SPD BERLIN
LANDESPARTEITAG 16./17. NOVEMBER 2018

Antrag 166/II/2018

Beschluss

Annahme in der Fassung der Antragskommission
Juso LDK
Der Landesparteitag möge beschließen:

Im Zeitalter der neuen Technologien: Freiheit, Privatsphäre und uns schützen!

Im Zeitalter der neuen Technologien: Freiheit, Privatsphäre und uns schützen!

Umgang, Einsatz und Auswirkungen von neuen Technologien allgemein:

Neue Technologien bieten vielfältige Möglichkeiten unser gesellschaftliches Miteinander neu zu gestalten. Sie können jedoch keine pauschale Lösung anbieten. Vor dem staatlichen Einsatz einer neuen Technologie muss fallspezifisch für jede Einzelne abgewogen werden, ob die Anwendung der Technologie eine Verbesserung zum Status Quo darstellt. Dabei sollten folgende fünf Punkte bedacht werden:

1. Neue Technologien bieten oft vermeintlich einfache Antworten auf komplexe Fragen und können somit politisch gut vermarktet werden. In der medialen Darstellung mag ein Schlagwort die „Lösung" darstellen, in der Realität greifen diese jedoch oft zu kurz. So werden zum Beispiel Vorratsdatenspeicherung zur Bekämpfung von Terror und Videoüberwachung gegen Drogen- und Bandenkriminalität präsentiert. Es ist offensichtlich, dass dies negative Erscheinungen komplexer gesellschaftlicher Prozesse sind, die nicht durch eine einzelne plakative Maßnahme gelöst werden können. Es wird vergeblich probiert, mit technischen Ansätzen soziale Probleme zu lösen. Allenfalls tragen diese Maßnahmen jedoch zur Bekämpfung der oberflächlichen Symptome bei.

2. Neue Technologien produzieren Daten und erlauben es, diese zu verarbeiten. Wenn diese Daten einmal vorhanden sind, ist es schwer ihren Missbrauch zu verhindern. Zum einen ist es für Bürger*innen schwer herauszufinden, welche Daten von ihnen erfasst und gespeichert werden. Zum anderen schafft jeder Datensatz auch immer ein Missbrauchspotential. Es existieren zwar Regeln und Kontrollorgane (Parlament, Verfassungsgericht), um das Überschreiten von Zuständigkeiten wie dem unerlaubten Eingriff in die Privatsphäre und Datenschutz-Verletzungen zu verhindern. Die Vergangenheit zeigt jedoch, dass es trotzdem immer wieder zu Missbrauch kommt. So haben einige Berliner Polizist*innen die Polizeidatenbank POLIKS auch genutzt um Nachbar*innen und Kolleg*innen auszuspionieren. Bürger*innen müssen darauf vertrauen, dass Behörden die Daten nicht unzweckmäßig verwenden. Weiterhin können Daten durch Sicherheitslücken in falsche Hände geraten bzw. bei Verschiebung der vorherrschenden politischen Interessen oder einem Regime-Wechsel missbraucht werden. Da es keine Garantie gibt, dass mit den heute gespeicherten Daten in zehn Jahren nach den jetzigen Vorstellungen umgegangen wird, müssen nach dem Grundsatz der Datensparsamkeit jeweils so wenig Daten wie möglich erfasst werden. Außerdem müssen Strukturen aufgebaut werden, die einen Missbrauch innerhalb der Behörden effektiver verhindert.Wir sehen einen Wandel von repressiven (aufklärende) zu präventiven (vorbeugenden) polizeilichen Maßnahmen. Hierbei stützen sich die präventiven Maßnahmen auf Daten und Algorithmen und nicht auf tatsächliche und individuelle Indizien. Die Gefahr ist, vor allem bei komplizierten Algorithmen, dass Verdachtsmomente und Grundrechtseingriffe nicht auf Fakten, sondern auf Statistik und Wahrscheinlichkeiten beruhend geschehen. Unbescholtene Verdächtigungen sind also unausweichlich.

3. Digitale Ansätze erfordern meist eine hohe Abstraktion, weshalb es vielen Bürger*innen schwerfällt, inhaltlich der öffentlichen Diskussion zu folgen oder sich zu beteiligen. Viele Menschen fühlen sich überfordert und denken, ihr technisches Wissen reiche nicht, um an der Diskussion teilzunehmen. Aber auch Politiker*innen sind davon betroffen und lassen neue Technologien in Behörden einsetzen. Versprechungen von Herstellern werden geglaubt, insbesondere, wenn eine neue Technologie angeblich Zeit, Geld oder Arbeitsaufwand sparen kann. Die gefühlte Objektivität und Intransparenz einer durch den Computer empfohlenen Entscheidung führt insbesondere unter Zeitdruck zur Umsetzung der Handlungsempfehlung durch die Behörden, ohne weitere Prüfung. Dies kann zu fatalen Fehlentscheidungen führen, wie z.B. der unrechtmäßigen Abschiebung eines Kurden aus dem Irak, bei dem das BAMF eine Sprachanalysesoftware zur Erkennung der Muttersprache eingesetzt hat. Die Software kannte seine Muttersprache allerdings gar nicht. Ein positives Ergebnis war also von vorneherein ausgeschlossen. Die Auswirkungen eines Technologie-Einsatzes können jedoch Jede*n betreffen, weshalb es wichtig ist, Menschen im kritischen Umgang mit Technologie auszubilden, aber auch Bürger*innen mit Alltagswissen in den Prozess der Technologie-Anschaffung einzubeziehen. Hinzu kommt, dass es (noch) wenig Nicht-Regierungsorganisationen gibt, die sich mit den Auswirkungen von Technik auf unsere Gesellschaft befassen und deshalb negative Folgen von neuen Technologien selten erkannt und thematisiert werden. In einer lebendigen Demokratie müssen alle Seiten ausreichend vertreten sein. Vor diesem Hintergrund ist es

besonders wichtig, die Empfehlungen von Expert*innen (z.B. CCC) bzgl. neuer Technologien und deren Einsatz in den politischen Entscheidungsprozess aufrichtig einzubeziehen.

4. Des Weiteren sind gerade Entscheidungen „intelligenter“ Systeme weder für Benutzer*innen noch für Betroffene klar zu durchschauen. Machine-Learning-Algorithmen nutzen bestehende Datensätze, um Entscheidungen zu treffen. Zum Beispiel könnte ein intelligentes Videoüberwachungssystem auf die Kriminalstatistik zurückgreifen, um zu entscheiden, ob eine Person kontrolliert werden sollte. Ein bereits bestehender Bias innerhalb dieser Datensätze beispielsweise institutioneller Rassismus in Form von Racial Profiling wird durch diese Algorithmen reproduziert und verfestigt. Dies widerspricht unserem Verständnis von Rechtsstaat, in dem jegliche Verurteilung bzw. Verdächtigung auf realen Beweisen beruhen müssen und nicht aufgrund statistischer Wahrscheinlichkeiten. Mit immer mehr Informationen, die Behörden zur Verfügung stehen, steigt außerdem die Wahrscheinlichkeit, dass sich darunter etwas Belastendes befindet. So könnte z.B. aus der Bekanntschaft mit einer Person aus vermeintlichen „Risikogruppen“ ein Verdachtsmoment konstruiert werden. Dies ermöglicht es, bei sehr vielen Menschen einen signifikanten Grundrechtseingriff zu rechtfertigen. Die präventiven Maßnahmen stützen sich auf Daten und Algorithmen und nicht auf tatsächliche und individuelle Indizien. Die Gefahr ist, dass Verdachtsmomente und Grundrechtseingriffe nicht auf Indizien, sondern auf Wahrscheinlichkeiten und Statistiken beruhen.

5. Des Weiteren sind die gesellschaftlichen Folgen vom Einsatz neuer Technologien schwer im Vorhinein abzusehen. So reproduzieren und verfestigen beispielsweise Machine-Learning Algorithmen bestehende Machtstrukturen. Hinzu kommt, dass unbekannt ist, wie diese Algorithmen zu ihren Ergebnissen kommen. Dies wiederspricht unserem Verständnis von Rechtsstaat, in dem jegliche Verurteilung bzw. Verdächtigung auf realen Beweisen beruhen muss und nicht aufgrund statistischer Wahrscheinlichkeiten aufgemacht werden darf.

Aus den genannten Gründen halten wir eine gewisse Skepsis gegenüber neuen Technologien und kritisches Hinterfragen der Notwendigkeit ihres Einsatzes für unbedingt notwendig. Die obige Auflistung ist allgemein formuliert und da jede Technologie spezifische Risiken birgt, muss jeder Punkt im Einzelfall vor dem Einsatz einer neuen Technologie umfangreich geprüft werden.

In Bezug auf Überwachungstechnologien gibt es die Forderung nach pauschalen Gesetzen, sodass die eingesetzten Überwachungsformen immer auf das technisch aktuell Machbare ausgeweitet werden sollen. Durch diese Bestrebung, Überwachung pauschal auszuweiten, wie es nur technisch möglich ist, verlieren wir die Fähigkeit, die einzelnen Maßnahmen auf Folgen und Tauglichkeit kritisch zu überprüfen. Die von uns oben dargelegte Einzelfallprüfung könnte und würde demnach nicht mehr stattfinden, stattdessen könnte die Exekutive unbemerkt von der Öffentlichkeit neue Instrumente einführen. Hierbei sollte auch die Möglichkeit der (Aus-)Nutzung und Verarbeitung der Daten in Zukunft z.B. bei veränderter politischer Lage oder Verschiebung unserer heutigen freiheitlich-demokratischen Werte beachtet werden

Der Einsatz von Technologien die über die reine Videoaufzeichnung hinaus gehen, lassen sich heute anhand von der Auswertung gespeicherter Daten mit Hilfe von Gesichtserkennungssoftware, aber auch der Echtzeitanalyse im Rahmen sogenannter intelligenter Kameras beobachten. Hieran können potenzielle Gefahren für zukünftige Entwicklungen erahnt werden. Ein Beispiel ist das Berliner Pilotprojekt am S-Bahnhof Südkreuz, bei welchem Passant*innen mit einer biometrischen Datenbank abgeglichen und automatisch identifiziert werden. Wenn solch „intelligente“ Kameras flächendeckend eingesetzt werden, können ganze Bewegungsprofile von Menschen erstellt werden und Jahrzehnte lang gespeichert werden. Ein Recht auf Anonymität und informationelle Selbstbestimmung ist dann nicht mehr gegeben. Von Bewegungsfreiheit kann nicht mehr die Rede sein, da es keine Möglichkeit sich der Überwachung (und Verdächtigung) zu entziehen. Die legalisierte Möglichkeit der massenhaften Identifizierung in Echtzeit ist ein enormer Schritt hin zu einem Überwachungsstaat. Aufgrund der Unsicherheit wie die Daten ausgewertet werden und der potenziell unsicheren Speicherung dieser höchst persönlichen Daten beginnt das Problem des Datenschutz bereits bei der Datensammlung und nicht erst bei Auswertung. Das oberste Gebot zum Schutz der Bürger*innenrechte sollte also Datensparsamkeit sein.

Ein weiteres grundlegendes Problem solcher intelligenter Systeme ist es, dass sie auf lernfähigen Algorithmen basieren, bei denen selbst dem Programmierer keine klare Grenze zwischen verdächtig und unverdächtig bekannt ist. Verhalten und Verdachtsmomente werden aufgrund statistischer Methoden vom Algorithmus erlernt und schließlich zur Entscheidung zwischen verdächtig und nicht verdächtig unterschieden. Dabei sind Algorithmen sind nicht objektiv, sondern verstärken bestehende Muster der Ungleichheit in der Gesellschaft. Die Beurteilung durch die im Moment eines Verdachtmoments alamierte Polizei unterliegt dem Bias der Entscheidungsempfehlung des Systems. Es muss unbedingt verhindert werden, dass wir die Unschuldsvermutung aufgeben und Menschen stattdessen aufgrund von Statistik und unklaren Entscheidungskriterien verdächtigen. Zum Anderen bedeutet dies einen schleichenden Demokratieabbau, da immer kleinere auffällige Verhalten als Vergehen gewertet werden und zu einer Rechtfertigung gegenüber Staatsorganen verpflichten.

SPD BERLIN
LANDESPARTEITAG 16./17. NOVEMBER 2018