817/J XXVI. GP

Eingelangt am 14.05.2018

Anfrage

der Abgeordneten Stephanie Cox, Kolleginnen und Kollegen

an den Bundesminister für Landesverteidigung

betreffend Anwendung von „Artificial Intelligence“ zur Unterstützung und Automatisierung von Entscheidungen („automated decision systems“)

BEGRÜNDUNG

Mit „Artificial Intelligence“ Entscheidungen (teilweise) automatisieren

Angesichts der schier unbegrenzten Ressourcen, die aktuell in die Entwicklung immer komplexerer Algorithmen fließen - Moores Gesetz, das scheinbar unbegrenzte Rechenleistung verspricht - und der fortschreitenden Digitalisierung unserer Gesellschaft, durch die in den letzten 2 Jahren mehr Daten erzeugt wurden als in allen Jahren zuvor, kann Software heute kognitive Leistungen erbringen, von denen man vor ein paar Jahren noch dachte, dass sie Menschen vorbehalten sind. Es verwundert also nicht, dass auf globaler Ebene eine Debatte über die Regulierung von „Artificial Intelligence“ („AI“) aufgekommen ist - nicht zuletzt wegen der kritischen Äußerungen des PayPal-, Tesla- und SpaceX-Gründers Elon Musk. Führende „AI- Forscher_Innen“ und in diesem Bereich tätige Unternehmer_Innen sorgen sich jedoch weniger um eine apokalyptische Zukunft à la „Terminator“, als um die (teilweise) Automatisierung von Entscheidung durch AI und die damit verbundene Verantwortungsübergabe an „Maschinen“.

Die Regierungsparteien haben Recht, wenn sie im Regierungsprogramm schreiben: „Neue digitale Technologien wie künstliche Intelligenz [...] werden noch nicht vorhersehbare Auswirkungen auf unsere Gesellschaft haben.“ (S. 58) Darum ist es notwendig darüber nachzudenken, wie unsere Gesellschaft mit dieser neuen Technologie umgehen wird, damit diese zum Vorteil der Gesellschaft genützt und nicht etwa missbraucht wird, um Vorurteile und bestehende Ungleichheiten in unserer Gesellschaft weiter zu verhärten.

Einerseits bietet der Einsatz von „AI“ große Vorteile, die auch für den Einsatz im öffentlichen Bereich sprechen. Insofern sind die Pläne der Regierungsparteien („Definition von Pilotprojekten in Zusammenarbeit mit der Wirtschaft, um die Umsetzung der digitalen Transformation in der öffentlichen Verwaltung zu fördern (künstliche Intelligenz etc.)“ [siehe Seite 81 im Regierungsprogramm]) zu begrüßen.

Gefahren beim Einsatz von „Artificial Intelligence“

Es gibt aber auch Herausforderungen beim Einsatz von AI. Dies gilt besonders für den Staat und öffentliche Einrichtungen, in deren Wirkungskreis oft sensible Lebensbereiche fallen. Hier einige der Gefahren beim Einsatz von AI:

1. „AI“ funktioniert nur dank einer großen Anzahl von Daten, auf deren Basis Algorithmen mit statischen Modellen Muster erkennen. Diese Daten transportieren notwendigerweise auch unsachliche Vorurteile (z.B. weil Sie aus menschlichen Entscheidungen abgeleitet wurden, die nicht (immer) objektiv sind). Man spricht in diesem Zusammenhang auch von „Algorithmic Bias“. Im Ergebnis kann das dazu führen, dass Algorithmen Entscheidungen vorschlagen oder treffen, die unsachlich oder sogar rechts- bzw. verfassungswidrig sind. (Ein bekanntes Beispiel, das dieses Problem illustriert, war etwa Microsofts Twitterbot ,,@TayandYou“, der durch die Interaktion mit anderen Twitternutzern innerhalb eines Tages nur noch rassistische Äußerungen von sich gab.)
2. Der Erfolg eines Algorithmus hängt immer von der Perspektive ab, d.h. man kann einen Algorithmus nur danach beurteilen, ob er ein bestimmtes Ziel erfüllt. Das bedeutet nicht nur, dass die Festlegung des Ziels (durch Menschen) zentral für die Funktionsweise eines Algorithmus ist, sondern auch, dass AI nicht ideologiefrei funktioniert.
3. „AI“ hat „blinde Flecken“, denn die grundlegenden mathematischen Modelle sind nichts weiter als vereinfachte Darstellungen bzw. Annahmen der Realität. Insofern ist „AI“ auch nicht unfehlbar.
4. Besonders problematisch ist aber, dass die meisten Algorithmen (noch) „Black Boxes“ sind, d.h. dass weder sie, noch ihre Schöpfer_Innen erklären können, wie Algorithmen zu ihren Ergebnissen kommen. AI kann sich also weder rechtfertigen, noch Verantwortung übernehmen.

Der Staat bzw. öffentliche Einrichtungen müssen sich also gut überlegen wo und wie sie AI bzw. Software, die Entscheidungen (teilweise) automatisiert („automated decision systems“) einsetzt und wie die Wirkung dieser Technologie überprüft werden kann.
Aufgrund der Neuheit der Technologie ist klar, dass nicht alle Regierungen und öffentlichen Einrichtungen sich bereits intensiv mit diesen Problemen auseinandersetzen konnten. Darum hat das „AI Now Institute“ im April 2018 ein „Framework“ für „Algorithmic Impact Assessments“ veröffentlicht.[1] Die Idee ist, Regierungen bei der großen Herausforderung, „automated decision systems" im öffentlichen Bereich zu implementieren, zu unterstützen.

Die unterfertigenden Abgeordneten stellen daher folgende

Anfrage

1. Wie definieren Sie in Ihrem Ministerium Technologien, die Entscheidungen (teilweise) automatisieren („automated decision systems“)?[2]

[1] Download unter: https://ainowinstitute.org/aiareport2018.pdf.
[2] Es ist notwendig diesen Begriff zu definieren und zwar in praxisrelevanter und angemessener Art und Weise, insb. im Hinblick auf den jeweiligen Anwendungskontext, damit die folgenden Fragen beantwortet werden können. Die Definition sollte nicht zu weit (wodurch z.B. jede Art von Software subsumierbar wäre) oder zu eng gefasst sein (und damit Technologien ausklammern, die eigentlich überprüft werden sollten). Ein Beispiel für die Definition eines solchen „automated decision systems", das sich auf individuelles „Profiling" (,,individual profiling“) beschränkt, findet sich in Art. 4 Z 4 der DSGVO.

2. Nutzt Ihr Ministerium bereits entsprechende Technologien, die Entscheidungen (teilweise) automatisieren?

    a. Falls ja, welche Technologien, werden in welchen Bereichen auf welche Art und Weise genützt?

    b. Falls ja, werden diese Technologien laufend überwacht, evaluiert und die Ergebnisse der Evaluierung veröffentlicht?

        i. Falls ja, wie bzw. mit welchen Methoden wird überwacht und evaluiert?

        ii. Falls nein: Weshalb nicht?

    c. Falls ja, mit welchen Organisationen wurde zusammengearbeitet, um diese Technologien zu implementieren (z.B. Softwarehersteller, Consultingdienstleister)? (Bitte um abschließende Aufzählung aller beteiligten Organisationen, inkl. Umschreibung ihrer Aufgaben und Leistungen)

    d. Wurden alle Leistungen, die im Zusammenhang mit der Implementierung solcher Technologien eingeholt wurden, öffentlich ausgeschrieben?

        i. Falls ja, bitte um Auflistung der Organisationen, Technologie und Datum/Zeitraum.

        ii. Falls nein, weshalb nein?

    e. Falls ja, wie bzw. aus welchen Mitteln wurde die Herstellung und Implementierung dieser Technologien finanziert? (Bitte um abschließende Auflistung aller angefallenen Kosten je beteiligter Organisation sowie für die jeweiligen erbrachten Leistungen).

    f. Falls nein, ist der Einsatz solcher Technologien künftig geplant?

        i. Falls ja, welche Technologien sollen künftig in welchen Bereichen auf welche Art und Weise genützt werden und wann sollen diese eingeführt werden?

3. Haben Sie es in Fällen, in denen entsprechende Technologien bereits eingeführt wurden, unternommen bzw. planen Sie vor jeder künftigen Einführung solcher Technologien,

    a. die Öffentlichkeit zeitgerecht und umfassend über die verwendete Technologie, deren Anwendungsbereiche und geschätzte Auswirkungen auf die Gesellschaft zu informieren?

        i. Falls ja, welche Informationsmaßnahmen wollen Sie setzen?

        ii. Falls nein, wieso nicht?

    b. der Öffentlichkeit im Rahmen eines Einbeziehungsprozesses („review process“) die Möglichkeit zu geben, Bedenken zu äußern, und diese aufzuklären?

        i. Falls ja, wie soll der „review process“ ausgestaltet sein?

ii. Falls nein, wieso nicht?

c. solche Technologien, deren Anwendung und Wirkung ex ante durch MitarbeiterInnen im Ministerium im Rahmen eines transparenten Prozesses evaluieren zu lassen und die Ergebnisse der Evaluierung zu veröffentlichen?

i. Falls ja, wie soll eine solche Evaluierung ausgestaltet sein?

ii. Falls nein, wieso nicht?

d. solche Technologien, deren Anwendung und Wirkung ex ante von der Öffentlichkeit sowie von externen Experten evaluieren zu lassen und die Ergebnisse der Evaluierung zu veröffentlichen?

i. Falls ja, wie soll eine solche Evaluierung ausgestaltet sein?

ii. Falls nein, wieso nicht?

e. solche Technologien und deren Wirkungen laufend durch MitarbeiterInnen im Ministerium zu überwachen und in regelmäßigen Abständen zu evaluieren und die Ergebnisse der Evaluierung zu veröffentlichen?

i. Falls ja, wie soll eine solche Evaluierung ausgestaltet sein?

ii. Falls nein, wieso nicht?

f. solche Technologien und deren Wirkungen in regelmäßigen Abständen durch externe Experten evaluieren zu lassen und die Ergebnisse der Evaluierung zu veröffentlichen?

i. Falls ja, wie soll eine solche Evaluierung ausgestaltet sein?

ii. Falls nein, wieso nicht?

4. Mit welchen (aktiven) Maßnahmen wollen Sie verhindern, dass entsprechende Technologien (unsachliche) Vorurteile („bias“) transportieren, und wann sollen diese Maßnahmen gesetzt werden?

5. Wie planen Sie Algorithmen nach Kriterien wie „Fairness“ oder „Gerechtigkeit“ zu evaluieren?

6. Wie planen Sie, Expert_Innen mit einschlägigem Fachwissen zu finden und zu beurteilen, ob die jeweiligen Experten über einschlägiges Fachwissen verfügen?

7. Zur effektiven Evaluierung von Algorithmen wird es unter Umständen nötig sein, Trainingsdaten oder vergangene Entscheidungen offen zu legen. Welche Herausforderungen sehen Sie im Falle der Einbeziehung der Öffentlichkeit und von externen Experten (insb. im Hinblick auf die Wahrung von Grundrechten)?

8. Welche Herausforderungen sehen Sie im Zusammenhang mit der Ausschreibung und Vergabe von Leistungen zur Implementierung von „automated decision systems“ (z.B. Betriebsgeheimnisse der Lieferanten) insb. im Zusammenhang mit der Einführung von Kontroll- oder Evaluierungsmaßnahmen - wie in dieser

Anfrage aufgeführt - und wie wollen Sie diesen Herausforderungen begegnen?

9. Planen Sie Prozesse oder Gremien einzuführen, um Einzelpersonen und anderen Rechtssubjekten die Möglichkeit zu geben, in effektiver Weise gegen sie betreffende automatisierte Entscheidungen in Ihrem Wirkungsbereich vorzugehen?

    a. Falls ja, wie sollen solche Prozesse und/oder Gremien ausgestaltet sein?

    b. Falls nein, wieso nicht?

10. Wird Ihr Ministerium der Regierung vorschlagen ein Gesetz zu verfassen, das u.a. sicherstellt, dass jedes Ministerium bzw. jede öffentliche Einrichtung

    a. Technologien definieren muss, die in ihrem Wirkungsbereich Entscheidungen (teilweise) automatisieren („automated decision systems“) und diese Definitionen ggf. laufend aktualisieren (z.B. bei Änderung des Anwendungskontextes) und veröffentlichen muss?

    b. vor, spätestens jedoch unmittelbar nach der Anschaffung solcher Technologien, die Öffentlichkeit umfassend über die verwendete Technologie, deren Anwendungsbereiche, Ziele und geschätzte Auswirkungen auf die Gesellschaft informieren muss?

    c. diese Technologien laufend überwachen, evaluieren und die Ergebnisse der Evaluierung veröffentlichen muss?

    d. der Öffentlichkeit im Rahmen eines Einbeziehungsprozesses („review process“) die Möglichkeit geben muss, Bedenken zu äußern und diese aufzuklären?

    e. solche Technologien, deren Anwendung und Wirkung intern sowie durch externe Experten, im Rahmen eines transparenten Prozesses evaluieren lassen muss?

    f. verpflichtet wird sicherzustellen, dass Einzelpersonen und andere Rechtssubjekte effektiven Rechtsschutz genießen, wenn sie in negativer Weise durch (teilweise) automatisierte Entscheidungen betroffen sind?

    (Bitte um getrennte Beantwortung für jeden der obigen Punkte a. bis f.)

    g. Falls unter a. bis f. mit Nein geantwortet wurde: Wieso nicht? (Bitte um getrennte Beantwortung für jede Verneinung der obigen Punkte a. - f.)