

29.04.2020

EVALUIERUNG: UMSETZUNG DER EMPFEHLUNGEN DER DATENETHIKKOMMISSION

Eine Evaluation der Umsetzung der Empfehlungen der Datenethikkommission durch die Bundesregierung und die Europäische Kommission

Impressum

Verbraucherzentrale

Bundesverband e.V.

Team

Digitales und Medien

Rudi-Dutschke-Straße 17

10969 Berlin

digitales@vzbv.de

INHALT

EVALUIERUNG: UMSETZUNG DER EMPFEHLUNGEN DER DATENETHIKKOMMISSION	1
INHALT	2
I. ZUSAMMENFASSUNG	2
1. Einleitung.....	2
2. Gesamtfazit	2
3. Bewertungsmethode.....	3
II. EVALUIERUNG DER UMSETZUNG EINZELNER EMPFEHLUNGEN	4

I. ZUSAMMENFASSUNG

1. EINLEITUNG

Im Oktober 2019 hat die Datenethikkommission (DEK) der Bundesregierung nach über einem Jahr intensiver Arbeit die zentralen Handlungsempfehlungen zu den Themen Künstliche Intelligenz (KI), algorithmische Systeme und Datenpolitik vorgestellt. Diese Empfehlungen enthalten wichtige Aufgaben für die Bundesregierung und den europäischen Gesetzgeber.

Die Bundesregierung hat die DEK im Juli 2018 eingesetzt. Als Mitglieder wurden neben dem Verbraucherzentrale Bundesverband (vzbv) Vertreter der Wirtschaft, Wissenschaft und Zivilgesellschaft benannt. Durch die paritätische Besetzung repräsentieren die von der DEK erarbeiteten Handlungsempfehlungen daher einen breiten gesellschaftlichen Konsens. Der vzbv hat im Oktober 2019 die Empfehlungen ausführlich bewertet und aufgezeigt, welche Aufgaben sich hieraus für die Bundesregierung und die EU-Kommission ergeben. Eine konsequente Umsetzung der Empfehlungen würde die Risiken algorithmischer Systeme minimieren und gleichzeitig Verbraucherschutz, Rechtsstaatlichkeit und das soziale Zusammenleben fördern. Der vzbv wird die Umsetzung einiger wesentlicher Empfehlungen der DEK durch die Bundesregierung und die EU-Kommission deshalb regelmäßig evaluieren.

2. GESAMTFAZIT

Insgesamt bleiben EU-Kommission und Bundesregierung in ihren aktuellen Vorhaben deutlich hinter hier evaluierten Empfehlungen der DEK zurück.

Die Bundesregierung als auch die EU-Kommission scheinen hier unter starkem Druck der Wirtschaft zu stehen. Dabei wird von Wirtschaft wie auch Politik häufig übersehen, dass ein großer Teil des berechtigten Misstrauens gegen algorithmische System darauf beruht, dass für Außenstehende nicht nachvollziehbar ist, inwieweit diese Systeme die rechtlichen Rahmenbedingungen beachten und beispielsweise Verbraucher nicht ungerechtfertigt diskriminieren. Würden die Vorschläge der DEK zu Transparenz, Nachvollziehbarkeit, Qualitätsvorgaben und Kontrolle dieser Systeme umgesetzt werden, würde

auch das Vertrauen der Verbraucher in diese Technologie steigen und damit die Akzeptanz für deren Einsatz im Alltag. Es sind auch keine Pläne der Bundesregierung erkennbar, ein Kompetenzzentrum Algorithmische Systeme einzurichten, das bestehende Aufsichtsbehörden durch methodisch-technischen Sachverstand bei der Kontrolle algorithmische Systeme unterstützt.

Ebenso vermisst der vzbv bei der Politik ein deutliches Bekenntnis zu einem Verbot von De-Anonymisierung und Aufhebung von Pseudonymisierung. Auch eine Verschärfung und Konkretisierung des Rechtsrahmens für Profilbildung und Scoring wird nicht aktiv angestrebt. Es steht zu befürchten, dass Verbraucher weiterhin vor ungerechtfertigter Profilbildung nicht geschützt werden.

Auch wenn die DEK ihre Empfehlungen erst vor gut einem halben Jahr veröffentlicht hat, bleibt festzuhalten, dass bereits jetzt erkennbar ist, dass einige Aspekte, die aus Verbrauchersicht wesentlich sind, in den bislang auf den Weg gebrachten Vorhaben fehlen. Es bleibt also noch viel zu tun für die Bundesregierung und die EU-Kommission, um durch einen ausgewogenen Regulierungsrahmen das Vertrauen der Verbraucher zu stärken.

3. BEWERTUNGSMETHODE

Die Bewertung des Aufgreifens der Empfehlungen der DEK erfolgt anhand einer 5er-Skala:



Die Empfehlung wurde/wird nicht umgesetzt



Die Empfehlung wurde/wird kaum umgesetzt



Die Empfehlung wurde/wird teilweise umgesetzt



Die Empfehlung wurde/wird größtenteils umgesetzt



Die Empfehlung wurde/wird vollständig umgesetzt

Die Bewertung des Verfahrensstands erfolgt anhand der Kategorien:

- *Nicht begonnen*
- *Begonnen*
- *Abgeschlossen*

II. EVALUIERUNG DER UMSETZUNG EINZELNER EMPFEHLUNGEN

1. Rechtsrahmen für Profilbildungen und automatisierte Entscheidungen

Was empfiehlt die Datenethikkommission?

Die DEK empfiehlt erstens die Schaffung eines konkreten und strengeren Rechtsrahmens für Profilbildung und Scoring, insbesondere in persönlichkeitsensiblen Bereichen. Damit soll das Risiko der Manipulation und der Diskriminierung effektiv reduziert werden (DEK-Forderung Nr. 3).

Zweitens sollen Anbieter zu technischen und mathematischen-prozeduralen Qualitätsgarantien verpflichtet werden. Ziel ist die Korrektheit und Rechtmäßigkeit algorithmisch ermittelter Ergebnisse durch Verfahrensvorgaben abzusichern. (DEK-Forderung Nr. 51).

Warum ist das wichtig?

Es greift tief in die Rechte und Freiheiten der Menschen ein, wenn Unternehmen ihr Verhalten und ihre Lebensumstände analysieren und bewerten. Die besonderen Beschränkungen der Datenschutz-Grundverordnung für automatisierte Entscheidungen¹ greifen hier jedoch zu kurz. Aktuell werden Verbraucherinnen und Verbraucher² daher nicht ausreichend vor Profilbildungen und ungerechtfertigten automatisierten Entscheidungen geschützt.

Zudem fehlen Qualitätsanforderungen an automatisierte Entscheidungen, die sicherstellen, dass die Systeme mit validen Annahmen und Modellen arbeiten, die Ergebnisse auf relevanten, richtigen Daten basieren und nicht diskriminieren.

Wer muss die Empfehlung umsetzen?

¹ Artikel 22 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

² Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

Die Umsetzung liegt bei der EU. Die DSGVO regelt europaweit Profilbildungen und automatisierte Entscheidungen, weist aber Schutzlücken auf. Die Bundesregierung wiederum sollte sich über den Rat der Europäischen Union für eine europäische Regelung einsetzen.

Wie bewertet der vzbv die bisherige Umsetzung?

- Die EU-Kommission schlägt in ihrem Weißbuch zur KI³ verpflichtende Anforderungen an die Datengrundlage für hochriskante Systeme vor. Ob etwa lernende Systeme anhand von Daten trainiert werden, die einen sicheren Betrieb garantieren, dass sie nicht durch verzerrte Daten diskriminieren und Anforderungen an Robustheit und Genauigkeit erfüllen. Dies ist zu begrüßen. Leider ist die Definition von Hochrisiko-Sektoren, für die diese Anforderungen gelten würden, zu eng gefasst. Viele Systeme mit einem hohen Schadenspotenzial wären somit nicht erfasst.
- Gut ist, dass sich die Bundesregierung dafür eingesetzt hat, dass die EU-Kommission die DSGVO auf Schutzlücken beim Scoring und der Profilbildung prüfen soll. In der KI-Strategie der Bundesregierung fehlt aber ein deutliches Bekenntnis zur Verschärfung und Konkretisierung des Rechtsrahmens für Profilbildungen und Scoring.

Bewertung



Die Empfehlung wurde/wird kaum umgesetzt

Status:

Begonnen

2. Anonymisierung und Pseudonymisierung

Was empfiehlt die Datenethikkommission?

Die DEK empfiehlt die Entwicklung von Verfahren und Standards für die Anonymisierung. Außerdem plädiert die DEK für die Einführung eines strafbewehrten Verbots einer De-Anonymisierung bisher anonymer Daten sowie ein Verbot der Aufhebung der Pseudonymisierung jenseits eng definierter Rechtfertigungsgründe. Ebenso wird empfohlen, die vielversprechende Forschung im Bereich synthetischer Daten weiter zu fördern (DEK-Forderung Nr. 20).

Warum ist das wichtig?

Anonyme Daten schützen die Privatsphäre von Verbrauchern. Allerdings ist eine einwandfreie Anonymisierung eine Herausforderung, insbesondere wenn solche Daten mit

³ Europäische Kommission, 2020, Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“, COM(2020) 65 final https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf

unbestimmten Empfängern geteilt, veröffentlicht oder aus verschiedenen Quellen zusammengeführt werden.

Auch ist die Anonymisierung in der DSGVO nicht absolut formuliert. Es gibt somit Anonymisierungsmaßnahmen und -techniken unterschiedlicher Qualität, die für verschiedene Zwecke unterschiedlich angemessen und geeignet sind. Daher sind Anforderungen an die Anonymisierung erforderlich. Beispielsweise muss geklärt werden, wann eine Anonymisierung hinreichend ist. Zudem bedarf es weiterer Schutzkonzepte, die das Risiko der De-Anonymisierung verringern.

Synthetische Datensätze werden künstlich aus original Datensätzen über echte Personen generiert. Sie enthalten keine Daten über natürliche Personen, besitzen aber dieselben statistischen Eigenschaften wie die Originaldaten. Deshalb kann man mit ihnen datenschutzfreundlich algorithmische Systeme trainieren.

Wer muss die Empfehlung umsetzen?

- Verfahren und Standards der Anonymisierung könnten durch die Unternehmen in Kooperation mit den Datenschutzaufsichtsbehörden festgelegt werden. Die Bundesregierung und die EU-Kommission sollten die Erarbeitung von solchen Standards unterstützen und fördern.
- Das Europäische Parlament und der Rat der Europäischen Union könnten nach einem Vorschlag der Europäischen Kommission weitere Schutzkonzepte für anonyme Daten beschließen, wie beispielsweise ein Verbot der De-Anonymisierung. Dies würde einen EU-weiten Flickenteppich an Regelungen verhindern.
- Die Bundesregierung ist in der Pflicht, sich über den Rat der Europäischen Union für eine entsprechende europäische Regelung einzusetzen.
- Die Förderung der Forschung im Bereich synthetischer Daten kann sowohl auf nationaler als auch europäischer Ebene erfolgen: Im Rahmen einer nationalen und europäischen Datenstrategie sowie über Programme zur Forschungsförderung.

Wie bewertet der vzbv die bisherige Umsetzung?

- In der Datenstrategie der EU-Kommission⁴ werden Fragen rund um die Anonymisierung von personenbezogenen Daten nicht thematisiert. Es ist bedauerlich, dass hier weder eine Förderung der Forschung an Anonymisierungstechnologien, noch konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten durch gesetzliche Vorgaben und die Entwicklung von Standards vorgesehen ist.
- In der nationalen Datenstrategie⁵ sowie in der KI-Strategie⁶ greift die Bundesregierung Fragen zur Anonymisierung und Pseudonymisierung von Daten auf. Sie möchte die Forschung in diesen Bereichen sowie im Gebiet der Erstellung synthetischer Trainingsdaten fördern. Auch möchte sie die Förderung auf europäischer Ebene anregen. Dies ist zu begrüßen und im Sinne der DEK. Der vzbv

⁴ Europäische Datenstrategie: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

⁵ Eckpunkte der Datenstrategie des Bundes: <https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-1693546>

⁶ KI-Strategie der Bundesregierung: <https://www.ki-strategie-deutschland.de/home.html>

bedauert jedoch, dass weiterführende Schutzkonzepte, wie ein Verbot von De-Anonymisierung und Aufhebung der Pseudonymisierung, in der Datenstrategie nicht thematisiert werden.

Bewertung



Die Empfehlung wurde/wird kaum umgesetzt

Status:

Begonnen

3. Regulierung und Förderung von Datenmanagement- und Datentreuhandsystemen

Was empfiehlt die Datenethikkommission?

Die DEK empfiehlt die Förderung von Forschung und Entwicklung im Bereich von innovativen Datenmanagement- und Datentreuhandsystemen, wie Privacy Management Tools (PMT) und Personal Information Management Services (PIMS). Diese Einführung von Datenmanagement- und Datentreuhandsystemen sollte auf europäischer Ebene erfolgen. Dies könnte dem Schutz von Verbrauchern vor vermeintlich neutralen Interessenverwaltern, die tatsächlich jedoch wirtschaftliche Eigeninteressen am Betreiben der Systeme haben, dienen (DEK-Forderung Nr. 21).

Warum ist das wichtig?

Datenmanagement- und Datentreuhandsysteme reichen von technischen Dashboards bis hin zu Systemen zur Datenverwaltung und Einwilligungsmanagement. Sind diese nutzerfreundlich und datenschutzkonform gestaltet, können sie Verbraucher bei der Kontrolle über die Verwendung ihrer Daten unterstützen – etwa bei der Einwilligung in AGBs und Datenschutzerklärungen.

Eine Regulierung muss sicherstellen, dass die Rechte des Einzelnen geschützt werden, insbesondere muss ausgeschlossen sein, dass die Betreiber wirtschaftliche Eigeninteressen an den Daten haben. Wenn die Datentreuhänder im Interesse der Nutzer handeln, können sie eine Schnittstelle zwischen der Datenwirtschaft und den Nutzern bilden.

Wer muss die Empfehlung umsetzen?

- Eine Regulierung von Datenmanagement- und Datentreuhandsystemen sollte durch den europäischen Gesetzgeber erfolgen. Diese Systeme sind de facto mehrseitige Plattformen und unterliegen direkten und indirekten Netzwerkeffekten, sodass sie vermutlich Daten von Nutzern aus unterschiedlichen Mitgliedsstaaten der EU bündeln werden.

- Die Förderung zur Erforschung und Entwicklung von Datenmanagement- und Datentreuhandssystemen kann sowohl auf nationaler als auch europäischer Ebene erfolgen.

Wie bewertet der vzbv die bisherige Umsetzung?

- Die EU-Kommission prüft im Rahmen ihrer Datenstrategie, ob „Vorschriften für Anbieter von Anwendungen für personenbezogene Daten oder für neuartige Datenmittler, wie Anbieter persönlicher Datenräume“ erforderlich sind, wobei deren Rolle als neutraler Vermittler gewährleistet werden muss. Dies wird durch den vzbv begrüßt.
- Laut ihrem Eckpunktepapier zur Datenstrategie möchte die Bundesregierung prüfen, „welche Voraussetzungen geschaffen werden müssen und welchen Beitrag vertrauenswürdige Datenräume und Strukturen von Datentreuhändern leisten können, um das freiwillige Teilen von Daten zu verstärken.“ Auch dies unterstützt der vzbv, soweit dabei auch den mit Datentreuhändern verbundenen Risiken begegnet wird.

Bewertung



Die Empfehlung wurde/wird kaum umgesetzt

Status:

Nicht begonnen

4. Datenportabilität und Pflicht zur Interoperabilität

Was empfiehlt die Datenethikkommission?

Datenportabilität ist das Recht einer Person, personenbezogene Daten bei einem Anbieterwechsel mitzunehmen. Durch diese bessere Kontrolle der eigenen Daten wird das **Recht auf informationelle Selbstbestimmung gestärkt**. Die DEK empfiehlt, die Datenportabilität zu erleichtern und zu befördern. Nötig sind laut DEK dafür die Erarbeitung branchenbezogener Verhaltensregeln für Unternehmen und Standards für Datenformate. Sie fordert eine Evaluierung, wie sich das bestehende Portabilitätsrecht auf den Markt auswirkt und wie eine weitere Stärkung der marktmächtigen Player verhindert werden kann (DEK-Forderung Nr. 22).

Warum ist das wichtig?

Datenportabilität erleichtert Verbrauchern die Übertragung ihrer Daten von einem Anbieter zu einem anderen. Dies kann den Anbieterwechsel fördern und damit zu mehr Wettbewerb führen.

Wer muss die Empfehlung umsetzen?

Laut DSGVO sind Unternehmen in der Pflicht, branchenbezogene Verhaltensregeln für interoperable Standards für Datenformate zu entwickeln, unter Einbeziehung der Datenschutz-Aufsichtsbehörden. Die Bundesregierung und die EU-Kommission sollten dies unterstützen und fördern.

Wie bewertet der vzbv die bisherige Umsetzung?

- Die EU-Kommission prüft im Rahmen ihrer Datenstrategie, ob es eines erweiterten Rechts des Einzelnen auf Datenübertragbarkeit gemäß Artikel 20 DSGVO bedarf. Dies ist zu begrüßen.
- Laut Eckpunktepapier zur Datenstrategie plant die Bundesregierung, die Forschung zur Entwicklung einer praxistauglichen Datenportabilität zu fördern. Dies ist im Sinne der DEK zu begrüßen. Mit einem Beteiligungsprozess zur Erarbeitung von Standards für Telemedien möchte die Bundesregierung⁷ Datenportabilität stärken – leider nur bei Sozialen Netzwerken und Messenger-Diensten. Dies ist als erster Schritt zu begrüßen, bleibt aber hinter der DEK-Empfehlung zurück.

Bewertung



Die Empfehlung wurde/wird teilweise umgesetzt

Status:

Begonnen

5. Risikoadaptierten Regulierungsansatz einführen

Was empfiehlt die Datenethikkommission?

Die DEK fordert mehr Kontrolle und eine nach Risiko gestaffelte Regulierung für algorithmische Systeme. Ein steigendes Schädigungspotenzial soll mit wachsenden Anforderungen und Eingriffstiefen der regulatorischen Instrumente einhergehen. Konkret empfiehlt die DEK fünf Regulierungsklassen. Algorithmische Systeme mit „unvertretbarem Schädigungspotenzial“ sollen sogar verboten werden können (etwa bestimmte autonome Waffensysteme). Bei der Risikobewertung sollen alle Komponenten, Entwicklungsschritte und ihre Implementierung im sozialen Kontext berücksichtigt werden (DEK-Forderung Nr. 36).

Warum ist das wichtig?

Algorithmische Systeme können wichtige Entscheidungen über Menschen treffen oder vorbereiten. Dabei können - absichtlich oder unabsichtlich – Einzelnen, Gruppen oder

⁷ S. 81 <https://www.bundesregierung.de/resource/blob/975292/1605036/61c3db982d81ec0b4698548fd19e52f1/digitalisierung-gestalten-download-bpa-data.pdf?download=1>

der Gesellschaft große Schäden entstehen. Die Risiken umfassen beispielsweise Diskriminierungen, Verletzung von Persönlichkeitsrechten, Gesundheit, wirtschaftliche Schäden, Ausschluss von Teilhabe und Autonomie jedes Einzelnen. Je höher das Schadenspotenzial einer Anwendung, umso wichtiger ist es, sicherzustellen, dass sie rechtskonform, gerecht und sicher funktioniert.

Wer muss die Empfehlung umsetzen?

Der abgestufte **risikoadaptierte Regulierungsansatz** für algorithmische Systeme muss durch den europäischen Gesetzgeber etabliert werden. Dies ist ordnungspolitisch sinnvoll, um eine Zersplitterung der Regulierungslandschaft in Europa zu vermeiden. Eine europaweit einheitliche Regelung schafft Rechtssicherheit für Unternehmen und Verbraucher. Zudem sollte über das Marktortprinzip der europäische Regelungsrahmen quasi zum internationalen Standard – ähnlich wie die DSGVO (der sogenannte „Brussels Effect“) werden.

Wie bewertet der vzbv die bisherige Umsetzung?

Das Weißbuch zur KI der EU-Kommission schlägt vor, hochriskante Systeme, im Rahmen einer europäischen Regulierung, verpflichtenden Anforderungen zu unterwerfen. Der vorgeschlagene Ansatz bleibt in verschiedenen Aspekten hinter dem zurück, was die DEK empfiehlt:

Der Ansatz ist binär. Ein abgestuftes Regulierungssystem mit mehreren Risikoklassen ist leider nicht vorgesehen.

Die Definition des Risikos und potenziellen Schadens ist zu eng gefasst. Neben Schaden/Risiken für Einzelne müssten auch Auswirkungen auf die Gesellschaft und einzelne soziale Gruppen sowie ökonomische Schäden berücksichtigt werden.

Leider begrenzt der Ansatz zur Definition von Hochrisiko-Anwendungen den Anwendungsbereich der KI-Regeln auf bestimmte Sektoren. Aber auch außerhalb der Hochrisiko-Sektoren gibt es Anwendungen, die aufgrund ihrer Risiken strengerer Regeln bedürfen. Etwa wenn künftig Persönlichkeitsanalysen auf Basis von Social Media Daten mitentscheiden, ob man Zugang zu Onlinemarktplätzen erhält.⁸

Bewertung



Die Empfehlung wurde/wird kaum umgesetzt

Status:

Begonnen

6. Kennzeichnungspflicht für algorithmischen Systeme

⁸ <https://www.businessinsider.de/international/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1/?r=US&IR=T>

Was empfiehlt die Datenethikkommission?

Die DEK empfiehlt eine Kennzeichnungspflicht für algorithmische Systeme mit einem gewissen Risikopotenzial. Verbrauchern soll deutlich gemacht werden, ob und in welchem Umfang algorithmische Systeme zum Einsatz kommen. Unabhängig von den Risiken der Anwendung, sollte immer eine Kennzeichnungspflicht gelten, wenn bei der Interaktion mit algorithmischen Systemen eine Verwechslungsgefahr zwischen Menschen und Maschine besteht. Ausnahmen wären Fälle, in denen man eine maschinelle Stimme erwartet, etwa bei Bahnhofsdurchsagen (DEK-Forderung Nr. 45).

Warum ist das wichtig?

Digitale Sprachassistenten sind beispielsweise bereits so hoch entwickelt, dass viele Menschen am Telefon nicht erkennen, ob es sich bei dem Anrufer um eine Maschine handelt. Manche Systeme sollen in Echtzeit Emotionen von Menschen erkennen und auswerten. Menschen sollten darauf aufmerksam gemacht werden müssen, dass sie mit einem algorithmischen System interagieren. Dann können sich Verbraucher beispielsweise für oder gegen einen Dienst entscheiden und/oder vor der Inanspruchnahme zusätzliche Informationen einholen und sich gegen Irreführungen wehren. Ebenso müssen Betroffene, wenn wichtige Entscheidungen über sie automatisiert vorbereitet oder getroffen werden, wissen, dass das passiert und in welchem Umfang. Nur dann können Sie ihre entsprechenden Rechte ausüben und beispielsweise die Datengrundlage überprüfen und sich gegen Diskriminierung wehren.

Wer muss die Empfehlung umsetzen?

- Die Umsetzung einer Kennzeichnungspflicht muss durch den europäischen Gesetzgeber erfolgen. Mit der DSGVO liegt ein europäischer Rechtsrahmen vor, in dem bereits Informationspflichten im Bereich Datenschutz geregelt werden. Eine horizontal geregelte Kennzeichnungspflicht muss deshalb komplementär dazu auf europäischer Ebene angesiedelt werden.
- Gleichwohl muss sich die Bundesregierung über den Rat der Europäischen Union für eine entsprechende europäische Regelung einsetzen.

Wie bewertet der vzbv die bisherige Umsetzung?

Das KI-Weißbuch schlägt vor, eine Kennzeichnungspflicht für hochriskante Anwendungsfälle einzuführen. So soll sichergestellt werden, dass Verbraucher sich bewusst sind, wenn sie mit einer KI interagieren. Nach dem Weißbuch zur KI würde die Kennzeichnungspflicht nur für Hochrisiko-Anwendungen gelten. Der kumulative Ansatz zur Definition von Hochrisiko-Anwendungen begrenzt den Anwendungsbereich einer Kennzeichnungspflicht auf hochriskante Anwendungen innerhalb vorab definierter Hochrisiko-Sektoren. Aber auch außerhalb dieser Hochrisiko-Sektoren gibt es riskante KI-Anwendungen, die strengerer KI-Regeln bedürfen. Insofern ist der bislang im Weißbuch vorgeschlagene Ansatz zu eng gefasst und sollte erweitert werden.

Bewertung



Die Empfehlung wurde/wird kaum umgesetzt

Status:

Begonnen

7. Individuelle Erklärung für Betroffene einer Entscheidung

Was empfiehlt die Datenethikkommission?

Die DEK empfiehlt, Betreiber von algorithmischen Systemen in bestimmten Bereichen zu verpflichten, betroffenen Personen eine **individuelle Erklärung** der konkreten Gründe der Entscheidung über sie zu geben. Dies soll zusätzlich zur allgemeinen Erläuterung der Logik (Vorgehensweise) und Tragweite des Systems erfolgen (DEK-Forderung Nr. 47).

Warum ist das wichtig?

Auskunftsrechte sind für Verbraucher zentral, um algorithmenbasierte Entscheidungen nachvollziehen und individuell überprüfen zu können. Nur so können sie ihre – beispielsweise in der DSGVO festgelegten – Rechte wahrnehmen und eine Entscheidung fundiert anfechten. Etwa um sich gegen Diskriminierungen oder Fehlentscheidungen zu wehren. Wesentlich ist dabei, dass Verbraucher verständlich, relevant und konkret informiert werden und ihnen das Ergebnis für den Einzelfall erläutert wird (anders als bei der allgemeinen Informationspflicht nach DSGVO, bei der die Funktionsweise eines algorithmischen Systems allgemein dargelegt wird).

Wer muss die Empfehlung umsetzen?

- Die Umsetzung einer Pflicht für Betreiber zur individuellen Erklärung muss durch den europäischen Gesetzgeber erfolgen. Mit der DSGVO liegt ein europäischer Rechtsrahmen vor, in dem bereits Informationspflichten und Auskunftsrechte im Bereich Datenschutz geregelt werden. Eine horizontal geregelte Pflicht für Betreiber zur individuellen Erklärung sollte komplementär dazu auf europäischer Ebene angesiedelt werden.
- Gleichwohl muss sich die Bundesregierung über den Rat der europäischen Union für eine entsprechende Regelung einsetzen.

Wie bewertet der vzbv die bisherige Umsetzung?

- Das KI-Weißbuch schlägt verpflichtende Anforderungen für hochriskante algorithmische Systeme vor (unter anderem zu Transparenz gegenüber Aufsichtsbehörden, Dokumentationspflichten und eine Kennzeichnungspflicht). Bedauerlicherweise ist eine Pflicht für Betreiber der Systeme, Betroffenen eine individuelle Erklärung für die konkreten Gründe einer Entscheidung, jedoch nicht vorgesehen.
- In der KI- und Datenstrategie der Bundesregierung findet sich kein klares Bekenntnis für eine Verpflichtung der Betreiber algorithmischer Systeme, Betroffenen die getroffene Entscheidung individuell zu erklären. Laut KI-Strategie will die Bundesregierung lediglich prüfen, inwieweit Transparenz, Nachvollziehbarkeit und Überprüfbarkeit von KI-Systemen hergestellt werden kann. Dies ist aus Verbrauchersicht zu wenig und zu unverbindlich.

Bewertung



Die Empfehlung wurde/wird nicht umgesetzt

Status:

Nicht begonnen

8. Pflicht zur Erstellung und Veröffentlichung einer Risikofolgenabschätzung

Was empfiehlt die Datenethikkommission?

Die DEK will Betreiber von algorithmischen Systemen (ab einem gewissen Schädigungspotenzial) zur Veröffentlichung einer Risikofolgenabschätzung verpflichten. Diese sollte auch bei der Verarbeitung nicht-personenbezogener Daten greifen und Risiken außerhalb des Datenschutzes berücksichtigen: Risiken für die Selbstbestimmung, Privatheit, körperliche Unversehrtheit, persönliche Integrität sowie das Vermögen, Eigentum und Diskriminierung. Zudem soll die Risikofolgenabschätzung neben den zugrundeliegenden Daten und der Logik des Modells auch Qualitätsmaße und Fairnessmaße zu den zugrundeliegenden Datenmodellen berücksichtigen: Etwa zu Bias (Verzerrungen) oder (statistischen) Fehlerquoten, die ein System bei der Vorhersage oder Kategorienbildung aufweist (DEK-Forderung Nr. 49).

Warum ist das wichtig?

Die in der DSGVO vorgesehene Folgenabschätzung (Art. 35 Abs. 1 DSGVO) umfasst ausschließlich Informationen zu den Folgen bezüglich des Schutzes personenbezogener Daten und keine umfassende Risikoanalyse algorithmischer Systeme.

Vertrauen in algorithmische Systeme kann nur auf Grundlage einer informierten öffentlichen Debatte und Bewertung um die Chancen und Risiken dieser Systeme entstehen.

Um diese Debatte führen zu können, müssen die grundlegenden Eigenschaften und potenziellen Risiken algorithmischer Systeme öffentlich zugänglich sein. Dafür muss etwa bekannt sein, auf welche allgemeine Datengrundlage ein Machine-Learning-basiertes algorithmisches System trainiert wurde, welche Datenkategorien einbezogen werden oder auf welche Kriterien das System optimiert.

Wer muss die Empfehlung umsetzen?

- Die Einführung einer Pflicht für Betreiber von algorithmischen Systemen zur Erstellung und Veröffentlichung einer Risikofolgenabschätzung muss durch den europäischen Gesetzgeber erfolgen: Eine Regelung der Risikofolgenabschätzung sollte in diesem Rahmen erfolgen, um eine europaweit einheitliche Regelung zu erhalten, die Rechtssicherheit für Unternehmen sowie hohe Schutzstandards für alle Verbraucher in Europa sicherstellt.
- Gleichwohl muss sich die Bundesregierung über den Rat der Europäischen Union für eine entsprechende Regelung einsetzen.

Wie bewertet der vzbv die bisherige Umsetzung?

- Das KI-Weißbuch schlägt lediglich vor, Entwickler von hochriskanten Systemen zu verpflichten, den Betreibern der Systeme oder Behörden Informationen bezüglich der Fähigkeiten und Grenzen des Systems vorzulegen. Etwa der Zweck des Systems, die Bedingungen, unter denen es bestimmungsgemäß funktionieren sollte und Genauigkeitsmaße. Es handelt es sich dabei um keine umfassende Risikoanalyse, die auch Systemrisiken im sozioökonomischen Kontext betrachtet. Vor allem ist keine Pflicht zur Veröffentlichung der Folgenabschätzung vorgesehen, so wie von der DEK gefordert. Dies ist aus Verbrauchersicht nicht ausreichend und sollte dringend nachgebessert werden.
- Der vzbv bedauert, dass weder aus der KI-Strategie noch der Datenstrategie der Bundesregierung hervorgeht, dass die Bundesregierung darauf hinarbeitet, eine Pflicht zur Erstellung und Veröffentlichung einer Risikofolgenabschätzung auf europäischer Ebene voranzutreiben.

Bewertung



Die Empfehlung wurde/wird nicht umgesetzt

Status:

Nicht begonnen

9. Pflicht zur Dokumentation und Protokollierung

Was empfiehlt die Datenethikkommission?

Die DEK fordert eine Pflicht zur Dokumentation und Protokollierung der Programmabläufe der Software bei sensiblen Anwendungen, die nachhaltige Schäden verursachen können. Die dabei verwendeten Datensätze und Modelle sollen so dokumentiert und protokolliert werden, dass Aufsichtsbehörden diese im Rahmen einer Kontrolle nachvollziehen können. Zudem sollen Anforderungen an die Dokumentation und Protokollierung konkretisiert werden, um Rechtssicherheit für die verantwortlichen Betreiber/Entwickler zu schaffen (DEK-Forderung Nr. 50).

Warum ist das wichtig?

Aufsichtsbehörden müssen auch komplexe Systeme nachvollziehen können. Dies ist nur gewährleistet, wenn die Prozessschritte, Datengrundlage, algorithmisches Modell etc. entsprechend dokumentiert werden. Die Dokumentationspflicht muss dabei den gesamten Prozess der Entscheidungsfindung beziehungsweise Entscheidungsvorbereitung eines algorithmischen Systems umfassen (etwa das Trainingsmodell und Trainingsdaten, Entscheidungen über die Kriterien, nach denen ein Modell optimiert wurde). Nur dann kann eine externe Aufsicht effektiv kontrollieren, ob ein System rechtskonform ist, beispielsweise hinsichtlich des Diskriminierungsverbots.

Wer muss die Empfehlung umsetzen?

- Eine Regelung zur Dokumentation und Protokollierung sowie ein Anforderungskatalog an eine rechtssichere Dokumentation und Protokollierung müssen in einen europäischen Rechtsrahmen Eingang finden.
- Gleichwohl muss sich die Bundesregierung über den Rat der Europäischen Union für eine entsprechende Regelung einsetzen. Anforderungen an die Dokumentation und Protokollierung werden auch über nationale Normungsgremien (in Deutschland zum Beispiel das DIN) etabliert. In dieser Hinsicht sollte auch die Bundesregierung aktiv werden.

Wie bewertet der vzbv die bisherige Umsetzung?

- Das KI-Weißbuch schlägt Pflichten zur Aufbewahrung von Daten und Aufzeichnungen vor. Im Falle einer Kontrolle sollen Entscheidungen von KI-Systemen damit zurückverfolgt und überprüft werden können. Die Pflicht zur Aufbewahrung und Dokumentation umfasst unter anderem: Informationen zu Trainingsdaten, Trainingsmethoden, Methoden für Programmierung, Training, Erprobung und Validierung der Systeme. Der vzbv bedauert, dass die Datensätze an sich nur in bestimmten Fällen vorgehalten werden sollen. Problematisch ist, dass aufgrund des vorgesehenen zu engen Anwendungsbereichs viele relevante Systeme nicht erfasst wären.
- Es ist zu begrüßen, dass die Bundesregierung gemeinsam mit dem DIN Projekte zur Entwicklung von Normungsroadmaps im Bereich KI initiiert hat. Diese beschäftigen sich auch mit dem Thema der Dokumentation und Protokollierung von Methoden, Programmabläufen und Datengrundlagen algorithmischer Systeme.

Bewertung



Die Empfehlung wurde/wird teilweise umgesetzt

Status:

Begonnen

10. Schaffung eines bundesweiten Kompetenzzentrums Algorithmische Systeme

Was empfiehlt die Datenethikkommission?

Die Datenethikkommission fordert die Schaffung eines bundesweiten Kompetenzzentrums Algorithmische Systeme. Dieses soll die bestehenden Aufsichtsbehörden unterstützen, vor allem durch methodisch-technischen Sachverstand. Insbesondere bei der Kontrolle, inwieweit algorithmische Systeme Recht und Gesetz einhalten (DEK-Forderung Nr. 56).

Warum ist das wichtig?

Die technisch-methodische Expertise, um die Rechtmäßigkeit und gesellschaftliche Auswirkungen algorithmischer Systeme nachvollziehen zu können, kann nicht bei allen Aufsichtsbehörden vorausgesetzt werden. Eine technisch versierte „Unterstützungseinheit“ ist nötig. Die Durchsetzung gesetzlicher Rahmenbedingungen würde damit weiter bei den bisher zuständigen Behörden liegen.

Wer muss die Empfehlung umsetzen?

Die Schaffung eines bundesweiten Kompetenzzentrums Algorithmische Systeme zur Unterstützung der nationalen Aufsichtsinstitutionen muss durch die Bundesregierung erfolgen.

Wie bewertet der vzbv die bisherige Umsetzung?

- Das KI-Weißbuch sieht eine europäische Governance-Struktur für KI vor. Diese soll aber vor allem die Koordination und Zusammenarbeit der nationalen und europäischen Aufsichtsbehörden unterstützen. Eine Unterstützung der Aufsichtsbehörden bei ihrer Aufsichtstätigkeit im Sinne der DEK ist leider nicht vorgesehen.
- Zwar kündigt die Bundesregierung in ihrer KI-Strategie an, die „Einrichtung beziehungsweise den Ausbau von staatlichen Stellen und privaten Prüfinstitutionen zur Kontrolle algorithmischer Entscheidungen“ zu prüfen. Bedauerlicherweise ist aber keine Initiative der Bundesregierung zur Schaffung eines bundesweiten Kompetenzzentrums Algorithmische Systeme im Sinne der DEK bekannt. Im Rahmen der KI-Strategie wurde zwar das „Observatorium Künstliche Intelligenz in Arbeit und Gesellschaft“ geschaffen. Eine direkte Unterstützung bestehender Aufsichtsbehörden lässt sich jedoch aus dessen Aufgabenbeschreibung nicht erkennen.

Bewertung



Die Empfehlung wurde/wird nicht umgesetzt

Status:

Nicht begonnen