen siehe Mc Grath, Ausgeschremst?, DFN-Infobrief Recht 05/2022.

United States Signals Intelligence Activities vom 07.10.2022)[5] und durch Verordnungen des US-Generalanwalts einige Regelungen geschaffen, mit denen die Anforderungen an das Datenschutzniveau, wie es der EuGH gefordert hat, erfüllt werden sollen. Allerdings sind eine Executive Order des Präsidenten und Verordnungen des Generalanwalts zunächst einmal lediglich interne Verwaltungsanweisungen und keine förmlichen Gesetze.

II. Die Entscheidung

Nun hat die EU-Kommission die US-amerikanischen Regelungen geprüft. Dabei ist sie zu dem Schluss gekommen, dass diese ausreichende Gewähr dafür leisten, dass die Daten europäischer Bürger:innen angemessen geschützt sind. Sie stützt diese Einschätzung auf die mit dem Datenschutzrahmen verbundenen Anforderungen und Garantien.

Möchten sich US-Unternehmen in dem Rahmen bewegen und ihre Datenverarbeitung auf den Angemessenheitsbeschluss stützen, müssen sie sich dazu verpflichten, detaillierte Datenschutzpflichten einzuhalten. Dies umfasst zum einen umfassende Löschpflichten, wenn die Daten für den Zweck, für den sie ursprünglich erhoben wurden, nicht mehr gebraucht werden. Zum anderen bestehen Beschränkungen und Garantien bei der Datenweitergabe an Dritte. Auch in diesem Falle sind die Daten weiterhin zu schützen. Zudem werden verschiedene Rechtsbehelfe gegen eine unbefugte Datenverarbeitung eingeführt, wie beispielsweise unentgeltliche Streitbeilegungsverfahren oder auch eine Schiedsstelle.

Auch US-Behörden sollen Beschränkungen und Garantien beim Datenzugang unterliegen. Der Zugang von Sicherheitsbehörden soll auf das notwendige und verhältnismäßige Maß zum Schutz der nationalen Sicherheit beschränkt sein. Für EU-Bürger:innen soll ein unabhängiges und unparteiisches Rechtsbehelfsverfahren eingerichtet werden. Zu diesem Zweck soll auch ein neues Gericht zur Datenschutzprüfung geschaffen werden. Dadurch soll Beschwerden mittels verbindlicher Anordnungen Abhilfe geleistet werden.
Für europäische Unternehmen soll dieser Schutz auch dann bei der Datenübermittlung in die USA gelten, wenn diese sich auf andere Grundlagen, wie etwa Standardvertragsklauseln stützt.

III. Weiterer Verlauf

Auf Grundlage dieser Einschätzung hat die EU-Kommission am 13.12.2022 das Verfahren zur Annahme eines Angemessenheitsbeschlusses für den Datenschutzrahmen EU-USA eingeleitet. Als nächstes wurde dieser Entwurf dann dem Europäischen Datenschutzausschuss (EDSA) zur Prüfung übermittelt. Danach erfolgt die Einholung der Zustimmung eines Ausschusses von Vertretern der Mitgliedstaaten und der Kontrolle durch das Europäische Parlament. Abschließend soll die Kommission den Angemessenheitsbeschluss endgültig annehmen.

Allerdings ist noch nicht klar, wie schnell diese nächsten Etappen abgeschlossen sein werden. Die US-Seite hat ihren Sicherheitsbehörden nämlich beispielsweise gewisse Übergangsfristen eingeräumt. Inwieweit der Angemessenheitsbeschluss vor deren Ablauf in Kraft treten wird, ist fraglich.

Nach Inkrafttreten soll die Wirksamkeit des Datenschutzrahmens regelmäßig durch die Europäische Kommission, die europäischen Datenschutzbehörden und US-Behörden evaluiert werden, um deren Umsetzung und Auswirkungen auf die Praxis festzustellen.

IV. Ausblick

Auch wenn dieser Datenschutzrahmen und insbesondere die Regelungen in den Vereinigten Staaten in die richtige Richtung zeigen, bleibt mit Spannung abzuwarten, wie lange er dieses Mal Bestand haben wird. Deutsche Datenschützer:innen und insbesondere der Kläger gegen die vorherigen Regelungen, Max Schrems mit seiner Organisation NOYB - Europäisches Zentrum für digitale Rechte, haben bereits ihre Bedenken geäußert.[6] Unklar ist zum Beispiel das Verhältnis zum Cloud Act, der den US-amerikanischen Sicherheitsbehörden umfangreiche Zugriffsmöglichkeiten auf Daten auch von Nicht-Amerikanern gewährt. Dazu zählen auch Befugnisse, US-amerikanische Unternehmen

5 Abrufbar unter: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (zuletzt abgerufen am 11.01.2022).

6 Hierzu bereits Mc Grath, Ausgeschremst?, DFN-Infobrief Recht 05/2022.

zu verpflichten, auch solche Daten zu offenbaren, die gar nicht auf Servern in den USA liegen.[7] Zudem bemängelte der EuGH in seinen Entscheidungen die US-amerikanische Praxis der anlasslosen Überwachung, der durch die US-Regelungen lediglich mit Rechtsbehelfsmöglichkeiten in den USA begegnet wurde.

Daher erscheint es nicht als unwahrscheinlich, dass sich der EuGH auch mit diesem transatlantischen Datenschutzrahmen befassen wird. Erst dann werden wir erfahren, ob die angekündigten Garantien und Schutzmechanismen tatsächlich ausreichen, um das vom europäischen Datenschutzrecht geforderte Schutzniveau zu erfüllen.

Bis dahin bleibt es wohl leider weiterhin bei der bisherigen Rechtsunsicherheit bei der Übermittlung von personenbezogenen Daten in die USA. Angesichts der aktuellen Übermacht der US-amerikanischen Anbieter von Softwarelösungen beispielsweise für Hochschulen, bei der oftmals auch eine Datenübermittlung an diese erfolgt, wäre eine sichere Rechtsgrundlage jedoch dringend vonnöten. Bis tatsächlich irgendwann Rechtssicherheit eingetreten ist, bleibt es bei dem Rat, die Datenübermittlung insbesondere in die Vereinigten Staaten weiterhin auf ein absolutes Minimum zu beschränken.

Darüber hinaus besteht auch bei der Übermittlung in andere Drittstaaten, wie etwa dem Vereinigten Königreich nach dessen EU-Austritt[8], der Bedarf an Rechtssicherheit. In dieser Hinsicht sollen die Abkommen mit den USA stets auch Vorbildcharakter für weitere Abkommen haben. Solange jedoch deren Wirksamkeit unsicher ist, können sie diesem Auftrag natürlich nicht gerecht werden.

7 Zu diesem Problemkreis siehe auch John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 02/2022.

8 Zu Regelungen auf britischer Seite siehe auch John, Kleingedrucktes ganz groß: Klauseln für Klauseln, DFN-Infobrief Recht 07/2022.

Musk? Oh no! Mastodon!

Immer mehr öffentliche Stellen nutzen Mastodon statt Twitter

von Justin Rennert

Nach der Übernahme von Twitter durch Elon Musk wechseln immer mehr Nutzer auf die dezentrale Alternative Mastodon. Auch einige öffentliche Stellen betreiben inzwischen eine Mastodon-Instanz. Wir geben einen Überblick über die Funktionsweise von Mastodon und zeigen auf, welche Hochschulen bereits auf Mastodon aktiv sind.

I. Grundfunktionen von Mastodon

Seit Elon Musk Twitter im Oktober 2022 übernommen hat, findet ein Exodus aus der Plattform statt. Zahlreiche Nutzer wandern zu anderen sozialen Netzwerken ab, weil sie nicht einverstanden sind mit Musks Machtfülle und seinem willkürlichen Umgang mit bestimmten Inhalten. So sperrte Twitter nach der Übernahme die Konten mehrerer bekannter US-Journalisten manuell. Sven Giegold, Staatssekretär im Bundeswirtschaftsministerium, reagierte in einem Brief an die EU-Kommission: Mit großer Sorge habe er Twitters neue Plattformregelungen sowie deren abrupte Änderungen und willkürliche Anwendung zur Kenntnis genommen.

Am Himmel der Twitter-Alternativen leuchtet derzeit wohl kein Stern so hell wie das Netzwerk Mastodon. Hierbei handelt es sich um ein dezentrales soziales Netzwerk. Doch was bedeutet überhaupt „dezentral“ und was leistet Mastodon im Vergleich zu anderen sozialen Netzwerken? Und welche Chancen liegen darin für öffentliche Stellen, insbesondere für Hochschulen? Diese Fragen möchten wir im vorliegenden Beitrag beantworten. Doch, first things first: ein kurzer Überblick über die Grundfunktionen von Mastodon:

Auf Mastodon können Nutzer:innen ähnlich wie bei Twitter öffentliche Posts absetzen. Die Posts heißen dort nicht „Tweets“, sondern „Tröts“ (englisch: „Toots“). Die Zeichenlänge für solche Tröts ist auf 500 Zeichen begrenzt; das ist zwar mehr als bei Twitter, zeigt aber: Auch bei Mastodon geht es um Kurznachrichten, um Microblogging. Nutzer:innen bekommen die Tröts solcher Mitnutzer:innen angezeigt, denen sie gefolgt sind. Die Anzeige erfolgt dabei streng chronologisch. Anders als bei den allermeisten Social-Media-Plattformen findet also keine Priorisierung gewisser Inhalte durch Algorithmen statt. Nutzer:innen bekommen in ihrer Timeline schlichtweg die Inhalte zuerst angezeigt, die andere zuletzt gepostet haben. Die Entwickler von Mastodon möchten Nutzer:innen dadurch die Kontrolle über ihre Timeline zurückgeben und für mehr Transparenz sorgen – wie genau die Algorithmen großer Online-Plattformen funktionieren, ist mittlerweile wohl nicht einmal den Plattformbetreibern selbst mehr genau bekannt.

II. Dezentralität und die Bedeutung der Heimatinstanz

So weit, so gut. Die Grundfunktionen von Mastodon sollten noch keinen Internetnutzer vom Hocker hauen. Nun zu dem ominösen Begriff der „Dezentralität“. Dezentralität bedeutet, dass theoretisch jeder einen eigenen Mastodon-Server betreiben kann. Es gibt also nicht den einen Mastodon-Server und die eine Webseite, auf der das Netzwerk erreichbar ist. Vielmehr kann jedermann einen eigenen Mastodon-Server betreiben und so seine eigene Version des sozialen Netzwerks hosten. Der Mastodon-Entwickler selbst nennt diese Versionen „Instanzen“. Derzeit existieren ca. 3.900 solcher Instanzen. Um eine Instanz zu betreiben, sind zwei Dinge notwendig: der Quellcode von Mastodon sowie ein Server, auf den man den Quellcode laden kann, damit die Instanz für andere über den Browser abrufbar ist. Dezentralität ist also nur dann möglich, wenn der Quellcode für jedermann frei

zugänglich ist. Mastodon ist deshalb ein Open-Source-Projekt. Der aktuelle Quellcode ist beispielsweise abrufbar auf Github.[1] Den Quellcode entwickelt hat die in Berlin ansässige Mastodon gGmbH, die im Jahr 2016 von Eugen Rochko gegründet wurde. Für den Betreiber einer Mastodon-Instanz fallen Kosten an: Die wichtigsten Kostenpunkte sind die Kosten für den Server sowie die Kosten für Moderator:innen. Die meisten Mastodon-Instanzen werden derzeit von Privatpersonen betrieben, die die Kosten über Spenden der Nutzer:innen refinanzieren.

Bedeutet das nun, dass derzeit ca. 3.900 soziale Netzwerke vollkommen unabhängig voneinander koexistieren? Nein, denn ein weiteres wichtiges Funktionsprinzip von Mastodon ist die Interoperabilität. Das bedeutet folgendes: Zwar müssen sich Nutzer:innen bei der Accounterstellung zunächst für eine Instanz entscheiden (dies wird dann ihre sog. „Heimatinstanz"), jedoch ist es ihnen ohne weiteres möglich, mit Nutzern anderer Instanzen zu interagieren. Das bedeutet: Sie sehen die Posts auf anderen Instanzen und können auf diese antworten oder sie an die eigenen Follower weitergeben (statt „retweet" heißt das bei Mastodon „boosten").

Die Wahl der Heimatinstanz hat daher zunächst eine ideelle Komponente. Anderen Nutzer:innen wird stets angezeigt, auf welcher Heimatinstanz das Gegenüber unterwegs ist. Die Heimatinstanz dient auch der Identifikation mit anderen Nutzer:innen auf der Instanz und kann die Zugehörigkeit zu einer Gruppe anzeigen. So finden sich zum Beispiel auf der Instanz „ruhr.social" viele Bewohner:innen des Ruhrgebiets, geschichtsinteressierte Personen finden womöglich auf der Instanz „historians.social" ihr Zuhause.

Doch die Wahl der Heimatinstanz hat auch harte technische Folgen. Denn der Instanzenbetreiber und die von ihm ausgewählten Moderator:innen können die Instanzen beliebig moderieren. Sie können einzelne Posts als sensibel markieren, Nutzeraccounts einfrieren oder gleich ganz blockieren. Zudem können sie die eigene Instanz abschirmen von Inhalten bestimmter externer Webseiten und anderer Mastodon-Instanzen. Das hat zur Folge, dass Nutzer:innen von Instanz A Inhalte der Nutzer:innen von Instanz B nicht mehr angezeigt werden. Der Instanzenbetreiber hat also weitreichende Kompetenzen, weswegen die Wahl der Instanz gut überlegt sein sollte. Die Moderation erfolgt zwar häufig anhand von sog. „Serverregeln", deren Einhaltung durch den Instanzenbetreiber ist aber nicht erzwingbar. Zudem kann nicht jeder Instanzenbetreiber alle Inhalte auf der eigenen Instanz im Blick haben: Moderation bedeutet Zeitaufwand und menschliche Arbeitsleistung. Viele Instanzenbetreiber hosten einen Mastodon-Server hobbymäßig und haben nicht die notwendige Zeit, um eine umfassende Moderation zu gewährleisten. Die Serverregeln unterscheiden sich dabei von Instanz zu Instanz. Während einige Betreiber beispielsweise Werbung generell untersagen, dulden andere Werbung in bestimmten Grenzen. Viele Instanzen weisen zudem darauf hin, dass sich die Nutzer:innen an die jeweils geltenden Gesetze halten müssen und dass rechtswidrige Inhalte entfernt werden. Dies ist ein Hinweis, dessen es selbstverständlich nicht bedürfte. Auch Mastodon ist kein rechtsfreier Raum; insbesondere das Urheberrecht, das Datenschutzrecht und das Strafrecht gelten auf Mastodon ohnehin.

III. Rechtsstellung von Instanzbetreiber:innen

Wie konsequent das geltende Recht auf Mastodon durchgesetzt wird, hängt wiederum von der Wahl der Heimatinstanz ab. Dies gilt zunächst im Hinblick auf das Datenschutzrecht. Wählen Nutzer:innen eine Instanz, deren Server in den USA stehen, so ist jedenfalls aktuell noch davon auszugehen, dass US-Sicherheitsbehörden Zugriff haben auf die gespeicherten personenbezogenen Daten. Wollen Nutzer:innen dies vermeiden, so ist ihnen die Wahl eines in der EU beheimateten Servers zu empfehlen.

Und auch für das Urheberrecht macht die Wahl der Heimatinstanz einen Unterschied. Hier gilt das sog. Schutzlandprinzip. Danach ist das Urheberrecht desjenigen Staates anzuwenden, für den Schutz beansprucht wird. Klingt kompliziert? Ein Beispielsfall macht dies etwas deutlicher: Der in Deutschland ansässige Buchverlag B meldet sich auf der fiktiven Instanz „california.social" an. Er entdeckt, dass Nutzer:innen auf der Instanz Bücher hochladen, für die der Verlag die Rechte hält. Gegen diesen Upload möchte er nun vorgehen. Problem: Die Server der Instanz stehen in den USA. Die Instanz richtet sich vor allem an Personen, die in Kalifornien leben. Der Beschreibungstext für die Instanz ist komplett auf Englisch gehalten und auf der Instanz bewegen sich tatsächlich zumeist Bewohner Kaliforniens. Ist nun das

1 https://github.com/mastodon/mastodon - zuletzt abgerufen am 09. Januar 2023.

deutsche Urheberrecht anwendbar? Nach der Rechtsprechung des Bundesgerichtshofs (BGH) ist deutsches Recht nur dann anwendbar, wenn das Online-Angebot einen „hinreichenden wirtschaftlich relevanten Inlandsbezug“ aufweist. Diese Frage ist im Wege einer Abwägung zu entscheiden. Gegen den wirtschaftlich relevanten Inlandsbezug spricht hier, dass die Instanz ausschließlich in englischer Sprache gehalten ist und sich besonders an die Bewohner Kaliforniens und eben nicht an deutsche Staatsbürger:innen richtet.

Im Strafrecht gilt hingegen das sog. Territorialitätsprinzip. Danach gilt das deutsche Strafrecht für Taten, die in Deutschland begangen wurden. Aber was heißt nun „in Deutschland begangen?“. Dies kann sowohl die Tathandlung als auch den Taterfolg meinen. Wir machen dies wieder deutlich anhand eines Beispielsfalls: Ein fiktiver Nutzer A, deutscher Staatsbürger und Nutzer der fiktiven Instanz „bottrop.social“ wird von dem amerikanischen Staatsbürger B, Nutzer der fiktiven Instanz „california.social“ auf Mastodon beleidigt. B hat seinen Post in San Diego abgeschickt; für A ist der Post allerdings in Bottrop abrufbar. Handlungsort wäre in dem Fall San Diego, Erfolgsort Bottrop. Denn in Bottrop nimmt A den Post zur Kenntnis, hier tritt also der Beleidigungserfolg ein. Das deutsche Strafrecht wäre somit anwendbar. A könnte auch in Deutschland Anzeige erstatten, woraufhin die in Deutschland zuständige Staatsanwaltschaft ermitteln würde. Die Beurteilung des Erfolgsortes ist allerdings von Delikt zu Delikt verschieden. Insbesondere bezüglich des Volksverhetzungstatbestandes haben die Gerichte in den vergangenen Jahren unterschiedlich entschieden.

IV. Öffentliche Stellen und Hochschulen als Instanzenbetreiber:innen

Auch einige öffentliche Stellen und Hochschulen betreiben derzeit schon eine eigene Mastodon-Instanz oder einen Mastodon-Account. Wie schon gezeigt: Der Betrieb einer Instanz und der Betrieb eines Accounts sind zwei gänzlich verschiedene Dinge. Für den Betrieb einer Instanz muss die jeweilige Behörde einen Server betreiben und gegebenenfalls eigene Moderator:innen einstellen. Mit dem eigenen Account betreiben die staatlichen Stellen in der Regel Öffentlichkeitsarbeit und informieren über die eigene behördliche Tätigkeit. Universitäten könnten so zum Beispiel über aktuelle Forschungsprojekte informieren oder die Studierenden mit Mitteilungen für ihr Studium versorgen und Veranstaltungshinweise geben.

Der Betrieb einer eigenen Instanz ist vor allem mit Blick auf das Datenschutzrecht reizvoll. Denn seit längerer Zeit bestehen Bedenken gegen die Nutzung großer amerikanischer Online-Plattformen durch öffentliche Stellen. Die Datenschutzkonferenz (DSK) hat zuletzt in einem Gutachten aus dem März 2022 den Standpunkt vertreten, dass Behörden gemeinsam mit Facebook datenschutzrechtlich verantwortlich sind, wenn sie eine Facebook-Fanpage betreiben. Die DSK vertritt den Standpunkt, dass eine Rechtsgrundlage für den Betrieb von Facebook-Fanpages durch Behörden nicht bestünde.[2] Insbesondere hätten die Behörden keine Informationen darüber, wie Facebook mit den Daten verfährt. Beim Betrieb einer eigenen Mastodon-Instanz ist hingegen nur die staatliche Stelle datenschutzrechtlich verantwortlich und kann für Konformität mit der Datenschutzgrundverordnung (DSGVO) sorgen.

Im Oktober 2020 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) eine eigene Mastodon-Instanz ins Leben gerufen. Diese ist abrufbar unter https://social.bund.de. Auf der Instanz des Bundes kann sich allerdings nicht jede/r beliebige Nutzer:in registrieren. Vielmehr können dort nur andere Bundesbehörden einen Account eröffnen. Die Instanz soll also die Öffentlichkeitsarbeit für den BfDI und andere Bundesbehörden ermöglichen. Derzeit sind auf dieser Instanz beispielsweise aktiv: das Bundesministerium für Wirtschaft und Klimaschutz (@BMWK@social.bund.de), das Bundesinnenministerium (@BMI@social.bund.de), das Auswärtige Amt (@AuswaertigesAmt@social.bund.de), das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (@BMWSB_Bund@social.bund.de) und die Bundesregierung im Ganzen/das Bundespresseamt (@Bundesregierung@social.bund.de).

Eine ähnliche Konstellation besteht für die Behörden des Landes Baden-Württemberg. Im Januar 2021 hat der damalige Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI), Dr. Stefan Brink, eine Instanz eingerichtet. Diese ist anrufbar unter: https://bawü.social. Viele Behörden des Landes haben dieses Angebot wohwollend aufgenommen, sodass auf der Instanz zahlreiche Behörden-Accounts existieren. Dazu

2 Gutachten der Datenschutzkonferenz v. 18. März 2022, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf - zuletzt abgerufen am 10. Januar 2023.

gehört eine größere Zahl von Landkreisen und Städten (die Stadt Freiburg etwa unter: @freiburg@xn--baw-joa.social).

Aber auch viele Baden-Württemberger Hochschulen haben sich inzwischen eigene Accounts auf der Instanz eingerichtet. Dazu gehören zum Beispiel: Uni Mannheim (@unimannheim@xn--baw-joa.social), Uni Freiburg (@unifreiburg@xn--baw-joa.social), die Uni Tübingen (@unituebingen@xn--baw-joa.social), die Uni Konstanz (@unikonstanz@xn--baw-joa.social) und die Hochschule Reutlingen (@Hochschule_Reutlingen@xn--baw-joa.social). Außerhalb Baden-Württembergs sind auf Mastodon anzutreffen beispielsweise die Universität Jena (@unijena@mastodon.social) und die Universität Bremen (@unibremen@wisskomm.social). Zahlreiche Forschungsorganisationen haben sich wie die Uni Bremen einen Account auf der Instanz „wisskomm.social“ erstellt. Diese wird betrieben vom Informationsdienst Wissenschaft e.V.

V. Fazit

Mastodon wird an Bedeutung für Hochschulen und Forschungseinrichtungen hinzugewinnen. Dies liegt zunächst daran, dass Twitter seit der Übernahme von Elon Musk ein immer unbeliebteres Kommunikationsmedium zu werden scheint. Zudem bestehen datenschutzrechtliche Bedenken gegen die Nutzung größerer amerikanischer Online-Plattformen. Mastodon bietet sich hier als datenschutzkonforme Alternative an – wenn die richtige Heimatinstanz gewählt wird.

Kurzbeitrag: Google brings light into the dark (pattern)

Google hat seine Cookie-Banner angepasst

von Klaus Palenberg

Die Verbraucherzentrale NRW hatte Google seiner Cookie-Banner wegen abgemahnt. Diese waren derart gestaltet, dass die Ablehnung von nicht notwendigen Cookies deutlich aufwändiger war, als die Annahme. Nach dem die Verbraucherzentrale NRW Klage vor dem Landgericht Berlin erhoben hatte, änderte Google seine Banner. Nun ist die Ablehnung von Cookies auf der gleichen Stufe wie die Annahme möglich. Die mit den ursprünglichen Bannern verbundene Gestaltungsform wird dark pattern genannt, wobei deren Zulässigkeit sehr umstritten ist.

I. Dark pattern bei Cookie-Bannern

Viele Betreibende von Websites bedienen sich einer Cookie-Banner-Gestaltung, bei der es sehr leicht ist, das Setzen von Cookies[1] zuzulassen. Sie abzulehnen versteckt sich dahingegen häufig in irgendwelchen Einstellungsmöglichkeiten und erfordert meist mehrere Klicks. Auch werden oft farbige Gestaltungen so gewählt, dass einem das Annehmen ins Auge springt, wohingegen das Ablehnen gesucht werden muss. All diese Gestaltungsformen werden unter den Begrifflichkeiten „dark pattern“ oder „nudging“ diskutiert. Es ist hoch umstritten und bislang höchstrichterlich auch nicht geklärt, ob eine solche Gestaltung mit den datenschutzrechtlichen Vorgaben vereinbar ist. Einzig geklärt in diesem Bereich ist, dass die Einwilligung nicht vorausgewählt sein darf und die Ablehnung dann nur per Opt-out möglich ist (Europäischer Gerichtshof, Urteil vom 01.10.2019 – C-673/17 und im Anschluss hieran Bundesgerichtshof, Urteil vom 28.05.2020 – I ZR 7/16). All diesen Gestaltungen ist gemein, dass die Ablehnung nicht notwendiger Cookies zwar tatsächlich möglich ist, diese jedoch künstlich erschwert wird. Im Gegensatz hierzu ist die Einwilligung für die Cookies in diesen Fällen problemlos und ohne Umwege möglich.

II. Abmahnung

Eine solche Form eines Cookie-Banners verwendete auch Google beispielsweise auf der Internetseite www.google.de. Auf der ersten Seite des Banners gab es die Auswahlmöglichkeiten, alle Cookies anzunehmen oder in ein Einstellungsmenü zu gelangen. In diesen Einstellungen wiederum wurden drei Kategorien von Cookies vorgestellt, deren Setzen jeweils einzeln abzulehnen war. Somit bedurfte es zur Ablehnung sämtlicher nicht notwendiger Cookies mehrerer Klicks, wohingegen die Annahme durch einen einzigen Klick möglich war.

In dieser Gestaltung sah die Verbraucherzentrale NRW einen Verstoß gegen nationales und europäisches Datenschutzrecht und mahnte Google wegen der Verwendung unzulässiger Cookie-Banner ab. Das Setzen von Cookies richtet sich zum einen nach Art. 5 Abs. 3 S. 1 der Richtlinie 2002/58/EG (ePrivacy-RL) und zum anderen nach § 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)[2]. § 25 Abs. 1 TTDSG fordert dabei eine Einwilligung „auf der Grundlage von klaren und umfassenden Informationen“ i.S.d. Verordnung (EU) 2016/679 (DSGVO).

1 Dazu, was Cookies überhaupt sind und wie sie funktionieren, siehe John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022.

2 Siehe hierzu John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022.

III. Ausblick und Folgen

Nachdem Google dem Unterlassungsbegehren der Verbraucherzentrale NRW nicht nachkam, erhob diese Klage bei dem Landgericht Berlin. Im Laufe des Verfahrens gab Google dann doch die geforderte Unterlassungserklärung ab und änderte seine Cookie-Banner. Nun befinden sich die Auswahlmöglichkeiten zum Ablehnen und Annehmen aller nicht notwendiger Cookies auf derselben, ersten Ebene. Daraufhin erklärte die Verbraucherzentrale NRW das Verfahren für erledigt, wodurch das Verfahren vor einem Urteilsspruch beendet wurde.

Google hat mit seiner lobenswerten Entscheidung, den Klageanspruch anzuerkennen und seine Banner zu ändern, zwar dafür gesorgt, dass kein entsprechendes Urteil ergehen musste. Zugleich hat Google aber damit auch verhindert, dass die Frage nach der Zulässigkeit einer solchen Banner-Gestaltung (höchst-) richterlich geklärt wird. Daher lässt sich die Entscheidung von Google nicht auf andere Websitebetreibende übertragen. Allerdings hat mit Google einer der größten Profiteure von Cookie-basierter Werbung seine Praxis des dark pattern jetzt zumindest merklich eingeschränkt. Wie groß der damit verbundene Gewinn für den Datenschutz der Nutzenden tatsächlich im Ergebnis ist, wird sich erst noch zeigen müssen. Google hatte nämlich bereits zuvor angekündigt künftig weniger auf Cookies und mehr auf andere Tracking-Methoden zur Nutzenden-Verfolgung zurückzugreifen.

Auch ist offen, inwieweit sich andere Website-Betreibende ein Beispiel an Google nehmen und ihre Cookie-Banner ebenfalls anpassen. Auf jeden Fall aber lässt sich festhalten, dass im Hinblick auf Cookie-Banner noch viele Fragen offen sind und unklar ist, wie es mit ihnen weitergeht. Werden sie in Zukunft nutzerfreundlicher gestaltet werden, wie in diesem Fall? Werden sie von sogenannten Personal Information Management Systemen (PIMS)[3] abgelöst, wie es das TTDSG vorsieht? Oder werden Cookies gar gänzlich von neuen Tracking-Technologien abgelöst? Doch auch im letztgenannten Fall könnten sich die gleichen oder zumindest ähnliche Fragen wie bei den aktuellen Cookie-Bannern auch in Zukunft stellen.

Dieses Verfahren zeigt, dass zwar gerade im Bereich von Cookies und der Gestaltung von Cookie-Bannern erhebliche Rechtsunsicherheiten bestehen. Betreibende von Websites, wie etwa Hochschulen, sollten aber nicht darauf vertrauen, dass diese Unwägbarkeiten von den Datenschützenden allein zu ihren Gunsten ausgelegt werden. Vielmehr besteht auch auf deren Seite ein erhebliches Interesse an Rechtssicherheit, welche im Moment vor allem durch (höchstrichterliche) Urteilssprüche zu erwarten ist. Dass ein derart bedeutender Anbietender wie Google nun seine Rechtsauffassung in dieser Frage geändert zu haben scheint, sollte Anlass genug sein, die eigenen Cookie-Banner zu überprüfen und gegebenenfalls auf Gestaltungen aus dem Bereich dark pattern oder nudging zu verzichten.

3 Siehe hierzu John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn