

Regulierungslücken und informationstechnische Risiken im Verfassungsschutzgesetz NRW

Eine sachverständige Positionierung zur automatisierten Datenanalyse

Datum 12. Juni 2026 — **Status** Offizielle Publikation (Version 1.0)

Herausgeber: Deutsches Institut für zukunftsfähige KI e.V. (DIZK)

Autor: Oliver Kölsch — Vorstandsvorsitzender DIZK e.V., Zertifizierter IT-Sachverständiger (BISG e.V.), Lead Auditor (ISO/IEC 42001, ISO 9001:2015)

Executive Summary: Kernforderungen des DIZK

Die am 1. April 2026 in Kraft getretene Novelle des Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG NRW) sowie die hiergegen gerichtete Verfassungsbeschwerde verdeutlichen die Dringlichkeit einer rechtssicheren und technisch belastbaren AI-Governance in Sicherheitsbehörden. Das Deutsche Institut für zukunftsfähige KI e.V. (DIZK) identifiziert in den aktuellen Vorschriften zur automatisierten Datenanalyse erhebliche Defizite in der Auditierbarkeit und Reproduzierbarkeit.

Der Gesetzgeber wird zur Umsetzung folgender Maßnahmen aufgefordert:

- Keine Eingriffsschwellen durch unvalidierte Scores: Algorithmische Scores, statistische Korrelationen oder KI-generierte Priorisierungen dürfen ohne zusätzliche, durch Tatsachen belegte menschliche Bewertung keine eigenständige Grundlage für Grundrechtseingriffe bilden.
- Nachweis einer normbasierten AI-Governance: Vor dem Produktiveinsatz von Analysesystemen ist ein unabhängig auditiertes KI-Managementsystem nach ISO/IEC 42001:2023 nachzuweisen.
- Abgestuftes Auditmodell für Drittanbieter: Proprietäre Systeme bedürfen im hoheitlichen Kernbereich zwingend überprüfbarer Sicherheitsarchitekturen (z. B. Quellcode-Escrow, Red-Teaming unter Geheimschutz), um digitale Souveränität zu gewährleisten.
- Nachweisbare Schutzarchitektur für Berufsgeheimnisträger: Der Schutz privilegierter Kommunikation muss durch technisch vorgelagerte Privilegienfilter (Ex-ante) und nicht primär durch nachträgliche Löschpflichten (Ex-post) sichergestellt werden.

1. Einordnung: Der normative und rechtspolitische Rahmen

Das neue VSG NRW regelt unter anderem den Zugriff auf Videoüberwachungen (§ 20), den Einsatz von Systemen zur automatisierten Datenanalyse unter Nutzung maschinellen Lernens (§ 26) sowie die Übermittlung personenbezogener Daten zur Entwicklung und Überprüfung von IT-Produkten (§ 36).

Die hiergegen geführte verfassungsrechtliche Auseinandersetzung trifft einen berechtigten technischen Kern: Die automatisierte Analyse von Massendaten stellt einen eigenständigen, schweren Grundrechtseingriff dar, da aus vorhandenen Daten neues Wissen generiert wird. Auch wenn § 26 VSG NRW formale Schutzmechanismen vorsieht, wie den Ausschluss weiterlernender Systeme, das Verbot der Internetanbindung und den Vorbehalt einer Letztbewertung durch einen Sachbearbeiter, greifen diese Vorgaben informationstechnisch zu kurz.

Ohne externe Validierung, transparente Schwellenlogik und dokumentierte Erklärverfahren bleiben diese internen Mechanismen unbestimmt und einer unabhängigen Kontrolle entzogen.

2. Technische Analyse (§ 26 VSG NRW): Validität und Grundrechtseingriffe

Klassische Analysesysteme operieren regelbasiert und deterministisch. Moderne Machine-Learning-Verfahren (ML) liefern hingegen probabilistische Scores. Bei fixierter Modellversion ist die Inferenz (der Entscheidungsweg) zwar deterministisch reproduzierbar, das zugrundeliegende Ergebnis bleibt jedoch eine stochastische Näherung.

- **Skalierung von False Positives:** Bei der Massendatenanalyse und den bei nachrichtendienstlichen Zielpersonen naturgemäß sehr niedrigen Basisraten erzeugen selbst Modelle mit hoher relativer Treffergenauigkeit in absoluten Zahlen viele „False Positives“. Ein stochastischer Treffer oder eine systemseitige Priorisierung lösen im operativen Betrieb faktisch Folgemaßnahmen aus.
- **Das Dilemma der menschlichen Letztentscheidung:** Die gesetzliche Vorgabe, wonach KI-Ergebnisse zwingend durch menschliches Personal plausibilisiert werden müssen (§ 26 Abs. 2 VSG NRW), ist nur wirksam, wenn das System Explainability (Erklärbarkeit) bietet. Fehlen Audit-Logs, Modellkarten oder Ex-post-Erklärverfahren, kann der Sachbearbeiter die Entscheidungsparameter des Modells nicht logisch nachvollziehen. Die menschliche Kontrolle verkommt zur Formalie (Automatisierungsbias).

3. Normenbasierte Governance: ISO-Standards und der EU AI Act

Die Anforderungen an behördliche Analysesysteme müssen zwingend etablierten Compliance- und Qualitätsmaßstäben folgen.

- **Zertifizierbares KI-Managementsystem:** Das DIZK fordert die Implementierung der ISO/IEC 42001:2023. Dieser Standard definiert die Voraussetzungen für Aufbau, Betrieb und fortlaufende Verbesserung eines AI-Management-Systems. In Kombination mit einem etablierten Qualitätsmanagement (z. B. nach ISO 9001:2015 bzw. der kommenden Fassung mit Harmonized Structure) lassen sich messbare Metriken für Zuverlässigkeit und Datenqualität ableiten.
- **Der EU AI Act als Benchmark:** Aus juristischer Sicht sieht der EU AI Act eine Bereichsausnahme für die nationale Sicherheit vor. Informationstechnisch betrachtet definiert die Verordnung jedoch den unwiderruflichen Stand der Technik für Hochrisiko-Systeme (High-Risk AI). Die dort vorgesehenen Prinzipien zur Datenvalidierung, menschlichen Aufsicht und Risikominimierung müssen als technische Benchmark für polizeiliche und nachrichtendienstliche Softwaresysteme dienen, ungeachtet juristischer Ausnahmetatbestände.

4. Digitale Souveränität und abgestufte Auditierung (§ 36 VSG NRW)

§ 36 VSG NRW eröffnet Einsatz- und Trainingsszenarien, die bei der Nutzung proprietärer Drittanbieterplattformen erhebliche Souveränitäts- und Auditrisiken erzeugen. Ohne transparente Prüfmechanismen führt die Auslagerung behördlicher Analysen an externe Dienstleister (z. B. im Rahmen von Neuvergaben) zu einem kritischen Vendor Lock-in und einer intransparenten „Black Box“-Architektur.

Das DIZK plädiert nicht zwingend für die vollumfängliche, öffentliche Offenlegung aller Trainingsdaten – dies ist datenschutzrechtlich und geheimsschutztechnisch oft nicht umsetzbar. Gefordert wird stattdessen ein abgestuftes Auditmodell:

Proprietäre Systeme dürfen im staatlichen Kernbereich nur eingesetzt werden, wenn unabhängige Sachverständige unter Geheimschutz Zugriff auf Quellcode (Escrow), Modelllogiken, Software-Stücklisten (SBOM) und Validierungsdatensätze erhalten. Klauseln zum Nicht-Training von Basismodellen mit behördlichen Einsatzdaten müssen vertraglich und technisch erzwungen werden.

5. Technischer Schutz von Berufsgeheimnisträgern (§ 9 VSG NRW)

Der Schutz des Kernbereichs privater Lebensgestaltung sowie der vertraulichen Kommunikation von Berufsgeheimnisträgern (Rechtsanwälte, Journalisten, Abgeordnete, Geistliche) ist in § 9 VSG NRW geregelt. Diese Vorgaben basieren jedoch primär auf nachträglichen Löscho- oder Unterbrechungspflichten (Ex-post).

In der automatisierten, KI-gestützten Analyse ist eine Ex-post-Löschung unzureichend. Wenn geschützte Daten einmal aggregiert, indexiert und zur Feature-Bildung der KI genutzt wurden, ist ihr Einfluss auf das Modell kaum reversibel („Machine Unlearning“ ist technisch hochkomplex und fehleranfällig). Geschützte Kommunikation muss daher zwingend – soweit es der Stand der Technik zulässt – durch vorgelagerte Privilegienfilter, Quarantänebereiche und sichere Trennungsmechanismen vor der irreversiblen algorithmischen Verarbeitung isoliert werden.

Kontakt: Oliver Kölsch (Vorstandsvorsitzender)

E-Mail: hello@dizk.de | Web: www.dizk.de

Neusatz am 21.10.2026 im Erscheinungsbild des DIZK, Satz in Bahnschrift. Text unverändert aus der Fassung vom 12. Juni 2026 (Version 1.0), Kontaktadresse aktualisiert; Reihennummer 02 vergeben am 21.10.2026.

DIZK Positionspapier 02 – Version 1.0, veröffentlicht am 12.06.2026. dizk.de/publikationen