

Antrag

Initiator*innen: Kirsten Bock, Norbert Tretkowski (Sprecher*innen LAG Medien und Netzpolitik), Maya Diederichs, Moritz Bührmann (Sprecher*innen LAG Demokratie und Recht), Sebastian Bonau, Konstantin von Notz, Jörn Pohl (dort beschlossen am: 23.10.2025)

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 für den Einsatz von grundrechts- und datenschutzkonformen, transparenten und quelloffenen Analysesystemen in Sicherheitsbehörden einzusetzen. 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-V0) 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

58 sein, die eine solche Identifizierung unter strenger Beachtung von
59 Verfassungs- und Europarecht ermöglichen und gleichzeitig den Schutz der
60 Persönlichkeitsrechte gewährleisten.

Begründung

Die digitale Transformation stellt unsere Gesellschaft vor neue Herausforderungen im Spannungsfeld zwischen Sicherheit und Freiheit. Der im Koalitionsvertrag 2022-2027 verankerte Anspruch auf digitale Souveränität steht im Widerspruch zum Einsatz proprietärer Überwachungssoftware aus Drittstaaten wie der Einsatz von Software des hoch umstrittenen US-Unternehmens Palantir aus dem direkten Umfeld von Präsident Donald Trump. Die zunehmende Tendenz, umfassende Datenanalysesysteme ohne ausreichende Rechtsgrundlagen und demokratische Kontrolle einzusetzen, gefährdet Grundrechte und untergräbt das Vertrauen der Bürger*innen in staatliches Handeln. Wie aktuelle Entwicklungen in anderen Bundesländern zeigen, besteht zudem die Gefahr einer schleichenden Ausweitung staatlicher Überwachungsbefugnisse. Deutsche und europäische Alternativen mit erheblichen Vorteilen mit Blick auf den notwendigen Grundrechtsschutz und die Beachtung höchstrichterlicher Vorgaben sind längst verfügbar oder können bestenfalls, das hat EUROPOL gezeigt, unter vollumfänglicher Einbeziehung der Datenschutzaufsichtsbehörden entwickelt werden. Die Berlin Group (Internationale Arbeitsgruppe für Datenschutz in der Technologie) hat Richtlinien für den datenschutzkonformen Einsatz von Gesichtserkennungstechnologien erarbeitet, die als Grundlage für eine verantwortungsvolle Nutzung dieser Technologien dienen können. Auch während der Anhörung des Innenausschusses des Bundestags zum sogenannten „Sicherheitspaket“, das die letzte Bundesregierung vorgelegen hat, hat wichtige Hinweise für einen grundrechtskonformen Einsatz gegeben, die zwingend beachtet werden sollten. Diese Richtlinien und Vorgaben sollten in Schleswig-Holstein konsequent beachtet und umgesetzt werden.

Der Koalitionsvertrag betont die Bedeutung von IT-Sicherheit, digitaler Souveränität und eines effektiven Daten- und Grundrechtsschutzes. Die Ende-zu-Ende-Verschlüsselung ist dabei ein zentrales Element zum Schutz der digitalen Kommunikation. Eine Schwächung dieses, auch gesetzlich verbrieften Rechts der Nutzer*innen würde nicht nur die Privatsphäre der Bürger*innen und ihre informationelle Selbstbestimmung gefährden, sondern auch die IT-Sicherheit insgesamt untergraben.

Mit diesem Antrag bekräftigen wir unsere Verpflichtung, digitale Grundrechte zu schützen, auszubauen und gleichzeitig den Sicherheitsbehörden effektive Werkzeuge zur Bekämpfung von Kriminalität an die Hand zu geben, die ihnen nicht regelmäßig von höchsten Gerichten wieder aus der Hand geschlagen werden. Wir verweisen darauf, dass Sicherheit und Freiheit keine Gegensätze sind, sondern sich vielmehr gegenseitig bedingen.

Es sollen grundrechts- und datenschutzkonforme Analysesysteme eingesetzt werden.

Diese sollen von deutschen oder europäischen Firmen kommen.

Verschlüsselung und anonyme Nutzung müssen gestärkt werden.

Kriterienkatalog:

- Entscheidungen der Software müssen nachvollziehbar sein
- So wenig Daten speichern wie nötig
- Prüfung der Software
- Daten müssen gelöscht werden
- Erfasste Zeugen und Begleitpersonen müssen geschützt werden
- Keine Videoüberwachung im öffentlichen Raum
- Keine Vorratsdatenspeicherung
- Daten nur in zertifizierten Computerräumen speichern
- Keine Polizeiarbeit wegen Wahrscheinlichkeit von Straftaten
- Zugriff auf das System einschränken und dokumentieren

Suche nach Personen im Internet nur in Ausnahmefällen.

Unterstützer*innen

Florian Juhl (OV Pinneberg), Melissa Sieber (KV Schleswig-Flensburg), Jessica Leutert (KV Kiel), Marcel Beutel (KV Ostholstein), Lutz Sonntag (KV Flensburg), Zoé Engel (KV

Lübeck), Andrea Eva Dreffein-Hahn (KV Pinneberg), Jennifer Herbert (KV Kiel), Markus Suhr (KV Rendsburg-Eckernförde), Lasse Bombien (KV Rendsburg-Eckernförde), Susanne Lohmann (KV Stormarn), Fabian Osbahr (KV Segeberg), Jan Kürschner (KV Kiel), Mathias Schmitz (KV Pinneberg), Carsten Nielsen (KV Flensburg), Robert Lemke (KV Lübeck), Maria Fischer (KV Schleswig-Flensburg), Lorenz Mayer (KV Segeberg), Conny Clausen (KV Flensburg), Sebastian Rautert (KV Pinneberg), Stefan Lansberg (KV Plön), Jörn Peter Böning (KV Plön), Silke Schiller-Tobies (KV Kiel), Carina Hennecke (KV Rendsburg-Eckernförde), Sascha Peukert (KV Lübeck), Birgit Graf (KV Herzogtum Lauenburg), Ullrich Kruse (KV Stormarn), Katrin Stange (KV Pinneberg), Annette Granzin (KV Ostholstein), Oliver Voigt (KV Kiel), Gabriele Braune (KV Ostholstein), Henning In den Birken (KV Pinneberg), Britta Mohr (KV Rendsburg-Eckernförde), Adrian Grimm (KV Kiel), Reimo Schaaf (KV Ostholstein)