A23

Antrag

Initiator*innen:

Titel: **Digitale Freiheitsrechte stärken – Für eine grundrechtskonforme Sicherheitspolitik im digitalen Raum**

Antragstext

Der Landesparteitag möge beschließen:

1. Die Landtagsfraktion von BÜNDNIS 90/DIE GRÜNEN Schleswig-Holstein wird aufgefordert, sich dafür einzusetzen, dass beim Einsatz von Analysesystemen in Sicherheitsbehörden nur solche Lösungen gewählt werden, die grundrechts- und datenschutzkonform, transparent und quelloffen sind. Dabei soll die im Koalitionsvertrag verankerte digitale Souveränität durch den Einsatz deutscher oder europäischer Softwarelösungen, bestenfalls Eigenentwicklungen, gestärkt werden.

2. Bei der Bekämpfung von Cyberkriminalität setzt sich die Landtagsfraktion für Lösungen ein, die die Ende-zu-Ende-Verschlüsselung als Grundpfeiler digitaler Sicherheit bewahren und stärken. Das Recht der Nutzer*innen auf anonyme und pseudonyme Nutzung ist zu stärken. Hierzu ist die Landesregierung aufzufordern, ein Konzept zu erarbeiten, wie Strafverfolgungsbehörden effektiv arbeiten können, ohne Verschlüsselungstechnologien zu schwächen.

3. Für den Einsatz von Datenanalysesystemen ist ein Kriterienkatalog zu entwickeln, der folgende Aspekte umfasst und gesetzlich hinreichend bestimmt festgeschrieben wird:

    1. Transparenz der Algorithmen und Entscheidungsprozesse,

Entscheidungen müssen den Grundsätzen des Rechts folgen, also nachvollziehbar sein
2. Datensparsamkeit und strenge Zweckbindung
3. Regelmäßige unabhängige Evaluierung der Systeme durch unabhängige Wissenschaft und/oder Aufsichtsbehörden
4. Klare Löschfristen für erhobene Daten
5. Besonderer Schutz von Personen, die aufgrund von Zeugenschaft, als Begleitpersonen etc. im System registriert werden
6. Ausschluss biometrischer Massenüberwachung im öffentlichen Raum ("intelligente Videoüberwachung") sowie keine anlasslose Massenüberwachung a la Vorratsdatenspeicherung im digitalen Raum
7. Kein automatischer Abruf aus Registern
8. Speicherung von Daten ausschließlich in vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten, deutschen oder europäischen Rechenzentren
9. Ausschluss von "Predictive Policing"
10. Nachvollziehbares Rollen- und Zugangsmanagement, das den Einsatz des Werkzeugs protokolliert und unrechtmäßigem Einsatz vorbeugt

4. Die Landtagsfraktion setzt sich für die Förderung und Entwicklung deutscher oder europäischer Alternativen zu proprietären Überwachungssystemen wie diejenigen des hoch umstrittenen US-Unternehmens Palantir aus dem direkten Umfeld von Präsident Donald Trump ein. Hierfür sollen auch Kooperationen mit Forschungseinrichtungen und deutschen wie europäischen Technologieunternehmen angestrebt werden.

5. Die nachträgliche Identifizierung einzelner verdächtiger Personen zur Abwehr dringender und gewichtiger Gefahren, etwa durch einen Abgleich im Internet, kann in eng begrenzten und klar geregelten Ausnahmefällen ein wichtiges Instrument für die Sicherheitsbehörden sein. Die damit verbundenen tiefen Grundrechtseingriffe erfordern jedoch hohe rechtsstaatliche Sicherungsmechanismen. Insbesondere muss sichergestellt sein, dass die technische Umsetzung verfassungs- und europarechtskonform möglich ist. Inwieweit das tatsächlich möglich ist, ist derzeit noch unklar. Ein Verfahren, um die Einhaltung dieser Prinzipien zu überprüfen und zu gewährleisten, kann die Einrichtung eines KI-Reallabors (Art. 59 Abs. 2 KI-VO) für Sicherheitsbehörden sein. Dort könnten in sicherer Umgebung unter Einbindung von Aufsichtsbehörden souveräne, passgenaue und rechtskonforme Lösungen entwickelt werden. Da es sich um einen tiefgreifenden Grundrechtseingriff handelt, können dies nur Verfahren sein, die eine solche Identifizierung unter strenger Beachtung von Verfassungs- und Europarecht ermöglichen und gleichzeitig den Schutz der Persönlichkeitsrechte gewährleisten.