Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

„Datenschutz und Künstliche Intelligenz – Regulierung von KI in Deutschland und der EU sowie aktuelle und künftige Einsatzgebiete von KI“

von MinDirig´n Tanja Jost
Abteilungsleiterin 2
beim Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit (BfDI)

4. TÜV Rheinland Datenschutzkonferenz

Hamburg

27. Oktober 2022

Es gilt das gesprochene Wort

Meine sehr geehrten Damen und Herren,

eigentlich war ja fest eingeplant, dass Herr Professor Kelber an dieser Stelle zu Ihnen sprechen sollte. Aber leider ist die internationale Datenschutzkonferenz in Istanbul dazwischengekommen, die vom Veranstalter um eine Woche verschoben wurde und bei der eine Teilnahme des BfDI´s als Mitglied des Exekutivkomitees zwingend ist.

Herr Professor Kelber hat mich daher gebeten, ihn an dieser Stelle vielmals zu entschuldigen und seinen Vortrag hier bei Ihnen zu übernehmen, was ich natürlich sehr gerne tue. Bevor ich beginne, möchte ich mich kurz vorstellen: Mein Name ist Tanja Jost und ich leite die Abteilung 2 des BfDI, die sich mit technologischem Datenschutz, Telekommunikation und Telemedien befasst.

I. [Einleitung]

Künstliche Intelligenz oder kurz KI ist vermutlich das Thema, das Datenschützerinnen und Datenschützer seit nunmehr vielen Jahren als DIE große Herausforderung der Zukunft bezeichnen. Und das vermutlich auch zurecht. KI ermöglicht uns Dinge, über die die Meisten von uns vor 20 Jahren noch nicht einmal nachgedacht haben. Viele sind sicherlich gut, andere haben zumindest einen faden Beigeschmack.

Vielleicht haben auch Sie in der letzten Woche mitbekommen, dass die französische Datenschutzaufsichtsbehörde CNIL die Firma Clearview AI mit einer Geldbuße in Höhe von 20 Millionen Euro belegt hat; dem höchstmöglichen Betrag für den ihr vorgeworfenen Datenschutzverstoß.

Wer noch nicht von Clearview AI gehört hat: Die Firma sammelt ohne Zustimmung der Betroffenen Fotos aus dem Internet – nach eigenen Angaben mittlerweile bereits mehr als 30 Milliarden Bilder – und trainiert damit eine KI-Gesichtssuchmaschine, die an Unternehmen und Sicherheitsbehörden vermarktet wird.

Die Geldbuße ist übrigens schon die vierte in diesem Jahr. Zusammen mit entsprechenden Strafen aus England, Italien und Griechenland beläuft sich die Gesamtsumme daher bereits auf rund 70 Millionen Euro.

Dieses Beispiel zeigt meines Erachtens sehr schön, was Künstliche Intelligenz für uns ausmachen kann. Zum einen übt sie eine wahnsinnige Faszination ob der bahnbrechenden neuen Möglichkeiten auf uns aus. Gleichermaßen stellt sie uns aber auch vor die große Herausforderung einen Weg zu finden, wie wir im Interesse der Allgemeinheit mit ihr umgehen müssen.

Ich möchte daher im Folgenden drei Fragen ansprechen, um das Thema ein wenig näher zu beleuchten:

1. Was verstehen wir eigentlich unter KI und wo und wie kann sie eingesetzt werden?
2. Was sind die gesellschaftlichen und vor allem datenschutzrechtlichen Risiken beim KI-Einsatz?

   und

3. Wie können oder sollten wir mit KI umgehen, um sie sicher nutzbar zu machen?

II. [Was ist KI?]

Lassen Sie uns zunächst den Begriff KI einmal etwas genauer betrachten.

Wenn man die Menschen auf der Straße fragt, was sie unter Künstlicher Intelligenz verstehen, wird vermutlich die Hauptantwort sein: „Ein wie ein Mensch selbstständig logisch denkender und sich kognitiv alleine weiterentwickelnder Computer“; oder einfacher: „Eine Maschine, die sich wie ein Mensch verhält“.

Tatsächlich ist diese sogenannte „starke KI“ nur ein kleiner Teil des Begriffs Künstliche Intelligenz und darüber hinaus auch der Teil, dessen praktische Umsetzung aktuell noch nicht wirklich absehbar ist.

Der in der Praxis weitaus relevantere Teil von KI ist der Versuch, Computer so zu programmieren, dass sie eigenständig Probleme bearbeiten und beispielsweise mittels maschinellem Lernen Lösungsmöglichkeiten entwickeln können. In der Regel erfolgt dies mittels Algorithmen, die es schaffen, in großen Datenmengen Muster zu erkennen und zu analysieren, um dann gegebenenfalls in einem weiteren Schritt basierend auf diesen Erkenntnissen Vorhersagen über die Wahrscheinlichkeit von Verhalten oder dem Eintreten von bestimmten Ereignissen zu treffen.

Interessanter als eine formelle Definition des Begriffs Künstlicher Intelligenz sind allerdings die allgemein unter KI zusammengefassten praktischen Ansätze, bei denen bereits heute an vielen Stellen Daten verarbeitet werden. Anwendungen im Bereich der Künstlichen Intelligenz, algorithmenbasierte Entscheidungsprozesse und lernende Systeme dringen in alle Lebensbereiche vor und bieten vielfach Lösungsansätze, die ohne KI kaum denkbar wären. Der Innovationswert, der sich aus solchen Anwendungen ergibt, ist dabei enorm.

Nehmen wir als Beispiel den medizinischen Bereich. Dort unterstützt KI Ärzte beispielsweise bei der Röntgendiagnostik. Computer schaffen es hier, Tumore in einem sehr frühen Stadium mit einer so hohen Trefferquote zu erkennen, wie sie nicht einmal von spezialisierten Fachärzten mit langjähriger Berufserfahrung erreicht werden kann.

Auch im Bereich der Chirurgie unterstützen Computer und Maschinen Mediziner bei komplexen Operationen, die vor wenigen Jahren entweder noch nicht einmal denkbar oder aber zumindest mit einem erheblich höheren Risiko verbunden waren.

Doch auch in unserem „gewöhnlichen“ Alltag begegnen wir mittlerweile regelmäßig KI-Anwendungen. Ich gehe fest davon aus, dass fast 100% der hier Anwesenden ein Smartphone in der Tasche haben. Vielleicht nicht ganz so viele nutzen bei diesem auch die Funktion der Sprachassistenz, die genauso ein Beispiel für Künstliche Intelligenz ist, wie die Suchmaschinen von Google, Startpage, Bing oder anderen Anbietern.

Weitere Beispiele sind Navigationssoftware mit Stauprognosen, Wettervorhersagen, Übersetzungssoftware, Smart Home Anwendungen und so weiter und so fort…

Allem gemein ist, dass KI eingesetzt werden soll, um unser Leben zu vereinfachen und damit besser zu machen. In den meisten Fällen, wie auch den gerade eben genannten Beispielen, scheint das – zumindest auf den ersten Blick – auch der Fall zu sein.

Auf den zweiten Blick zeigt sich dann allerdings nicht selten, dass die mit KI-Anwendungen in der Regel einhergehende Verbreitung von immer mehr Daten neben den unbestreitbaren Vorteilen auch neue Möglichkeiten für tiefgreifende Verletzungen von Grundrechten mit sich bringen kann.

Und das bringt uns dann auch schon zu unserer zweiten Frage: Was sind die gesellschaftlichen und datenschutzrechtlichen Risiken von Künstlicher Intelligenz?

III. [Was sind die Risiken von KI?]

KI-Systeme können die Freiheiten und Rechte natürlicher Personen in vielerlei Weise beeinträchtigen. Denn die vielen Vorteile, die KI mit sich bringt, basieren in der Regel auf der Auswertung von vielen und oft auch personenbeziehbaren Daten. Je nachdem wie KI eingesetzt wird, birgt sie damit das Potential für massive Grundrechtseinschränkungen und Diskriminierungen.

1. [Beispiele für „risikobehaftete“ KI]

Das wohl plakativste und drastischste Beispiel in diesem Kontext ist die staatliche Überwachung in der Volksrepublik China. Hier wurde ein totalitäres System digitaler Überwachung aufgebaut, das unter anderem auf einer weitreichenden Vernetzung von Videokameras basiert, die mit Gesichtserkennungstechnologien ausgestattet sind. Von der Gesichtsbiometrie über Iris-Scans und Stimm-Mitschnitte – je mehr Merkmale der Staat erlangt, desto genauer und schneller kann er Individuen erkennen. Darauf basierend wird dann mit Hilfe von KI auch das Social Scoring, ein gigantisches Kontrollsystem für die gesamte Bevölkerung, unterstützt.

Doch nicht nur, wo KI gezielt zur Unterdrückung und Diskriminierung von einzelnen oder Gruppen von Menschen missbraucht wird, besteht die Gefahr, dass ihr Einsatz auch unbeabsichtigt zu eben denselben Folgen führen kann.

Vor wenigen Jahren gab es beispielsweise einen groß angelegten Test der Bundespolizei am Berliner Bahnhof Südkreuz. Hier sollten verschiedene KI-Systeme getestet werden, die anhand biometrischer Gesichtserkennung Personen identifizieren sollten, die sich im Bereich der Bahnhofskameras bewegten.

Dass diese Technik noch nicht den Reifegrad entwickelt hat, der uns in Kinofilmen gerne suggeriert wird, zeigte sich dann auch bei der Auswertung der Ergebnisse: Das Beste der drei getesteten Systeme schaffte eine durchschnittliche Erkennungsquote von rund 65%.

Noch interessanter als dieser Wert war aber eine andere Zahl aus dem Abschlussbericht; nämlich die zur sogenannten Falschakzeptanzrate. Hierzu heißt es wörtlich:

„Unter Berücksichtigung eines Personenaufkommens von ca. 1.000 Personen/Stunde, das den Erfassungsbereich einer (intelligenten) Videokamera frequentiert, wären somit während der Betriebszeit des Bahnhofs drei bis vier falsch-positive Treffermeldungen pro Kamera und Stunde einzukalkulieren.“

Konkret bedeutet das, dass sich in einem Wirkbetrieb dieser KI-Anwendung wegen ihrer Fehlerhaftigkeit je nach Personenaufkommen täglich eine zwei- bis dreistellige Zahl an unschuldigen Personen einer möglichen repressiven polizeilichen Maßnahme ausgesetzt sehen könnte, weil die KI sie mit jemand anderem verwechselt hat.

Wenn man dann noch dazu nimmt, dass die Fehlerkennungen überproportional weibliche Personen mit einem ethnischen Hintergrund betreffen, kommen wir nicht umhin zu sagen, dass auch KI faktisch diskriminieren kann.

Ein weiteres Beispiel ist der Einsatz von Künstlicher Intelligenz im Beschäftigtenumfeld. Hier können Arbeitgeberinnnen und Arbeitgeber auch schon heute KI bzw. algorithmische Systeme in verschiedenen Bereichen einsetzen. So gibt es beispielsweise Angebote zur Unterstützung bei der Personalauswahl.

Diese algorithmenbasierten Auswahlverfahren funktionieren, indem unter anderem die schriftlichen Bewerbungsschreiben und Lebensläufe abgeglichen bzw. auf bestimmte Schlüsselwörter hin analysiert werden. Ebenso können Sprach- oder Videoaufnahmen von Bewerberinnen und Bewerbern in Jobinterviews hinsichtlich bestimmter Kriterien ausgewertet werden.

Dabei muss sich die aus dem Einsatz der KI ergebende Diskriminierung nicht einmal gezielt sein. Oft besteht das Problem einfach in der fehlenden Transparenz der von der KI verwendeten Maßstäbe. Denn nicht selten kommt es vor, dass das System aus den Daten, mit denen es trainiert wurde, die falschen Schlüsse zieht. Bei einem Bewerbungsprozess des Konzerns Amazon stellte sich beispielsweise nachträglich heraus, dass Frauen aus dem Bewerberpool aussortiert wurden, da die KI den Umstand, dass im Vorfeld mehr Männer eingestellt wurden, falsch interpretiert hatte und sich so die Diskriminierungsmuster noch weiter verstärkten.

2. [Datenquellen und Verarbeitungsprozesse]

Hier zeigt sich dann auch ein weiterer Schwachpunkt – oder vielleicht sagen wir besser ein weiteres Risiko – der KI. Genauso wichtig wie die eigentlichen KI-Algorithmen sind die Daten, die für das Training einer KI genutzt werden. Erfolgt hier eine falsche Auswahl der Daten, kann dies weitreichende Folgen haben. Denn wie ich bereits eingangs erwähnt habe, dient Künstliche Intelligenz vor allem dazu, riesige Datenmengen zu durchsuchen und zu analysieren um – teils selbstlernend – aus ihnen Schlüsse zu ziehen und darauf basierend Entscheidungen zu treffen.

Gerade weil KI vor allem Möglichkeiten schafft, um riesige Datenmengen sinnvoll verarbeiten zu können, rücken zudem Fragen des Datenzugangs als Grundlage für einen KI-Einsatzes immer mehr in den Vordergrund. Teilweise wird mittlerweile sogar eine sogenannte „Kultur des Datenteilens“ beschworen. Das ist aber gerade aus datenschutzrechtlicher Sicht ein bedeutender Narrativwechsel.

Für den Bereich der nicht-personenbezogenen Daten mag dieses Narrativ auf den ersten Blick problemlos erscheinen. Doch bei genauerem Hinsehen stellen wir auch hier fest, dass bei weitem nicht alles schwarz und weiß gesehen werden kann. Denn im Zeitalter von Big Data wird es immer schwerer von wirklichen rein anonymen Daten zu sprechen.

Auch anonyme Datenbestände sind veränderlich. Durch Kombination mit weiteren Daten, die nicht zuletzt durch das Internet mannigfaltig vorhanden und leicht zugänglich sind, kann eine Re-Personalisierung in vielen Fällen zumindest nicht mehr vollständig ausgeschlossen werden. Ironischerweise sind es dann auch gerade KI-Anwendungen, die genutzt werden, um entspreche Datenbündelungen vorzunehmen und diese dann wieder als Datenquelle für weitere Prozesse zu verwenden.

Für die einen mag es darum gehen, Daten und die mit ihnen erschließbaren Informationen aus den sogenannten Datensilos zu befreien. Für Datenschützer geht es hingegen um Datenbestände, die erst durch die Wahrung des Gebots der Zweckbindung im Sinne der Betroffenen steuerbar und kontrollierbar werden.

Gerade dieser elementare datenschutzrechtliche Grundsatz ist aber bei vielen Anwendungen der Künstlichen Intelligenz in der Praxis nur schwer nachvollziehbar.

Bei speziell für das Training von KI-Systemen erhobenen personenbezogenen Daten stellt sich zudem die Frage nach der adäquaten Rechtsgrundlage für ihre Erhebung.

Nehmen wir das Beispiel von Notbremsassistenten in modernen Autos und Bussen. Es ist schon lange bekannt, dass Notbremsassistenten einen signifikant positiven Einfluss auf die Unfallstatistik haben. Ihre Entwicklung ist also grundsätzlich im Interesse der Allgemeinheit und damit auch grundsätzlich geeignet, bei der Abwägung berechtigter Interessen ein überwiegendes Interesse auf Seiten der Hersteller zu begründen.

Das im Auge zu haben ist wichtig vor dem Hintergrund, dass viele der Fahrassistenten in hohem Maß auf der Auswertung von Daten aus Video- und Audiosensoren beruhen. Im Rahmen der Entwicklung einer KI-basierten Fahrfunktion werden mit Testfahrzeugen nach Aussagen der Hersteller etwa eine Million Kilometer an Entwicklungsfahrten geleistet, um möglichst umfassend Video- und Audiodaten aus konkreten Verkehrssituationen aufzuzeichnen, die dann in den Entwicklungsstätten der Hersteller oder ihrer Zulieferer für das Training der speziellen Fahrfunktion auf Basis der speziellen Sensoren verwendet werden.

Würde man das Bildmaterial mit personenbezogenen Daten, wie Autokennzeichen oder Gesichtern von Personen verpixeln, bestünde das Risiko einer geringeren Funktionssicherheit. Das ist aber nicht hinnehmbar, wenn man die Verkehrssicherheit nicht gefährden will.

Ebenso ist es problematisch, datenschutzrechtlich sensible Bereiche, wie die Umgebung von Krankenhäusern, Kirchen, Schulen, Kindergärten, Spielplätzen usw. bei den Entwicklungsfahrten auszusparen, weil dann die Trainingsdaten nicht umfassend genug sein würden, um auch in diesen Bereichen eine sichere Funktion zu gewährleisten.

Es entsteht also im Rahmen der Entwicklung – und zwar nicht nur in diesem Beispiel – mit großer Wahrscheinlichkeit ein datenschutzrechtlich sensibler Datenbestand mit einem entsprechend hohen Schutzbedarf. Hier muss sichergestellt werden, dass die Entwickler die erforderlichen technisch-organisatorischen Maßnahmen auch durchführen, um eine zweckfremde Verwendung der Daten durch Unbefugte soweit wie möglich auszuschließen. Daten die nicht mehr erforderlich sind, müssen konsequent gelöscht werden und die betroffenen Personen müssen bestmöglich über die Verarbeitung ihrer Daten informiert werden, um deren Betroffenenrechte zu wahren.

3. [unerkannte Datenverarbeitung]

Ein wesentliches datenschutzrechtliches Risiko von KI-Systemen ist also die in vielen Fällen mangelnde Transparenz der mit Ihnen verbundenen Datenverarbeitungsprozesse.

Im eben erwähnten Beispiel der Fahrassistenten registriert man als Passant wohlmöglich gar nicht, dass man videographisch erfasst wird. Doch auch dort, wo Menschen selbst den Anlass dafür setzen, dass ihre personenbezogenen Daten von Künstlicher Intelligenz verarbeitet werden, ist ihnen dieser Umstand in vielen Fällen gar nicht bewusst.

Ein klassisches Beispiel hierfür ist die Profilbildung bei der Nutzung sozialer Netzwerke. Selbst wenn man penibel darauf achtet, wie dort die Privatsphäre-Einstellungen gewählt wurden und was man im Internet preisgibt, kann man nicht unbedingt verhindern, dass mitunter massenhaft Daten über einen gesammelt werden, ohne es überhaupt zu bemerken.

Unternehmen wie Facebook und Co. werten nicht nur das aus, was wir als Bilder posten oder im Netzwerk schreiben. Sie analysieren zum Beispiel auch, wie wir schreiben. Algorithmen bewerten anhand unserer Tippgeschwindigkeit und der Art, wie wir tippen (also z.B. ob wir viele Fehler machen oder Worte und Satzteile immer wieder neu formulieren), wie unsere aktuelle Stimmungslage ist. Sind wir erregt und verärgert, oder traurig oder depressiv… der Algorithmus findet es heraus und das Unternehmen lässt es in das Profil einfließen, das es über jeden seiner

Nutzerinnen und Nutzer anlegt (und eventuell auch über die, die die Plattform nicht nutzen).

Die Profile der Unternehmen werden dabei so aussagekräftig, dass sie ein ziemlich genaues Bild unseres Lebens wiederspiegeln. Das beschränkt sich nicht nur auf Informationen, wo wir wohnen und uns gerne in unserer Freizeit aufhalten, was wir am liebsten essen und was unsere Hobbies sind oder wo wir gerne einmal Urlaub machen würden.

In den Datenbanken schlummern auch Informationen, die wir vielleicht nicht einmal mit unseren engsten Freunden oder Verwandten teilen würden, z.B. unsere politische Einstellung, depressive Gedanken oder Angstzustände, oder potentielle Krankheiten. Alles zusammengestellt von einem Algorithmus, der unsere Posts, Internetrecherchen, Webseitenbesuche und eben Dinge wie die Tippgeschwindigkeit auswertet.

Ein weiteres Beispiel, das ich allerdings nur kurz anreißen möchte, sind die von mir ebenfalls bereits erwähnten Sprachassistenten. Vor wenigen Jahren war die Empörung groß, als sich herausstellte, dass diese zum einen viel mehr Gespräche und Daten erfassen als die meisten gedacht haben und zum anderen diese Audiodateien nicht nur genutzt wurden, um den mit Ihnen übermittelten Befehl auszuführen und danach gelöscht wurden.

Vielmehr wurde bekannt, dass Aufzeichnungen der auch unbewusst erstellten Gesprächsmitschnitte, die mitunter höchstintime Inhalte betrafen, gespeichert und von Mitarbeiterinnen und Mitarbeitern der Unternehmen „zur Verbesserung ihres Angebots“ manuell abgetippt und ausgewertet wurden.

Trotzdem ist die Zahl der Alexas und Co. in den Wohn- und Schlafzimmern dadurch nicht zurückgegangen. Die KI sammelt weiter fleißig Daten und erstellt daraus Profile, die immer detaillierter und aussagekräftiger werden.

4. [Vermessung der Gesellschaft]

Das bringt mich zu einem letzten Risiko der Künstlichen Intelligenz, dass ich heute ansprechen möchte: die Durchklassifizierung der Gesellschaft.

Und hierbei schließt sich wieder der Kreis zu meinem ersten Beispiel, dem Social Scoring in China. Damit will ich um Gottes Willen nicht andeuten, dass wir auf einem ähnlichen Weg sind. Allerdings müssen wir uns bewusst sein, dass die KI auch hier bei uns die Möglichkeiten geschaffen hat, uns in Gruppen einzuteilen.

Anders als in China erfolgt diese Klassifizierung nicht durch den Staat, sondern überwiegend durch große privatwirtschaftliche Unternehmen, die wie eben dargestellt, jede Gelegenheit nutzen, unsere Daten zu erheben und zusammenzuführen.

Warum? … Daten bedeuten Informationen und Wissen und daraus wiederum kann man letztendlich Profit schlagen. Denn noch relevanter als die konkreten Daten des Einzelnen ist die Vergleichbarkeit dieser Daten mit denen von anderen Menschen und die sich daraus ergebende Möglichkeit, möglichst ausspezifizierte Schulbladen zu bilden, in die jeder Mensch einsortiert werden kann.

Wie detailliert diese Kategorien sind, kann man erkennen, wenn man sich einmal die Angebote von Datenhändlern – oder „Cloud Based Analytics Anbieter“, wie sie sich oft gerne bezeichnen – anschaut. Hier finden sich hunderte von Klassifizierungen, wie zum Beispiel „anspruchsvolle Singles“, „einflussreiche Paare“, „Eintopf und Camping“, „Golfspieler und Gourmets“ oder „Kinder und Wein“. Die Gruppe „paranoide Datenschützer“ habe ich zwar noch nicht gefunden, aber wer weiß…

Das mag auf den ersten Blick vielleicht amüsant klingen. Faktisch zeigt es aber, dass wir alle mit Unterstützung der KI in eben solche Schubladen sortiert werden.

Sie alle hier haben in irgendeiner Weise eine gewisse Datenschutzaffinität, sonst wären Sie nicht hier. Daraus kann man schließen, dass zumindest viele von Ihnen sich zumindest der Grundproblematik bewusst sind. Einige nutzen vielleicht sogar gar keine Soziale Medien und wähnen sich damit auf der sicheren Seite.

Leider steht zu befürchten, dass auch Sie nicht darum herumkommen werden, von der KI in eine möglichst passende Schublade einsortiert zu werden und eventuell dadurch gewissermaßen in eine Art „Sippenhaft“ genommen zu werden, auch wenn Sie eigentlich gerade nicht den Stereotyp ihrer Kategorie darstellen. Im besten Fall hat das keine unmittelbaren Auswirkungen. Aber vielleicht entscheidet auch irgendwann einmal ihre Versicherung, dass die Gruppe, in die Sie einsortiert wurden, aufgrund ihres Verhaltens ein höheres Risiko für Schadenseintritte aufweist und erhöht deshalb Ihren Versicherungsbeitrag, unabhängig davon, dass diese „Schadensgeneigtheit“ bei Ihnen selbst gar nicht gegeben ist.

5. [Zwischenfazit]

Wir sehen also: Künstliche Intelligenz hat bei allen Vorzügen, die sie unbestritten mit sich bringt, mitunter auch Nebenwirkungen, die ein nicht unerhebliches Risiko für die Grundrechte der Bürgerinnen und Bürger darstellen können.

Das bedeutet natürlich nicht, dass man sicherheitshalber der KI den Rücken kehren sollte. Ein solcher Vorschlag wäre weder realistisch noch sinnvoll und zukunftsorientiert. Allerdings ist es eine zentrale gesellschaftliche und politische Aufgabe, die Technologie so zu gestalten, dass sie den Menschen und seine Rechte in den Mittelpunkt stellt und dabei gleichzeitig innovative Entwicklungen und einen breiten Einsatz in vielen Bereichen ermöglicht.

Und das bringt mich zu meiner dritten und letzten Frage: Wie sollen wir mit Künstlicher Intelligenz umgehen?

IV.[Wie sollten wir mit KI umgehen?]

Vorangestellt werden muss die Tatsache, dass schon jetzt KI zumindest in Teilen von der bestehenden Gesetzgebung reguliert wird – allen voran von der DSGVO. Gleichwohl bedarf es nach einhelliger Meinung in diesem Bereich ein großes Bedürfnis nach weitergehender spezifischer Regulierung.

1. [AI Act]

Vor diesem Hintergrund ist es erfreulich, dass auf EU-Ebene aktuell der Entwurf eines Artificial Intelligence Act (oder kurz AI Act) mit möglichen Vorgaben einer EU-Regulierung im Bereich der KI diskutiert wird. Dieser soll einen wesentlichen Beitrag dazu leisten, dass in der EU angewendete KI-Systeme künftig zuverlässig und vertrauenswürdig sind.

Damit gehen natürlich auch Bedenken (vor allem aus der Wirtschaft) einher, dass die Verordnung die Entwicklung von KI-Anwendungen und damit digitalen Fortschritt und Innovationen ausbremsen könnte. Den Begriff der Regulierung mit dem der Verhinderung gleichzusetzen, geht aber am Kern an der Sache vorbei.

Ganz im Gegenteil: Solide Vorgaben und ein sicherer Rechtsrahmen für die Entwicklung und den Einsatz von KI-Anwendungen führen für alle Akteure, insbesondere aber auch für Wirtschaft und Wissenschaft, zu der Planbarkeit und einem zuverlässigen Entwicklungsumfeld, das von dort seit langer Zeit gefordert wird.

Mit dem Entwurf des AI Act verfolgt die Kommission einen risikobasierten Ansatz, der für Anwendungen, die mit einem hohen Risiko einhergehen, bestimmte Qualitätsanforderungen vorsieht, wie etwa Protokollierungs- und Dokumentationsvorgaben, eine weitreichende Information der Nutzer, eine hohe Qualität der Datensätze oder auch eine menschliche Aufsicht zur Minimierung der Risiken. Dabei sind immer noch ausbaufähige Bereiche erkennbar, zumindest wird aber eine erste Grundlage für einen wirkungsvollen Regulierungsansatz geschaffen.

Allen Akteuren auf diesem Feld muss außerdem bewusst sein, dass KI-Anwendungen einen hochdynamischen Regulierungsrahmen erfordern, weil die Entwicklungen derart schnell voranschreiten, dass die bislang bewährten Regelungsmechanismen kaum Schritt halten können. Wie man dieser Dynamik aus regulatorischer Sicht und mit Blick auf den Aspekt der Innovationsförderung gerecht werden kann, das ist eine der großen Herausforderungen, vor der wir aktuell stehen.

Doch auch jenseits von Gesetzesvorhaben beschäftigen sich schon seit mehreren Jahren Datenschutzbehörden weltweit mit der Frage, wie man den datenschutzrechtlichen Herausforderungen der Künstlichen Intelligenz am besten begegnen kann.

2. [Hambacher Erklärung]

In Deutschland beispielsweise hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder mit ihrer Hambacher Erklärung eine Entschließung vorgelegt, in der datenschutzrechtliche Anforderungen, die beim Einsatz von KI erfüllt sein müssen, dargestellt werden.

Dazu gehören u. a. ein hohes Maß an Transparenz und Nachvollziehbarkeit der Ergebnisse und der Prozesse maschinengesteuerter Entscheidungen, der Grundsatz der Datenminimierung, die Einhaltung der Zweckbindung, aber auch die Vermeidung von Diskriminierungen und die klare Zurechnung von Verantwortlichkeiten.

3. [Datenethikkommission]

Auch die von der Bundesregierung eingesetzte Datenethikkommission, in der auch der BfDI Mitglied war, hat sich mit dem Thema KI auseinandergesetzt und dabei unter anderem gefordert, dass jegliche Nutzung von personenbezogenen Daten im KI-Bereich ethisch vertretbar sein sollte.

Um dies zu gewährleisten, regte die Kommission an, Maßnahmen gegen die Nutzung von KI für Zwecke der Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, sowie eine dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen zu ergreifen. Darüber hinaus sollte die Verwendung von personenbezogenen Daten bei KI Systemen im Rahmen personalisierter Risikoeinschätzung an enge Voraussetzungen geknüpft werden.

4. [EDSA]

Auf europäischer Ebene hat sich der Europäische Datenschutz-ausschuss gemeinsam mit dem Europäischen Datenschutzbeauftragten in einer Stellungnahme zum Entwurf des eben angesprochenen AI Acts ausführlich mit dem Thema KI auseinandergesetzt. Dabei hat er sich vor allem ausführlich zu KI-Systemen zur biometrischen Videoüberwachung positioniert und klargestellt, dass diese der grundsätzlichen Erwartung aller billig und gerecht denkenden Menschen widerspreche, im öffentlichen Raum anonym zu bleiben.

Um diese erhebliche Gefährdung von Grundrechten zu vermeiden, sollte ein allgemeines Verbot der Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen in öffentlich zugänglichen Räumen in Betracht gezogen werden. Ein solches Verbot sollte die Erfassung sämtlicher physischer Merkmale im weitesten Sinne, wie zum Beispiel Gesichtszüge, aber auch Gangart, Fingerabdrücke, DNA, Stimme, Tastenanschlagsmuster und andere biometrische Merkmale oder Verhaltenssignale, beinhalten.

Aufgrund ähnlicher Erwägungen sollte die Verwendung von KI zur Erkennung von Emotionen natürlicher Personen ebenso verboten werden.

Darüber hinaus sollte ein Verbot auch für solche KI-Systeme in Betracht gezogen werden, die natürliche Personen nach biometrischen Merkmalen in Cluster eingruppieren. Andernfalls bestünde die Gefahr, dass Menschen nach ethnischer Zugehörigkeit, Geschlecht, politischer oder sexueller Orientierung oder sonstigen Merkmalen, die zu den gemäß Artikel 21 der Charta der Grundrechte der Europäischen Union verbotenen Diskriminierungsgründen zählen, gruppiert werden.

V. [Schluss]

Sie sehen, meinen Damen und Herren, dass in dem Thema bereits einiges in Bewegung ist. Und das ist auch gut so, weil es schlichtweg dringend erforderlich ist.

Künstliche Intelligenz ist eine Schlüsseltechnologie, die gerade erst begonnen hat, unser Leben grundlegend zu verändern. Nicht wenige denken, dass sie unsere Gesellschaft ähnlich stark verändern wird, wie einst der Übergang zum auf fossilen Brennstoffen basierenden Maschinenzeitalter im 18. und 19.Jahrhundert. Es steht uns also etwas Großes bevor.

Wir stehen erst am Anfang dieses Wandels. Viele potenzielle Anwendungen stecken noch in den Kinderschuhen. Ich denke, wir sind gut beraten, die Chancen und Risiken dieser Entwicklung differenziert zu betrachten. Die Datenschutzbehörden sollten dazu beitragen, kluge Handlungsempfehlungen für die Zukunft zu unterstützen und das Thema insgesamt eng begleiten.

Dabei muss es unser Ziel sein, Innovationen zu fördern und dabei den bestmöglichen Datenschutz zu gewährleisten.

Ich danke Ihnen für Ihre Aufmerksamkeit.