Policy Sheet Europawahl 2019

KÜNSTLICHE INTELLIGENZ

Vertrauen in KI-basierte Systeme und Produkte schaffen!

Wenngleich Künstliche Intelligenz (KI) wissenschaftlich betrachtet kein neues Phänomen ist, so ist das politische Interesse an dem Thema in den letzten Jahren signifikant gestiegen. Durch den wachsenden Einsatz dringen KI-basierte Systeme immer stärker in die verschiedenen Lebensbereiche der Bürgerinnen und Bürger vor. Dabei eröffnen sich neben den Chancen dieser Technik, die es zu nutzen gilt, aber auch Risiken, welche beherrschbar gemacht werden müssen. So kann die KI Auswirkungen auf die Privatsphäre haben, haftungsrelevante Fragestellungen aufwerfen, und die Autonomie der Nutzer einschränken. Es werden große Datenmengen generiert, genutzt und ausgetauscht, die es gegen Manipulation und Ausspähen zu schützen gilt. Dies gilt insbesondere beim Einsatz von personenbezogenen Daten.

Sicherheit von und Vertrauen in KI-basierte Anwendungen sind für die gesellschaftliche Akzeptanz dieser Schlüsseltechnologie wichtige Grundvoraussetzungen. Dieses Sicherheitsbedürfnis wird durch aktuelle Umfragen bestätigt. Demnach wünschen sich 83% der Bürgerinnen und Bürger, dass Anwendungen mit KI von einer unabhängigen Stelle überprüft werden[1]. Hierfür sind hohe Qualitäts- und Sicherheitsstandards notwendig, basierend auf einem kohärenten und soliden Rechtsrahmen.

DIE AKTUELLE LAGE

Rechtsrahmen für KI-basierte Produkte unzureichend

- Durch das KI-basierte inhärente und selbstständige Lernen verändern sich Produkte oder Systeme während ihres Lebenszyklus und sind so in ihren Eigenschaften dynamisch. Die Funktionslogik, auf deren Basis das System Entscheidungen fällt, ist oftmals intransparent und nicht nachvollziehbar.
- Der aktuelle Rechtsrahmen, sowohl national wie europäisch, berücksichtigt diese neue Technologie und ihre Auswirkungen nur unzureichend. Es fehlen zudem Standards, Methoden und Prüfszenarien, um die Sicherheit der eingesetzten KI-basierten Systeme ganzheitlich zu bewerten.
- Viele ethische Fragestellungen, deren Antworten eine Orientierung im Umgang mit KI geben soll, werden aktuell noch diskutiert.

UNSERE POSITIONEN

Bestehenden Rechtsrahmen an neue Technologie anpassen

- Die rechtlichen Rahmenbedingungen für die Entwicklung und Nutzung von KI-Technologien sind insbesondere hinsichtlich Safety, Privacy und IT-Security zu überprüfen und ggf. anzupassen. Dabei ist mit Blick auf die EU-Binnenmarkgesetzgebung konsequent der New Legislative Framework (NLF) als kohärentes und international wettbewerbsfähiges Regelwerk zu nutzen. Bei notwendigen Anpassungen hinsichtlich der Sicherheits- und Datenschutzanforderungen sind die NLF-Instrumentarien heranzuziehen, um einen regulativen Flickenteppich

1 VdTÜV (2018), Mehrheit der Bundesbürger für Algorithmen-Checks, https://www.vdtuev.de/news/mehrheit-der-bundesbuerger-fuer-algorithmen-checks

zu vermeiden. Wesentliche NLF-Elemente sind die Definition grundlegender Produktanforderungen, Konkretisierung durch Normen und Überprüfung der Konformität durch akkreditierte unabhängige Stellen.

- Im Hinblick auf den Schutz persönlicher Daten muss von der Selektion der Trainingsdaten bis zur automatisierten Entscheidung in allen Prozessschritten ein durchgängig hohes Datenschutzniveau sichergestellt werden. Vor diesem Hintergrund ist der regulative Rahmen, wie beispielsweise die Datenschutzgrundverordnung, dahingehend zu überprüfen und gegebenenfalls anzupassen.
- Durch die zunehmende Abhängigkeit von Algorithmen für unsere digitale und vernetzte Gesellschaft ist eine hohe Resilienz vor Cyberangriffen für KI-Systeme unabdingbar. Die KI-Systeme müssen hinsichtlich der Vertraulichkeit der verarbeiteten und genutzten Daten, sowie hinsichtlich ihrer Verfügbarkeit und Integrität hohe Sicherheitsanforderungen erfüllen und diese fortwährend an die sich verändernde Bedrohungslage im Cyberraum anpassen.
- Die Nutzung KI-basierter Systeme setzt voraus, dass Rahmenbedingungen wie ethische Grundsätze und darauf aufbauende Gesetze Teil der KI sind und befolgt werden. Auch hier braucht es legislative Vorgaben. Der VdTÜV begrüßt daher die Initiative der EU-Kommission, entsprechende Ethikrichtlinien zu entwickeln.

Risikobasierte Sicherheitsbewertung für den gesamten Produktlebenszyklus vorschreiben

- Auch nach dem Inverkehrbringen müssen selbstlernende KI-Systeme fortwährend geprüft werden, um deren sichere Funktionsweise gewährleisten zu können. Für eine solche Sicherheitsbewertung benötigen unabhängige Prüfstellen Zugang zu KI-relevanten Daten.
- Zur Bewertung möglicher Risiken eines KI-Systems sind diese einer gesonderten Risikoanalyse zu unterziehen. In Abhängigkeit des daraus resultierenden Risikolevels sind entsprechend hohe Sicherheitsanforderungen zu definieren. KI-Systeme mit hoher Risikostufe müssen mit systematischen Selbstdiagnosemechanismen und ausfallsicheren Komponenten ausgestattet werden. Die automatische Überwachung der KI muss durch einen unabhängigen Dritten geprüft werden können. Sicherheitskritische KI-Systeme müssen reproduzierbar zu testen sein.
- Zur Nachvollziehbarkeit der Funktionsweise und Entscheidungsfindung von KI-Systemen/Deep Learning bedarf es zusätzlicher Forschung sowie eine enge Kooperation mit der Wissenschaft. Hier sollten durch den Gesetzgeber Anreize geschaffen werden.

Kontaktdaten

Ansprechpartner: Elisa Brummel
E-Mail: elisa.brummel@vdtuev.de
Tel.: +49 30 760 095 360
www.vdtuev.de/europawahl-2019/