Beschluss Unabhängig von Tech-Oligarchen

Gremium:	Landesdelegiertenkonferenz
Beschlussdatum:	21.06.2026
Tagesordnungspunkt:	8. Verschiedenes

Antragstext

1. Schluss mit Palantir – europäische Technologiesouveränität ist nicht verhandelbar

Palantir ist kein neutraler Technologieanbieter. Das Unternehmen steht für den offenen Angriff auf die Demokratie, Militarisierung und Totalüberwachung. NRW darf nicht von US-Konzernen abhängig sein – und schon gar nicht von solchen, die Überwachung als Geschäftsmodell und antidemokratisches Denken als Unternehmenskultur betreiben.
Deshalb ruft die LDK die Landesregierung NRW dazu auf:

- Keine neuen Verträge mit Palantir abzuschließen.
- Der Ausstieg aus Palantir muss ohne weiteres Zögern erfolgen.
- Alle relevanten Akteure müssen sich für eine schnellstmögliche bürgerrechtssensible europäische Alternative einsetzen.
- Schnellstmöglich die Ausschreibung für eine Alternativlösung zum Abschluss bringen.
- Europäische Softwarealternativen und offene, souveräne Infrastrukturen für Sicherheitsbehörden müssen aktiv gefördert werden.

2. Sicherheit braucht moderne Werkzeuge – aber mit Grundrechten, nicht gegen sie

Die Bedrohungslage hat sich verändert. Organisierte Kriminalität, Medien von sexualisierter Gewalt gegen Kinder im Netz, Cybercrime und terroristische Netzwerke sind datengetrieben. Ohne datengestützte Analysewerkzeuge sind Behörden strukturell unterlegen. Das ist eine Realität, der wir uns stellen müssen – aber sie rechtfertigt keine Abstriche bei Grundrechten.

Es braucht deshalb:

- Klare gesetzliche Grundlagen für den Einsatz automatisierter Datenanalyse – keine Graubereiche und keine unkontrollierten Praktiken.
- Strenge Verhältnismäßigkeit: Die Analyse polizeilicher und personenbezogener Daten darf nur zur Bekämpfung schwerster Straftaten und terroristischer Bedrohungen eingesetzt werden.
- Den Vorrang menschlicher Entscheidung: KI analysiert, doch Menschen treffen die Entscheidungen. Eigenständige Grundrechtseingriffe durch Algorithmen sind ausgeschlossen.
- Den Ausschluss diskriminierender und intransparenter Modelle.
- Wir streiten weiter mit Priorität für einen hohen Datenschutzstandard. Wir erkennen die Bedenken aus der Bürgerrechtsbewegung an und bleiben weiter im Austausch mit der Zivilgesellschaft. Gemeinsam arbeiten wir kontinuierlich für bürgerrechtskonforme Lösungen.
- Vollständige Protokollierung jeder Nutzung – transparent, nachvollziehbar, überprüfbar.
- Keine Software-Lösung, die dem US-Cloud-Act unterliegt.

3. Regeln statt Grauzone – und Kontrolle, die diesen Namen verdient

Automatisierte Datenanalyse war in den Sicherheitsbehörden lange Jahre längst Realität auf Basis von Generalklauseln, jedoch ohne eine transparente gesetzliche Regelung und ohne echte Kontrolle. Einen ersten Schritt haben wir mit dem Polizeigesetz NRW 2025 gemacht, das zum ersten Mal einen konkreten Rahmen bietet. Wir wollen diesen Rahmen konsequent erweitern.

- Unabhängige wissenschaftliche und parlamentarische Kontrollmechanismen, die wirksam sind und nicht nur auf dem Papier existieren.
- Verbindliche Einhaltung des Datenschutzes als Grundvoraussetzung.
- Strikte Anonymisierungs- und Pseudonymisierungspflichten.
- Einbettung in das europäische Datenschutzrecht und die EU-KI-Verordnung – die seit 2024 verbindliche Leitplanken für Hochrisiko-Systeme setzt.

Hierzu bedarf es einer regelmäßigen parlamentarischen / politischen Befassung mit den Chancen und Risiken sich schnell verändernden Technologien sowie die enge Einbindung wissenschaftlicher Erkenntnisse in der Sicherheitspolitik.