Chaos Computer Club
Stuttgart e.V.

18. August 2025

Stellungnahme

zum Entwurf des „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“ der Landesregierung BW vom 30.07.2025

Von Stefan Leibfarth

Chaos Computer Club Stuttgart e.V.

Der vorliegende Gesetzentwurf dient der Schaffung von Befugnissen zur Erhebung, Verarbeitung und Übermittlung von Standortdaten, zur eigenständigen Entwicklung von informationstechnischen Systemen und zur automatisierten Datenanalyse im Polizeigesetz Baden-Württemberg.

Diese Stellungnahme beschränkt sich auf den Entwurf einer Rechtsgrundlage für eine automatisierte Datenanalyse in § 47a und § 57a des Entwurfes mit Fokus auf Sicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) des geplanten informationstechnischen Systems und Abschätzung der Folgen für die Rechte der betroffenen Baden-Württemberger*innen.

Zusammenfassung

Der vorliegende Gesetzentwurf versucht offensichtlich, die durch das Bundesverfassungsgericht am 16. Februar 2023 (1BvR1547/19,1BvR2634/20) getroffene Entscheidung umzusetzen. Dies gelingt jedoch nicht. Des Weiteren sollte sich diese Anpassung des PolG nicht nur an grundgesetzlichen Leitplanken orientieren, sondern auch unter IT-Sicherheits- und Bürgerrechts-Gesichtspunkten sinnvoll gestaltet werden. Auch dies gelingt leider nicht in ausreichendem Maße. So gibt es keine klaren Vorgaben bzw. Einschränkung

hinsichtlich der zusammengeführten und verarbeiteten Daten bzw. Datenbanken, keine Untersagung der Nutzung sogenannter “Künstlicher Intelligenz” (KI), die Vorgaben bzgl. Transparenz der eingesetzten Software, sowie dessen Kontrolle sind ungenügend. All dies ist, angesichts des geplanten schwerwiegenden Grundrechtseingriffs, weder hinnehmbar noch objektiv begründet.

Bewertung der Regelungen im Einzelnen

Quelle und Speicherung der Daten

Die in § 47a (1) geplante Erlaubnis aus “polizeilichen Dateisystemen gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen, verknüpfen, abgleichen, aufbereiten, auswerten und bewerten” ist aus unserer Sicht **unbestimmt und damit zu weitreichend**.

Hier bedarf es einer **Einschränkung auf konkret aufgeführte Datenbanken** der Polizei in Baden-Württemberg. Andernfalls droht, auf Grund der parallel voranschreitenden internationalen Vernetzung von polizeilichen Systemen aus dem In- und Ausland, die Gefahr einer gigantischen Datenbank unabgrenzbaren Ausmaßes.

Das in § 47a (6) geplante “Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten” erscheint sinnvoll, wie dies jedoch in der Praxis bei bereits bestehenden Datensätzen angewandt werden soll ist unklar. Ebenso wie dies bei Daten von nicht-landeseigener Herkunft sichergestellt werden soll. Uns erscheint dies schlicht unmöglich und führt de facto zur **Aufhebung der Zweckbindung** der zusammengeführten Daten. Nach unserer Auffassung ist dies grundrechtswidrig, verstößt es doch gegen den Grundsatz der ‘Informationellen Selbstbestimmung’[1]. Auch ist diese Aufhebung geeignet das Vertrauen der Bürger in die Polizei zu beschädigen, muss doch zukünftig bei jedem Kontakt von der Aufnahme der eigenen Daten in diese gigantische Datenbank ausgegangen werden.

Die in § 47a (3) geplante “Beurteilung der Erforderlichkeit” beim Einbeziehen der genannten zahlreichen Datenquellen darf nicht dem Ermessen der Ermittlungsbehörden selbst überlassen werden, sondern sollte unter **Richter*innenvorbehalt** gestellt werden. Andernfalls droht auch hier ein massenhaftes Zusammenführen und Speichern großer Datenmengen.

Die auf der Analyseplattform gespeicherte Daten sollten **nach Abschluss der** hierfür ursächlichen Ermittlungen **in jedem Fall gelöscht werden** müssen und nicht erst “nach Ablauf von zwei Jahren”.

Dass “Personenbezogene Daten [...] aus einer Wohnraumüberwachung oder einer Online-Durchsuchung” nicht einbezogen werden dürfen ist positiv zu bewerten, geht jedoch nicht weit genug. Auf Grund der Eingriffstiefe in Grundrechte sollten zusätzlich **biometrische Daten, Daten aus anlasslosen Durchsuchungen** sowie alle Daten die von **Nachrichtendiensten** stammen, ausgeschlossen werden.

Auswertung der Daten

Das Bestreben der Landesregieren “sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden” (§ 47a (2)) bewerten wir grundsätzlich positiv, unklar bleibt jedoch wie dies konkret erreicht werden soll. Hierzu bedarf es mindestens einer **explizierten Untersagung der Nutzung von sogenannter “Künstlicher Intelligenz” (KI)** bei der Ermittlung von verdächtigen Personen. Denn besonders hier hat sich gezeigt, wie gesellschaftliche Minderheiten diskriminiert werden und sich hierdurch Ungleichheiten verfestigen[2].
Diese großen Probleme von “KI”, auch und besonders bei der Software des US-amerikanischen Überwachungskonzerns Palantir, hat glücklicherweise auch Innenminister Strobl erkannt: “Wir werden mit Palantir selber die KI-Nutzung nicht machen”[3]. Dies gilt es nun auch im Gesetz zu verankern.

Die in § 47a (7) getroffenen Regelung, welche der Polizei selbst die Möglichkeit gibt über die fallbezogene Nutzung der Analyseplattform entscheiden, lehnen wir ab. Die in Bayern bereits im Einsatz befindliche Instanz hat gezeigt, zu welch inflationärer Nutzung dies in der Praxis führt. Hier “nutzte die bayerische Polizei das System für alltäglichere Delikte – etwa bandenmäßigen Fahrraddiebstahl oder Geldautomatensprengungen”[4]. Um dem vorzubeugen halten wir für die Nutzung den **Richter*innenvorbehalt** für angemessen. Einzig bei Gefahr im Verzug wäre eine Anordnung der Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts als ausreichend zu definieren.

Vertraulichkeit, Transparenz und Kontrolle

Um der tatsächlichen Funktionsweise des geplanten Systems und den Schutz der in ihm gespeicherten Daten in angemessenem Maße sicher stellen zu können, bedarf aus unserer Sicht einiger Vorgaben, welche im aktuellen

Entwurf nicht enthalten sind.

Zentraler Punkt ist hierbei die **Veröffentlichung des Quelltextes** der neuen Analyseplattform. Gerade in grundrechts-sensiblen Bereichen der Datenverarbeitung dürfen sich der Staat und seine mündigen Bürger nicht auf Versprechen des Software-Anbieters verlassen. Statt dessen muss der Programmcode der genutzten Software zur öffentlichen Einsicht vorliegen. Dies ermöglicht es einer interessierten Öffentlichkeit zu prüfen, ob gesetzliche Vorgaben tatsächlich im Code umgesetzt wurden und nicht weitere, unzulässige Funktionen enthalten sind.

Auch bestünde dann die **Möglichkeit unabhängig zu prüfen**, ob seitens des Herstellers eine Hintertür für den ungewollten Zugriff auf bzw. Abfluss der im System gespeicherten Daten eingebaut wurde. Besonders bei der Nutzung von Produkten von Herstellern außerhalb der EU besteht hier ein erhöhtes Risiko, so sind z.B. US-amerikanische Hersteller zu Herausgabe von Daten auf von Ihnen betriebenen System verpflichtet (US CLOUD Act[5]).

Sollte sich gegen eine Vorgabe zur Veröffentlichung des Quelltextes entschieden werden, so muss mindestens den Landesbehörden durch den Hersteller Einsicht in den Quellcode gewährt werden. Vor dem Start der Analyseplattform muss deren **Quellcode von einer unabhängigen Partei geprüft** werden. Dies hat auch für jedes Update (= u.U. weitreichende Änderungen) zu erfolgen, macht es doch jede vorherigen Prüfung hinfällig. Dies gilt beispielsweise auch für den öffentlich diskutierten Prüfbericht der Software ‘Gotham’ des US-amerikanischen Überwachungskonzerns Palantir[6].

Der **Prüfauftrag ist vom LfDI zu erteilen und, zusammen mit dem Prüfergebnis, zu veröffentlichen.** Dies soll sicherstellen, dass bei der Beauftragung der Prüfung alle relevanten Teile/Aspekte der Software berücksichtigt werden; ein häufiges Problem dieser Art von Audits.

Neben eines ungewollten Abflusses von Daten durch einen Fehler oder eine Hintertür in der der Software, ist ein direkter Zugriff von Mitarbeitenden des Herstellers auf das Produktivsystem zu unterbinden. Sei es durch eine Fernwartungsschnittstelle oder physischen Zugriff im Rechenzentrum. Denn auch auf diesem Weg kann eine negative Beeinträchtigung der Integrität und Vertrauenswürdigkeit des Systems erfolgen.

Zusätzlich zu einer möglichst vertrauenswürdigen Plattform für die Analyse der Daten, bedarf es einer **regelmäßigen, unabhängigen Prüfung der konkreten Nutzung** durch die Beamten. Diese regelmäßigen,

verdachtsunabhängigen Stichproben sollten durch das Parlamentarische Kontrollgremium beauftragt werden. Die Veröffentlichung der Ergebnisse halten wir für geboten.

Digitale Souveränität

Neben der Möglichkeit die Vertraulichkeit der gespeicherten Daten zu prüfen und die Funktionsweise der Software nachvollziehen zu können, bietet Open-Source-Software weitere große Vorteile.

Durch Software unter eigenständiger Kontrolle des Staates hat kein kommerzieller, noch dazu ggf. außer-europäischer, Anbieter die Möglichkeit **Einfluss auf den weiteren Betrieb der geplanten Analyseplattform zu nehmen**. Denn selbst auf eigenen Systemen betriebene Software bedarf regelmäßiger Updates um Sicherheitslücken zu schließen, Fehler zu beheben, an neue Hardware oder an geänderte Datenquellen angepasst zu werden. Würden die Updates auf Grund von kommerziellen oder politischen Entscheidungen ausbleiben, wäre eine solche Plattform kurz bis mittelfristig nicht mehr betreibbar.

Auch verwendet proprietäre Software in aller Regel eigene Formate und Schnittstellen bei der Speicherung und dem Austausch von Daten. Dies erschwert den späteren Wechsel hin zu einer eigenständigen Lösung, der sogenannte **Lock-In-Effekt**.

Aus unser Sicht sollte sich die Landesregierung auch aus finanziellen Gründen für eine souveräne Softwarelösung entscheiden. Jeder Euro Lizenzkosten für eine kommerzielle Lösung ist ein fehlender Euro für eine eigenständige Entwicklung. Ein Muster, das sich leider in vielen Bereichen wiederholt. Dabei ist doch eine **europäische Lösung**, bei dem sich alle Partner die Kosten teilen und vom Ergebnis dauerhaft profitieren naheliegend.

Nutzung von Daten zur Entwicklung, Training, Tests und Validierung

Die in § 57a (1) vorgesehene Verarbeitung von unveränderte Daten und nicht anonymisierten oder zumindest pseudonymisierten Daten lehnen wir ab. Es ist grundsätzlich nicht nachvollziehbar, warum unveränderte Daten benötigt werden sollten oder wenigsten eine Pseudonymisierung vorgenommen werden kann. Dies ist insbesondere Notwendigkeit, da gerade Testsysteme in der Praxis oft nicht die Anforderungen an IT-Sicherheit erfüllen.

Auch ist keine unabhängige Prüfung, z.B. durch den LfDI vorgesehen.

Quellenangaben

1. BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83.
2. Dr. Carsten Orwat, ”Diskriminierungsrisiken durch Verwendung von Algorithmen” S. 66 ff. https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/Expertisen/studie_diskriminierungsrisiken_durch_verwendung_von_algorithmen.pdf (zuletzt abgerufen am 18. August 2025).
3. L·TV auf YouTube bei 9:01, “Innenminister Strobl verteidigt Polizei-Analysesoftware Palantir”, https://www.youtube.com/watch?v=CtcKBcb71VM (zuletzt abgerufen am 18. August 2025).
4. BR, “Umstrittene Polizei-Software: Wie Bayern Palantir nutzt” von 05.08.2025, abrufbar unter https://www.br.de/nachrichten/netzwelt/umstrittene-polizei-software-wie-bayern-palantir-nutzt (zuletzt abgerufen am 18. August 2025).
5. GovInfo, “CLOUD ACT” https://www.govinfo.gov/content/pkg/COMPS-15475/pdf/COMPS-15475.pdf#page=624 (zuletzt abgerufen am 18. August 2025).
6. SZ, “Bayerische Polizei darf umstrittene Analyse-Software von Palantir nutzen” https://www.sueddeutsche.de/bayern/bayern-analyse-software-polizei-fraunhofer-institut-1.5765122 (zuletzt abgerufen am 18. August 2025).